ID: 449950
Sample Name: Denver Water COVID-19 Response _ City of Denver.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 16:37:14
Date: 16/07/2021
Version: 33.0.0 White Diamond

Table of Contents

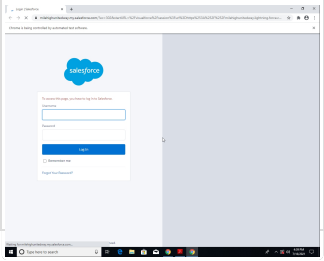
Windows Analysis Report Denver Water COVID-19 Resp…

Overview

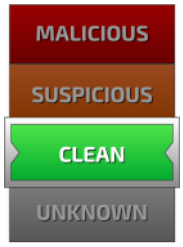
General Information

Sample Name:	Denver Water COVID-19 Response _ City of Denver.pdf
Analysis ID:	449950
MD5:	a7bcca2fdf7e024..
SHA1:	ecd2f0ba7b1e5f9..
SHA256:	3495047623e0f32.
Infos:	

Most interesting Screenshot:



Detection

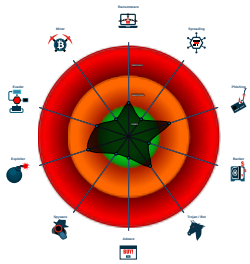


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Connects to many different domains
- Found iframes
- HTML body contains low number of …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- No HTML title found
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Unable to load, office file is protecte…

Classification



Analysis Advice

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

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 4532 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Denver Water COVID-19 Response _ City of Denver.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 4440 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Denver Water COVID-19 Response _ City of Denver.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6132 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 3488 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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12047842394824068586 --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=12047842394824068586 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6048 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1716,18340769791588095283,14740429863509864490,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=16938848815433914037 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5316 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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=787724751391022994 --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=787724751391022994 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5884 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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16674541699487182290 --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=16674541699487182290 --renderer-client-id=5 --mojo-platform-channel-handle=2128 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 6268 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'https://milehighunitedway.lightning.force.com/lightning/r/Account/0014T000004o6JxQAI/view' MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 6812 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,8292458995521785639,16987803382321267150,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

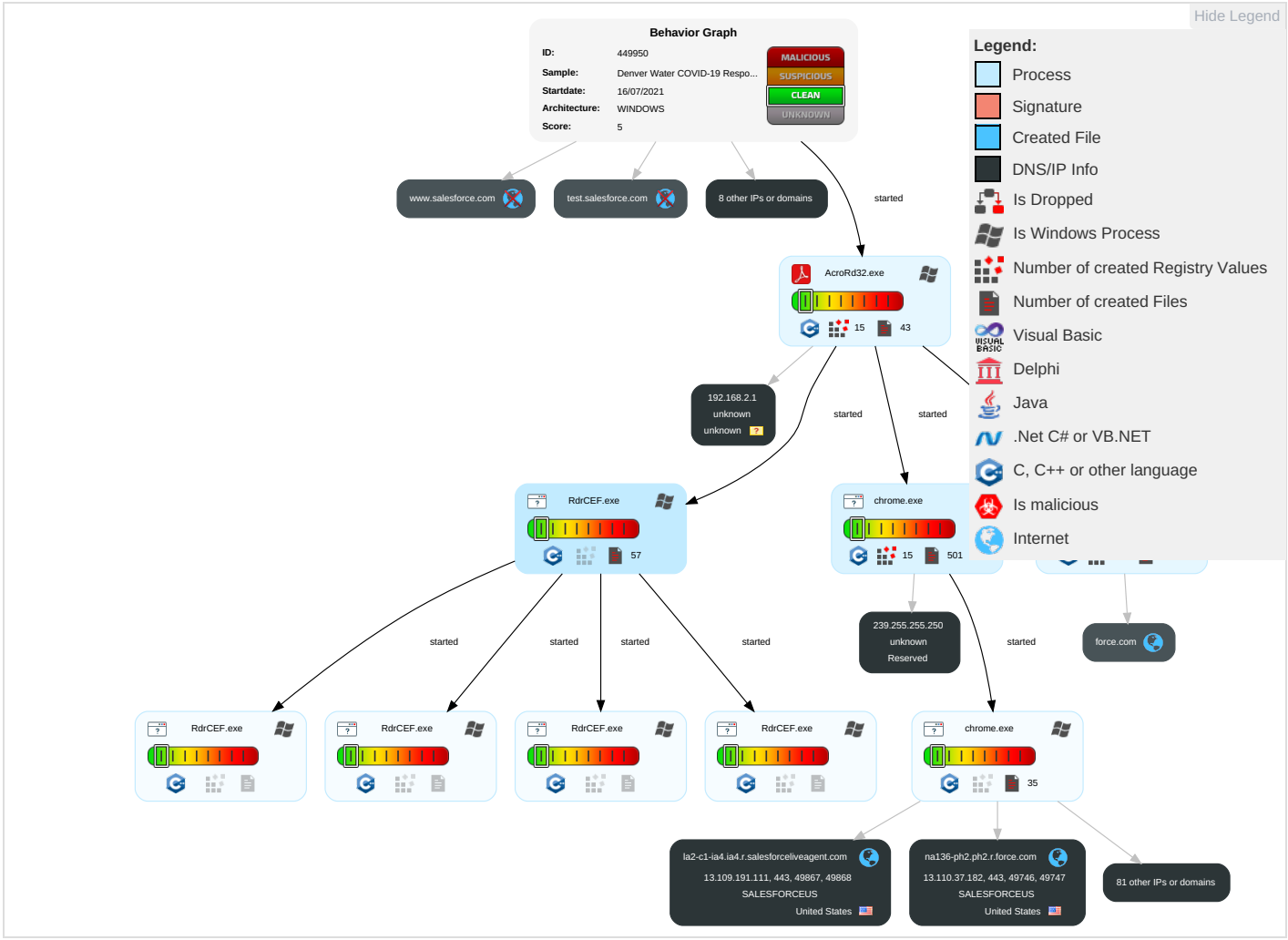
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Spearphishing Link 1	Exploitation for Client Execution 3	Path Interception	Process Injection 2	Masquerading 3	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Drive-by Compromise 1	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process 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 Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	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	D D D
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		C B F

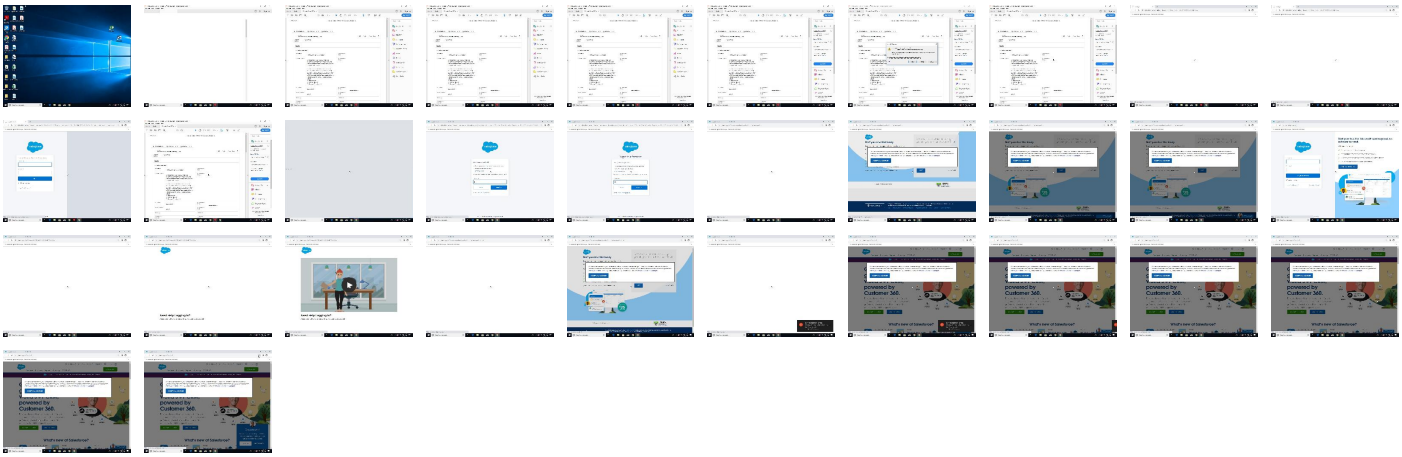
Behavior Graph

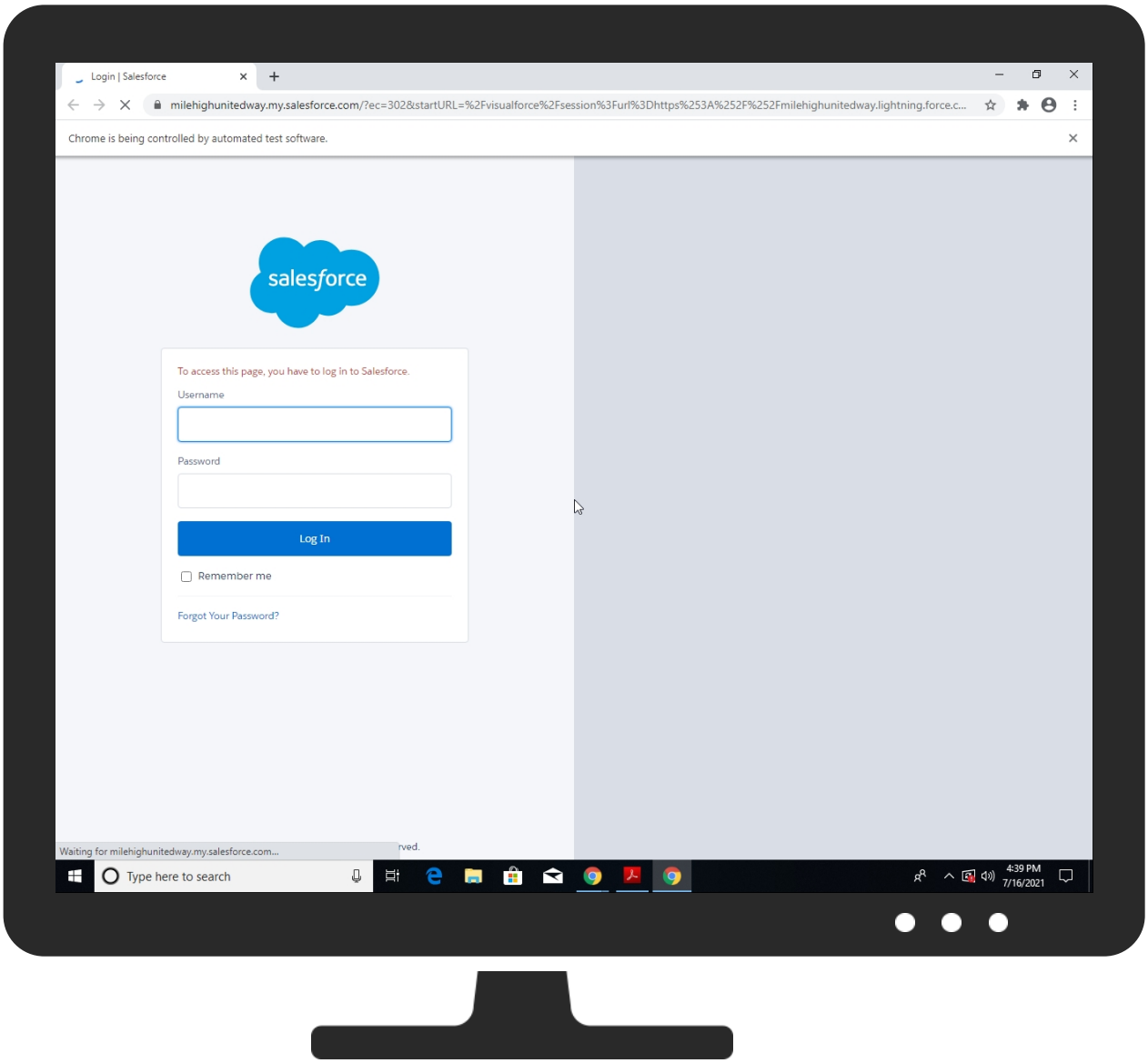


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.evgnet.com	0%	Virustotal		Browse
cs6.wpc.omegacdn.net	0%	Virustotal		Browse
api.company-target.com	1%	Virustotal		Browse
partners.salesforce.com.ssl.d2.sc.omtrdc.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ims-na1.adobelogin.comQ	0%	Avira URL Cloud	safe	
http://https://www.salesforce.com_oeu1626478795334r0.12259404291072418$$10681260716$$tracker_optimizely	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	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://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/r	0%	Avira URL Cloud	safe	
http://https://api.echosign.coml	0%	Avira URL Cloud	safe	
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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i.p	0%	Avira URL Cloud	safe	
http://https://www.salesforce.com_oeu1626478795334r0.12259404291072418$$10681260716$$layer_map	0%	Avira URL Cloud	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/R	0%	Avira URL Cloud	safe	
http://https://hosted-scratch.herokuapp.com/trial	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/iZ	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/iv	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
la2-c1-ia5.ia5.r.salesforceliveagent.com	13.110.41.111	true	false		high
na136-ph2.ph2.r.force.com	13.110.37.182	true	false		high
stats.l.doubleclick.net	108.177.15.154	true	false		high
cdn.evgnet.com	151.101.0.114	true	false	• 0%, Virustotal, Browse	unknown
p13nlog-1106815646.us-east-1.elb.amazonaws.com	54.225.136.92	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	52.211.113.33	true	false		high
test.l2.salesforce.com	85.222.152.194	true	false		high
salesforce.vidyard.com	54.205.5.87	true	false		high
d2pj9rkatqbt38.cloudfront.net	65.9.66.106	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs6.wpc.omegacdn.net	93.184.221.26	true	false	• 0%, Virustotal, Browse	unknown
na136-ph2.ph2.r.my.salesforce.com	13.110.39.181	true	false		high
na128-ia5.ia5.r.my.salesforce.com	13.110.46.75	true	false		high
la2-c1-ia4.ia4.r.salesforceliveagent.com	13.109.191.111	true	false		high
api.company-target.com	99.86.162.22	true	false	• 1%, Virustotal, Browse	unknown
raw.vidyard.com	34.234.32.98	true	false		high
a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com	3.227.80.201	true	false		high
location.l.force.com	161.71.8.169	true	false		high
force.com	23.1.35.132	true	false		high
www.google.ch	142.250.185.131	true	false		high
login.l2.salesforce.com	85.222.155.195	true	false		high
salesforce.us-1.evergage.com	34.192.141.216	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
partners.salesforce.com.ssl.d2.sc.omtrdc.net	15.236.176.210	true	false	• 0%, Virustotal, Browse	unknown
milehighunitedway.lightning.force.com	unknown	unknown	false		high
omtr2.partners.salesforce.com	unknown	unknown	false		high
c1.sfdcstatic.com	unknown	unknown	false		high
test.salesforce.com	unknown	unknown	false		high
login.salesforce.com	unknown	unknown	false		high
s.go-mpulse.net	unknown	unknown	false		unknown
kqitim5n3zwnuyhrti7a-pinofr-89940bd62-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
org62.my.salesforce.com	unknown	unknown	false		high
cdn.krxd.net	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
kqitim2qinjecyhrtjsa-f-61be14707-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
d.la2-c1-ia4.salesforceliveagent.com	unknown	unknown	false		high
c.salesforce.com	unknown	unknown	false		high
trial-eum-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
cdn.vidyard.com	unknown	unknown	false		high
www.salesforce.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
vfhbo3jsnvrutdkuee1akd0lj.litix.io	unknown	unknown	false		unknown
privacy-policy.truste.com	unknown	unknown	false		high
logx.optimizely.com	unknown	unknown	false		high
84-17-52-51_s-80-67-82-83_ts-1626446398-clienttons-s.akamaihd.net	unknown	unknown	false		high
a10681260716.cdn.optimizely.com	unknown	unknown	false		high
trial-eum-clienttons-s.akamaihd.net	unknown	unknown	false		high
service.force.com	unknown	unknown	false		high
d.la2-c1-ia5.salesforceliveagent.com	unknown	unknown	false		high
1737ad5b.akstat.io	unknown	unknown	false		unknown
assets.vidyard.com	unknown	unknown	false		high
play.vidyard.com	unknown	unknown	false		high
cdn.optimizely.com	unknown	unknown	false		high
salesforcecom.demdex.net	unknown	unknown	false		high
milehighunitedway.my.salesforce.com	unknown	unknown	false		high
a.sfdcstatic.com	unknown	unknown	false		high
c.go-mpulse.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://test.salesforce.com/	false		high
http://salesforce.vidyard.com/watch/MxeeKTO3x5oMx4jNVWWX4w	false		high
http://https://www.salesforce.com/form/signup/freetrial-elf-v2/?d=cta-li-promo-147#main	false		high
http://https://service.force.com/embeddedservice/5.0/esw.html?parent=https://www.salesforce.com/form/signup/freetrial-elf-v2/?d=cta-li-promo-147#main	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
85.222.152.194	test.l2.salesforce.com	United Kingdom		14340	SALESFORCEUS	false
13.110.69.75	unknown	United States		14340	SALESFORCEUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
52.211.113.33	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
3.227.80.201	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
52.1.220.4	unknown	United States		14618	AMAZON-AESUS	false
65.9.66.106	d2pj9rkatqbt38.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.186.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
93.184.221.26	cs6.wpc.omegacdn.net	European Union		15133	EDGECASTUS	false
34.192.141.216	salesforce.us-1.evergage.com	United States		14618	AMAZON-AESUS	false
85.222.155.195	login.l2.salesforce.com	United Kingdom		14340	SALESFORCEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.110.46.75	na128-ia5.ia5.r.my.salesforce.com	United States		14340	SALESFORCEUS	false
13.110.37.182	na136-ph2.ph2.r.force.com	United States		14340	SALESFORCEUS	false
13.109.191.111	la2-c1-ia4.ia4.r.salesforceliveagent.com	United States		14340	SALESFORCEUS	false
143.204.205.100	unknown	United States		16509	AMAZON-02US	false
15.236.176.210	partners.salesforce.com.ssl.d2.sc.omtrdc.net	United States		16509	AMAZON-02US	false
54.225.136.92	p13nlog-1106815646.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
13.110.39.181	na136-ph2.ph2.r.my.salesforce.com	United States		14340	SALESFORCEUS	false
54.76.54.153	unknown	United States		16509	AMAZON-02US	false
151.101.0.114	cdn.evgnet.com	United States		54113	FASTLYUS	false
34.234.32.98	raw.vidyard.com	United States		14618	AMAZON-AESUS	false
161.71.8.169	location.l.force.com	United States		14340	SALESFORCEUS	false
13.110.41.111	la2-c1-ia5.ia5.r.salesforceliveagent.com	United States		14340	SALESFORCEUS	false
54.205.5.87	salesforce.vidyard.com	United States		14618	AMAZON-AESUS	false
34.248.156.174	unknown	United States		16509	AMAZON-02US	false
151.101.192.114	unknown	United States		54113	FASTLYUS	false
99.86.162.22	api.company-target.com	United States		16509	AMAZON-02US	false
142.250.185.131	www.google.ch	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	449950
Start date:	16.07.2021
Start time:	16:37:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Denver Water COVID-19 Response _ City of Denver.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean5.winPDF@56/327@67/33
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Security Warning found • Close Viewer • Browse: https://milehighunitedway.my.salesforce.com/secur/forgotpassword.jsp?locale=us&lqs=startURL%3D%252Fvisualforce%252Fsession%253Furl%253Dhttps%25253A%25252F%25252Fmilehighunitedway.lightning.force.com%25252Flightning%25252Fr%25252FAccount%25252F0014T000004o6JxQAI%25252Fview%26ec%3D302 • Browse: https://www.salesforce.com/form/signup/freetrial-elf-v2/?d=cta-li-promo-147 • Browse: https://test.salesforce.com/ • Browse: http://salesforce.vidyard.com/watch/MxeeKTO3x5oMx4jNVWWX4w • Browse: https://www.salesforce.com/form/signup/freetrial-elf-v2/?d=cta-li-promo-147#main • Browse: https://www.salesforce.com/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:38:10	API Interceptor	10x Sleep call for process: RdrCEF.exe modified
16:39:33	API Interceptor	5x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.20.184.68	HocVKWxT9F.dll	Get hash	malicious	Browse	
	valRPointer.jpg.dll	Get hash	malicious	Browse	
	Remittance657.htm	Get hash	malicious	Browse	
	PRIaTJGJO2.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OLEACC.dll	Get hash	malicious	Browse	
	MFC42u.dll	Get hash	malicious	Browse	
	runsys32.dll	Get hash	malicious	Browse	
	0aSH9KLHMG.dll	Get hash	malicious	Browse	
	p9lCi2uQWY.dll	Get hash	malicious	Browse	
	runsys32.dll	Get hash	malicious	Browse	
	q7p7x4f4gX.dll	Get hash	malicious	Browse	
	q7p7x4f4gX.dll	Get hash	malicious	Browse	
	3rc4z6ltNu.dll	Get hash	malicious	Browse	
	f6718e02bc73edf5aab341fa0a7f75782bc72f7dd1a6e.dll	Get hash	malicious	Browse	
	6us663UjcE.dll	Get hash	malicious	Browse	
	xbK9XyU4LW.dll	Get hash	malicious	Browse	
	juON02msHS.dll	Get hash	malicious	Browse	
	juON02msHS.dll	Get hash	malicious	Browse	
	pvvCaP2Nma.dll	Get hash	malicious	Browse	
	IsNv5L683X.dll	Get hash	malicious	Browse	
93.184.221.26	http://pages.zuora.com/urI000sGAT0w0Q02zIxQZV0	Get hash	malicious	Browse	
	http://https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html	Get hash	malicious	Browse	
239.255.255.250	Dir.texas.gov_scanned_file.htm	Get hash	malicious	Browse	
	This computer is BLOCKED.html	Get hash	malicious	Browse	
	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	
	07xufnlKWd.exe	Get hash	malicious	Browse	
	VkaCSkmCiX.exe	Get hash	malicious	Browse	
	It.servicedesk_FAXit.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	
	Pending Doc Mail.html	Get hash	malicious	Browse	
	Machine Service.xlsx	Get hash	malicious	Browse	
	Machine Service.xlsx	Get hash	malicious	Browse	
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	
	invoice304393.html	Get hash	malicious	Browse	
	James.sowinski.html	Get hash	malicious	Browse	
	.HTM	Get hash	malicious	Browse	
	.HTM	Get hash	malicious	Browse	
	Globalfoundries#Scanned-thomas.caulfield.html	Get hash	malicious	Browse	
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVISBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	
	Remittance657.htm	Get hash	malicious	Browse	
	Setup_FileViewPro_2021.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.evgnet.com	http://https://encrypt.puzzledpuppy.com/	Get hash	malicious	Browse	• 151.101.64.114
	http://https://access-americas.ing.net/logon/LogonPoint/tmindex.html	Get hash	malicious	Browse	• 151.101.192.114
	a.exe	Get hash	malicious	Browse	• 151.101.128.114
p13nlog-1106815646.us-east-1.elb.amazonaws.com	212161C3EFE82736FA483FC9E168CE71#U007eC2#U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	• 54.84.79.88
	f2fR2CiaRu.exe	Get hash	malicious	Browse	• 34.197.14.190
	APRemittanceAdvice.xlsx	Get hash	malicious	Browse	• 3.227.112.137
	APRemittanceAdvice.xlsx	Get hash	malicious	Browse	• 54.225.136.92
	ACH REMITTANCE.xlsx	Get hash	malicious	Browse	• 52.45.207.82
	ACH REMITTANCE.xlsx	Get hash	malicious	Browse	• 52.54.121.241
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 34.199.177.216
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 3.227.150.155
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 3.210.195.34
	ACH WIRE INF0RMATION.xlsx	Get hash	malicious	Browse	• 34.206.132.96
	ACHWIREPAYMENTINFORMATION.xlsx	Get hash	malicious	Browse	• 52.70.29.70
	ACH REMITTANCE INFORMATION.xlsx	Get hash	malicious	Browse	• 54.83.3.241
	Red Gospel Mission Due Invoices.htm	Get hash	malicious	Browse	• 3.213.63.216
	Copy Of REMITTANCE.html	Get hash	malicious	Browse	• 52.206.2.145
	SecuriteInfo.com.XLSX.Onephish.B.genCamelot.17169.xlsx	Get hash	malicious	Browse	• 52.5.81.176

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.XLSX.Onephish.B.genCamelot.17169.xlsx	Get hash	malicious	Browse	• 3.225.88.81
	03 -16 - 2021 ACH REMITTANCE.xlsx	Get hash	malicious	Browse	• 52.71.207.224
	03 -16 - 2021 ACH REMITTANCE.xlsx	Get hash	malicious	Browse	• 54.210.71.80
	SecuriteInfo.com.XLSX.Onephish.B.genCamelot.9847.xlsx	Get hash	malicious	Browse	• 52.20.51.112
	A6C8E866.xlsx	Get hash	malicious	Browse	• 54.88.126.21
na136-ph2.ph2.r.force.com	http://https://storage.googleapis.com/dsafghjklbvc/9988.html#qs%3Dr-afcciafjbikkcfbaebccdfhaedbgbhjaeededababababaedahhaccafhdacfgjagejkjacb	Get hash	malicious	Browse	• 13.110.36.182
	http://125cf87b21e3.tc-traffic.com	Get hash	malicious	Browse	• 13.110.37.182

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Dir.texas.gov_scanned_file.htm	Get hash	malicious	Browse	• 104.16.18.94
	KLBV6Q7wcc.exe	Get hash	malicious	Browse	• 104.21.19.209
	ISttudHp32.exe	Get hash	malicious	Browse	• 172.67.208.68
	BIDA5wExN6.exe	Get hash	malicious	Browse	• 162.159.129.233
	HocVKWxT9F.dll	Get hash	malicious	Browse	• 104.20.184.68
	This computer is BLOCKED.html	Get hash	malicious	Browse	• 104.18.10.207
	triage_dropped_file.dll	Get hash	malicious	Browse	• 104.20.185.68
	INV420.xlsx	Get hash	malicious	Browse	• 172.67.197.226
	order 0721 Review .doc.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	• 172.67.169.145
	order PI specification N0-00128835%%.exe	Get hash	malicious	Browse	• 172.67.144.50
	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	• 104.20.139.65
	07xufnlKWd.exe	Get hash	malicious	Browse	• 104.21.51.99
	6rg5Enu1ks.exe	Get hash	malicious	Browse	• 104.23.99.190
	RFQ REF R2100131410 pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	samples.exe	Get hash	malicious	Browse	• 172.67.188.154
	VkaCSkmCiX.exe	Get hash	malicious	Browse	• 104.21.51.99
	deepRats.exe	Get hash	malicious	Browse	• 104.21.8.254
	Img 673t5718737.exe	Get hash	malicious	Browse	• 104.27.195.88
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 172.67.129.41
SALESFORCEUS	http://delivery.unlocklocks.com/HSOMEU?id=124732=Jx8EBwNQDgsBTwECUwcIUlUBUx0=QgtZWk8ADFsJdkUDDQ9cU1AITVAdXENVHwYOUlwHUlMHUgMPUFtXAVMPTwoQF0QMHktdXV9aR1cRThYXC10MAl4OWlUKEE1XDVscKjcseXNkW1BcT0UD&fl=DBdARkJeFhdeXFVXEVleAwhYDxhRB1tCAA8AVRBTHQELDhtTYg1eVkAc	Get hash	malicious	Browse	• 161.71.23.64
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 161.71.10.172
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 185.79.140.13
	http://https://fax.quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 136.147.42.7
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 136.147.42.135
	http://https://0fficefax365.quip.com/FENkAKwe58Ee	Get hash	malicious	Browse	• 185.79.140.13
	http://https://online-banking.kb4.io/XYWNl0aW9uPWeNsaWNrJnhVybD1okgdHRwgczovL3NljY3oVyZWQtbG9naW4ubmV0aL3BhZ2VzL2RiOTY4MTUzYzA0JnJlY2lwaWVudF9pZD03NDMxOTI2NzcmY2FtcGFpZ25fcnVuX2lkPTM5Nzk2Njc=	Get hash	malicious	Browse	• 85.222.155.67
	http://quip.com/LLroAibwIjjK	Get hash	malicious	Browse	• 185.79.140.13
	http://https://gs635.scout.es/DocuSign	Get hash	malicious	Browse	• 161.71.23.64
	http://https://account00.quip.com/KLMTAbWkf2YG/Secure-Message-Notification	Get hash	malicious	Browse	• 136.147.43.7
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 161.71.23.64
	http://https://quip.com/Vrk5AwJuoYZl/Secure-Message-Notification	Get hash	malicious	Browse	• 185.79.140.13
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 13.110.68.35
	http://https://call.lifesizecloud.com/4478671	Get hash	malicious	Browse	• 13.110.8.132
	http://https://us-tdm-tso-15eb63ff4c6-1626e-16939b523e6.force.com/nysba/login?c=to5OtXqGSMHWKoxDXd7ps9s7j_NEUhCwr_h6Q6yIv1EPCK2wzfx3rS4f66_gX.pIulGK5YxD.Mfm8rOEMT4YfMWqaCvrmmuRDUoJ7KruZZHpfdb7M7R9aGW7EgB28DOZ92Fv7BpOBilcHSza30m_b_nSZ5XfppwOUH.Tv5pEchdswhNVEKCyVLtrYcUNRH1oAOIeC_pe	Get hash	malicious	Browse	• 85.222.152.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.google.com/url?q=https://talibllc--c.documentforce.com/sfc/dist/version/download/?oid%3D00D4W0000092RKF%26ids%3D0684W000007pR1HQAU%26d%3D%252Fa%252F4W000000Putz%252Fms_BmovqE_WXkJYztxhvReEhZJLVdobKujH1zudqg3s%26operationContext%3DDELIVERY%26viewId%3D05H4W000000luGyUAI%26dpt%3D&sa=D&ust=1604432432908000&usg=AOvVaw2LctXUh7R_FyT0gHvTDxLU	Get hash	malicious	Browse	• 13.110.66.96
	http://https://bgqfwsaw9whw.com/we/ds/dxl/dive/index.php	Get hash	malicious	Browse	• 161.71.23.64
	http://https://www.bestflbeachhouse.com/Urgent-docs/microsoft/	Get hash	malicious	Browse	• 161.71.23.64
	http://https://mandrillapp.com/track/click/31051831/www.windstreamenterprise.com?p=eyJzIjoibkZVWFZGMEN0V2tTOGRnWTRlUDFFQl90Z1VrIiwidiI6MSwicCI6IntcInVcIjozMTA1MTgzMSxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy53aW5kc3RyZWFtZW50ZXJwcmlzZS5jb21cXFwvc3VwcG9ydFxcXC9cIixcImlkXCI6XCJjMGQxZTQ1ODEwN2M0YjI1YmFiNTVhZTNhYzFmOTY4Y1wiLFwidXJsX2lkc1wiOltcIjFjNWUyNDQ2NDZhNTgxZDQ5YTNmZGY1MzNmMGE2ZWUyMjkyODE3NGNcIl19In0	Get hash	malicious	Browse	• 136.147.57.1
SALESFORCEUS	http://delivery.unlocklocks.com/HSOMEU?id=124732=Jx8EBwNQDgsBTwECUwcIUlUBUx0=QgtZWk8ADFsJdkUDDQ9cU1AlTVAdXENVHwYOUlwHUlMHUgMPUFtXAVMPTwoQF0QMHktdXV9aR1cRThYXC10MAl4OWlUKEE1XDVscKjcseXNkW1BcT0UD&fl=DBdARkJeFhdeXFVXEVleAwhYDxhRB1tCAA8AVRBTHQELDhtTYg1eVkAc	Get hash	malicious	Browse	• 161.71.23.64
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 161.71.10.172
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 185.79.140.13
	http://https://fax.quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 136.147.42.7
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 136.147.42.135
	http://https://0fficefax365.quip.com/FENkAKwe58Ee	Get hash	malicious	Browse	• 185.79.140.13
	http://https://online-banking.kb4.io/XYWNl0aW9uPWeNsaWNrJnhVybD1okgdHRwgczovL3NljY3oVyZWQtbG9naW4ubmV0aL3BhZ2VzL2RiOTY4MTUzYzA0JnJlY2lwaWVudF9pZD03NDMxOTI2NzcmY2FtcGFpZ25fcnVuX2lkPTM5Nzk2Njc=	Get hash	malicious	Browse	• 85.222.155.67
	http://quip.com/LLroAibwIjjK	Get hash	malicious	Browse	• 185.79.140.13
	http://https://gs635.scout.es/DocuSign	Get hash	malicious	Browse	• 161.71.23.64
	http://https://account00.quip.com/KLMTAbWkf2YG/Secure-Message-Notification	Get hash	malicious	Browse	• 136.147.43.7
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 161.71.23.64
	http://https://quip.com/Vrk5AwJuoYZl/Secure-Message-Notification	Get hash	malicious	Browse	• 185.79.140.13
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 13.110.68.35
	http://https://call.lifesizecloud.com/4478671	Get hash	malicious	Browse	• 13.110.8.132
	http://https://us-tdm-tso-15eb63ff4c6-1626e-16939b523e6.force.com/nysba/login?c=to5OtXqGSMHWKoxDXd7ps9s7j_NEUhCwr_h6Q6yIv1EPCK2wzfx3rS4f66_gX.pIuIGK5YxD.Mfm8rOEMT4YfMWqaCvrmmuRDUoJ7KruZZHpfdb7M7R9aGW7EgB28DOZ92Fv7BpOBilcHSza30m_b_nSZ5XfppwOUH.Tv5pEchdswhNVEKCyVLtrYcUNRH1oAOIeC_pe	Get hash	malicious	Browse	• 85.222.152.195
	http://https://www.google.com/url?q=https://talibllc--c.documentforce.com/sfc/dist/version/download/?oid%3D00D4W0000092RKF%26ids%3D0684W000007pR1HQAU%26d%3D%252Fa%252F4W000000Putz%252Fms_BmovqE_WXkJYztxhvReEhZJLVdobKujH1zudqg3s%26operationContext%3DDELIVERY%26viewId%3D05H4W000000luGyUAI%26dpt%3D&sa=D&ust=1604432432908000&usg=AOvVaw2LctXUh7R_FyT0gHvTDxLU	Get hash	malicious	Browse	• 13.110.66.96
	http://https://bgqfwsaw9whw.com/we/ds/dxl/dive/index.php	Get hash	malicious	Browse	• 161.71.23.64
	http://https://www.bestflbeachhouse.com/Urgent-docs/microsoft/	Get hash	malicious	Browse	• 161.71.23.64
	http://https://mandrillapp.com/track/click/31051831/www.windstreamenterprise.com?p=eyJzIjoibkZVWFZGMEN0V2tTOGRnWTRlUDFFQl90Z1VrIiwidiI6MSwicCI6IntcInVcIjozMTA1MTgzMSxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy53aW5kc3RyZWFtZW50ZXJwcmlzZS5jb21cXFwvc3VwcG9ydFxcXC9cIixcImlkXCI6XCJjMGQxZTQ1ODEwN2M0YjI1YmFiNTVhZTNhYzFmOTY4Y1wiLFwidXJsX2lkc1wiOltcIjFjNWUyNDQ2NDZhNTgxZDQ5YTNmZGY1MzNmMGE2ZWUyMjkyODE3NGNcIl19In0	Get hash	malicious	Browse	• 136.147.57.1

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	07xufnlKWd.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Machine Service.xlsx	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Machine Service.xlsx	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	.HTM	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	.HTM	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Remittance657.htm	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Setup_FileViewPro_2021.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	INV_289553.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0IpZWFS8v8.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	#Ud83d#Udd0aMsg_ 3pm.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	MiiefP6Jj7.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	Admin's-Protected-Fax.htm	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sahiba_8.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	xSnF0lxFUX.exe	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	AhyARattach.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92
	attach.html	Get hash	malicious	Browse	• 85.222.152.194 • 34.248.156.174 • 13.110.39.181 • 54.76.54.153 • 151.101.19 2.114 • 34.192.141.216 • 151.101.0.114 • 85.222.155.195 • 34.234.32.98 • 13.110.69.75 • 52.211.113.33 • 13.110.46.75 • 3.227.80.201 • 13.110.37.182 • 52.1.220.4 • 161.71.8.169 • 13.109.191.111 • 13.110.41.111 • 54.205.5.87 • 54.225.136.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	07xufnlKWd.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	VkaCSkmCiX.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	A6uXdzis1N.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	m35HWit4so.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	p0TE6JV9Hr.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	jTSeQwTKtv.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	xes1eITfus.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	It.servicedesk_FAXit.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Machine Service.xlsx	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	UeEFnSPkuV.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Globalfoundries.htm	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	xSdXan6nb2.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	E9p5JOcy77.exe	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Globalfoundries#Scanned-thomas.caulfield.html	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVISBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66
	Remittance657.htm	Get hash	malicious	Browse	• 65.9.66.106 • 54.205.5.87 • 13.110.39.181 • 85.222.153.66

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:	moderate, very likely benign file
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 GM DS.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):	615
Entropy (8bit):	5.68439113937935
Encrypted:	false
SSDEEP:	12:vDRM9Q/jZiEiHDRM96NkZiEVDRM9XyZiE:7h/8E69NBExePE
MD5:	D482DA0C0FA109ED60EC9A58FBE86888
SHA1:	6E7B9FE3047623CECFEEE49B83345C5FE41E1C9F
SHA-256:	CFCB6F355CFA7E9F984862B938244A1D0064D7C460F3F6FF20FE3359CFEC9701
SHA-512:	90EDDDD820987B3B771069C3E2157A615461C57252870934C88F3B1BE7EF436978FD7158ACA11B803E8C41F4684E6C4F4704D7FF5ACBC54A6F324290B1B1EDF6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....].%/....."#.D..M..<.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....P.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....].%/....."#.DV....<.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....p`P.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .._.].%/....."#.Dl.)..<.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....I.....

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):	522
Entropy (8bit):	5.641208487482032
Encrypted:	false
SSDEEP:	12:V9zkXTZ9PQ+H9zVv1wi9PQh/P9zDS1O39PQ:XzkXTZ9PQ+dzVNf9PQhNzCa9PQ
MD5:	69D905FA84C8E1A388D0ED55513C681F
SHA1:	12E2C20D8F4AF7613A5E5823DB52C519AF67D722
SHA-256:	A6DD02B535D29F90DD702F22C908BFCF36BF3063CE5F78AB16BFD1AAAF33598E
SHA-512:	AD3740FC407856BF9E1CBCF79DD21BCA49DCF7BC6E3408337C8B7F9981BEF0C9FF1E4DBEC3B318FEF95D8555BC10C519378859946AAC5A2D84BD09523F0419E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...^].%/....."#.D....<.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....@.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ."..].%/....."#.D7UR..<.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....SJ.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..x.].%/....."#.Dr....<.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....p.....

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):	738
Entropy (8bit):	5.620151304135933
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFnS+ajvlUo6jf2yeRVFAFjVFAF54/ZGuvlUo6jE7yeRVFAFjVFAm:tB4v4nSZjSBGB4v454/ZjSB2B4v4AkSB
MD5:	FE0A22C38AF4E9355075A3DA774AD648
SHA1:	F458DA8018AD38D43E000944AA08D6F71B6E6828
SHA-256:	B9A7429C707E082EC16CBFA043524DBC80CC1CE492320994EE961C7F0A4F3642
SHA-512:	8AF6A275CBF033D5C97245C24583E5BB096685CFECC624EB7D19DD40396589527BACC0EBEB98EA0702E78F4FAA663B9BB0001D2D4FDA4B616A6DAC975E700F D5
Malicious:	false
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..I..<.A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....cC.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...].%/....."#.Dc...<.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....5.....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..$..<.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....KC^.....

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):	464
Entropy (8bit):	5.703793034044621
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RssU11JiWulHyA1TK6t7U/llMNtVYOFLvEWdFCi5Rsa5Aeew:IbRkiDqSWusshUtYbRkiDhehoWussLt
MD5:	0B13305863C53843D103D96AD92D57BB
SHA1:	7C8615B9B82A47E0F4621E6D90299B5E6DEEA2F8
SHA-256:	CFBEE64D6C9A516E45F72E81B39F74269C05C74C60A4EE8ED7C2027A96BF05D2
SHA-512:	051B6971ADD5EB2FF007326587B1F76283E357AB0ECD0CD03D2A458C1D650AF1357123ACBDF2BA9A3AEE629299F5621882190CCAB5F963F43F89F4F2C2ADDE 3
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ....].%/....."#.D.....<.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....yz.a.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..V.].%/....." #.D.....<.A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....WK.,.....

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):	5.5557033501491
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu+ejRVyh9PT41TK6t:pyixRuAejRV41TE
MD5:	4F10E3E902C7B4372C3C0D412DE8A8A7
SHA1:	5F3CB4C87A61C9AD66E847BFE2EE2969F4044910
SHA-256:	26D4A50C6AB7EC3F746E582D694785C7000891363835723403E8E68B94CCEA01
SHA-512:	D3AE950615F44115FB90ABC809A1CD5720632DB36EFF84615BA87067DA79E2EE4FFA69C780B3FEACAE34F7ECB988357FB6739DDB0339574ACF28CEB1440D65 9
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .K..].%/....."#.Dx|#..<.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....g.....

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):	5.593870126904983
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVpi125jlSco2sZl8xeGvP5m1TK5i:mvYOFLvEWdhwjQD2XSLZIl6P41TK6t
MD5:	E684B76D93D433E7ED1A216156CE5671
SHA1:	FEE47EE8E8E8932EF805F7515604B1FEAAE62DE2
SHA-256:	C6A9C9FABCD1999E279E1E150AB460660D650B36B06794CD31BC8922F36A7280
SHA-512:	78CBB228D58DBB36BFCA6A9422F3035AB8381B1AD5B73909F8F83C1F28370FA710E910CD63B3D1EA0465652250B7E94F5106BF9306FF281ADA8C930DD8488558
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....].%/....."#.D.....<.A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.542909074501602
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQNX22unlV6g1TK6t:2RHRQCa2k1
MD5:	6004D67AD733977F66A2F8D80ABBC9A3
SHA1:	0293C62C4008ECA82D9E6ABAF0E05B107CECC8A2
SHA-256:	53ECDB28739DE64DD1443E7F8C268C7957B39B1FC75E1F2D9102A6FE0AF855A7
SHA-512:	4999DDF786FE995F05BBD67877175AD7EE9336DC34E6978A4176918E04F2116461D78C4F8DC49FEF31AC232F2A1CFD789CFA0C1C163205349924C7AAB52EE9D
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .Y[.].%/....."#.D..#..<.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....X.^.....

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):	537
Entropy (8bit):	5.600529414745145
Encrypted:	false
SSDEEP:	12:Z5MZ0NXMuR/E15MJbMuR/Ey5MPe6MuR/E8:ZSWcuR/E1SJYuR/EySWTuR/E8
MD5:	D945C98FEC5B8BDAD8C6970ECB2A1338
SHA1:	D2A7B55ED37F7097039FAE5BFB67C5A9EBF54A93
SHA-256:	409C22F07EB3AA6D18309D07036A3475C8A6A3EAB914AA2369029E6BF9F806C6
SHA-512:	7554490982E3EF35FBB972AAC509821775EEB65266017FCBB46CCAC9589AD359DA3E2CF88A996B3D45A3D9941595A7903753792137496AB32810022E9B889763
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...^].%/....."#.D3....<.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....H.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....].%/....."#.D.-S..<.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....^q.....0\r..m.....3....<lb.. .._keyhttps://rna-resource.acrobat.com/base_uris.js .n..].%/....."#.DB....<.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....l.....

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):	5.494395677365045
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuZ8Wr+by0zBUKSAA1TK6tcX:pRS9r+beS
MD5:	AB93A45D946A4B44CBCBBF4BC5B748F3
SHA1:	CA918BEAD7C3CDA7B24BFB64F1D1061360E650F3
SHA-256:	0E191DAC9B4FCE57CAFB49D1F719449C65394E177EE59417C069495E990A4757
SHA-512:	6FE791565DF1012D7A65B2E44F090F034DF96AFB3AE9916A27E01BA430593D1139A2E443F08B6AB7CE19BB34563F84DFCA5461F9E49C596172CF134A43F7DDF2
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .f0.].%/....."#.D.e$..<.AQ..E.=....=h`t..t..3%A.F$..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
Category:	dropped
Size (bytes):	531

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Entropy (8bit):	5.591467804002959
Encrypted:	false
SSDEEP:	12:KkXxKMSCvU1XtUlMokXxKMSCvY3tUlJkXxKMSCv+DotUl:KkXxiCEXWMokXxiCA3WJkXxiCmkW
MD5:	4A1C22A1083E711C58190076AE07B1E9
SHA1:	88E1EA8AA0957030A95197F6A5A5FE6B22E099F3
SHA-256:	23BD21EB5235C9B96764D5BF3D1E0EF38EDE114514B3EAE7C924E2E4B65CFF53
SHA-512:	17D67089BB406757746A29C4C53A1E62C6CF64A85FD5869EF8CA87251F55445EA66AEB092F08FA189C731AFF898E7E934267F08C12C59BAB30861AFA9D066DA5
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .L.^].%/....."#.D+....<.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....RT.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ....].%/....."#.D9.R..<.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....>.....0\r..m.....1.....5...._k eyhttps://rna-resource.acrobat.com/plugins.js ./{.].%/....."#.D.V...<.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....k1.J.....

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):	561
Entropy (8bit):	5.600433795599596
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL97o/jryyM+VY1TK6tXlEkl9YOFLvEWsfOLkFuyyM+VY1TK6t2:5h6OL97o/nkxlbh6OLkwkqh6OLN/k6
MD5:	D214CC16E16A28BA2411DEC02CDC54CD
SHA1:	EEAE2E794383A02B7AA979789319A0AA30521441
SHA-256:	965412CD51780980F72F7EA699F0D92D16CF5BCE3FC78782589F77AB28F90F21
SHA-512:	F7DA1C184BB8BCFFEE52EA420A1DA9EAC8574E1C0686BC64D751A7521722AA59AC08742C08CF904E71E6D0A155E90736DF856E3BED5E48DE4F2575F4A6FB29 AB
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .Osr].%/....."#.D.....<.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....0\r..m.....;... I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....].%/....."#.D..}..<.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....*I.....0\r..m.....;...I....._keyhtt ps://rna-resource.acrobat.com/static/js/desktop.js ..].].%/....."#.Dd....<.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....oC.....

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):	732
Entropy (8bit):	5.641569761729137
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFeLe2wSeKaTLnfRVFAFjVFAFIFwSeKaTLnxRVFAFjVFAFVzwSeKaTj:UB4v4z2wzXLnfB4v4IFwzXLnxB4v4Vza
MD5:	9E9319CF9E31F49A6655F314EBFF9BBD
SHA1:	966AAD73EA190259B83DBEEB985C45FE8C027624
SHA-256:	33086754B999045D04F821A21CA19406CED7F79E049773A42581ECE943BF2B2B
SHA-512:	D89D9523A1CE8A84BB7EA6F4C0E881D57F1E0B777CFA05194434EC2C34967F93F9F40D755EA8E42CDB682BF8CF080E56E0CC07F9A461A09E1FEC406F911FE38 B
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..%.].%/....."#.D..S..<.A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....i.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/ plugin.js ....].%/....."#.D!W...<.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 .\..].%/....."#.D(.'..<.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....N.....

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):	5.512522683193305
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXup1atP11TK6t:BsR2Ese61c
MD5:	A6B13744AFCFA72930686FC23E1A9993
SHA1:	47F1259F7A7432C9EAF1F58201B87C6EC2A808B9
SHA-256:	F98AA3B5F50BAEE4B0202C8BE81A4441682F891234837B78C66604C0F9F4E462
SHA-512:	98FCA15ECB546B3A3519EFE1B74FA2EAFD8FC62C3E2AF1C4B5BC52A47A7CCAB23B9B4ECC22CA0FB024B81DB22AF7A27F26FD45F2704CB8E0C9AFCAF61D1C 4B3F
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ....].%/....."#.D7."..<.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.629369456843931
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQkch6MB7OhKlvA1TK6tH:RbR16jG6MBJkt
MD5:	E78C33F59A82D8A7848F336DAFB31C65
SHA1:	04EB9FF974B04801A23E55FE60779C9C00ECD78F
SHA-256:	EE2CA1B28191B6792B2AE183D86E5DE4FAC87B32091391E6E886BFB2C0330ECC
SHA-512:	360F01679B7C7B02DC7DE474D87E1FED72109A988616B4A98E5B302C1547637FABD602A0C6DC2F9F924CCD6595164330D87C9FF0E30C26A35CE781B2A450382
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .Z..].%/....."#.D.Z...<.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... V:z.....

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):	5.576255324902857
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuHqYgpnQdFt1TK6tP:B2geRHRQ6qb0
MD5:	5B83FD08693F458B9863060838CD7A33
SHA1:	29748B5A25AE4C2E7B63B8D92A8ECEB1823BE239
SHA-256:	410C1C9840E90B1916567C3B04E9F5E39F82D1113600A21456AC4590C209955E
SHA-512:	8A28C1EC9868C8D2AEBC0B380C1C1D4674C355D6CBA0FA2F022D9C1EDEF5BCA1A8BFBA7F51E6A02D760AC8A9E35CE042E80B3990772C38C7507491A8BD0C1 A47
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ....].%/....."#.D..$..<.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....s..N.....

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):	618
Entropy (8bit):	5.646776915978888
Encrypted:	false
SSDEEP:	12:WyeRlk+ct1wJJMyeRltXayt1wNyeRlv1EEt1w:WJMlfwJJMJVXayfwNJl9fw
MD5:	E2831B875FCBAA1B4EFBC08853E399CC
SHA1:	631E3AE5FC45B3307000E97C6E54D08457A2A47D
SHA-256:	456FDF3C0C3EFBEBD28D70EF87980638C68977C774F44E2003C070DF10C1896A
SHA-512:	02E63D99E425070887B3F177101E7C46F9ECB2E257B860F94AA52A0265A06CA2CC5B759EA97CEF3499C16CEE6EFE58DDC52C3896646347E731513E7956C6A52
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...u].%/....."#.D.. ..<.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ...u.f.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..{.].%/....."#.D#1...<.A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....!.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..D.].%/....."#.DG ...<.A.t\a.....x5.'OuE.C..@.....x..A..Eo.. .....A..Eo.....Q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.557600412616798
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu65AeIWDsqwK+41TK6t37l:wRhneerD9wK+Et
MD5:	D5A13D2119579D193284CD6727197CB8
SHA1:	EF3F30E1F177AC9BF0C55EEACC0B079A1EB0B126
SHA-256:	774E6CC13B3A9DDDC1C7C520B91CDD03DA5761DEB62F5EFDAC855625C264F317
SHA-512:	F401A2A6E7B01896A7BC8747661266BAE3F406402DC9058BDD8C8DD4C10E3FBDBC908549384C8AC4B9EF6ACDD8F81CACCD594010C11B0289310518F615FBEA BA
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ....].%/....."#.D.3...<.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....u.....

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):	690
Entropy (8bit):	5.627778622865002
Encrypted:	false
SSDEEP:	12:/RrROk/NZA/YfLEtRrROk/YV8mfLE43RrROk/tAfLE:/PJ/7AA4tPJ/Pm443PJ/tA4
MD5:	47117E472137DB0620223E38AE5598AC
SHA1:	FFA2D548A64B060C4C122158AE763F4D8BA957C0
SHA-256:	6A9E4B06C0EA332B4A7E0F9702C807647AEB1A3A051922C6E812097263FA3953
SHA-512:	814DCE62BFEC90621A565186B69D5FEDA8B145D290E5E4862996BE6028743580651987E778B96124793C84ABA610CA34110F094543F0E20F0FA02FFBD91ADDC4
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .J.u].%/....."#.D.. ..<.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....3.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..O.].%/....."#.D.....<.A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....D.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .. ..].%/....."#.D=....<.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....Yz.....

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):	558
Entropy (8bit):	5.624510768848606
Encrypted:	false
SSDEEP:	12:xqTJU8cCPLniBqTKNDCPLnDqT71iL5CPLn:APcMniQ+DMnGNiFMn
MD5:	BC51BA354CE8E8E854E1DEE070BF5DCF
SHA1:	DDC7CD6E4446DB2831A72A52A94A279BD9430F03
SHA-256:	E39B7FBBAB700C2BAA5125B511B4745315F820FE8683CFE8AD7CD1AEE2507631
SHA-512:	82DD2FFC9EAD9E1F9CAE8278C163EDE9011CBA87F7AB24C2214BB9F1F414205D0FBC3EBA8CD0E24BD3FADA7DE1E4BE0A38E1F551ABB3010FCD9CCF6E84FE BEF1
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...q].%/....."#.D.....<.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....).....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....].%/....."#.D..}..<.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....{.....0\r..m.....:....f....._keyht tps://rna-resource.acrobat.com/static/js/config.js .HP.].%/....."#.D.....<.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.659461857538949
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAu+v14h91IsEJ41TK6tX52YOFLvEWdMAu6teQkeIsEJ41TK6tsMN:zRMQNUWsDURM+eneIsDeZRMn17WsD
MD5:	11B3ABA71D7FD5F2A993EE2093DA78DE
SHA1:	406740427EEBA318CE3926D5634254077ADB5D73
SHA-256:	806A0C8A9C20B48F4325CF03C45B930786EAFB4B57724C40966EE8FF60FEF595
SHA-512:	39D99721DD74916175FB6F981F9C121467FE0B31A8F1C2D958A2D798B8FA9B89882312A00D2810D82F5823C732CC5FAD879E4E1CA89350623A5C5CB406504522
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....].%/....."#.D..I..<.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... ....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....].%/....."#.D.....<.A..z._a...'.v.....4p3..1.']...A..Eo.....A..E o.....9=.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..4.].%/....."#.DD4#..<.A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....zG:.....

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):	630
Entropy (8bit):	5.644648280041985
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
SSDEEP:	12:6lJRJeeCFoMoMlJRQeFRTFoMfqMlJRwXFoM:YX/CFoMTvFhFoMFuXFoM
MD5:	6BDD7011ACE4F417564F081D5AC2AF93
SHA1:	97A501E4162055C4FA8D075692BFEFD65F0AD8A7
SHA-256:	E5921AE23C3C40F6C7543EFEEF14897FD389F802ADFB76E0E66437489CD1C5B9
SHA-512:	62C02D2749B5B9FE7BAABFA6558C9B6373010A3DAA8C222B5D987C4BFABDC93C8AC77CDF3BDBE51FDF95375FDF4C045FE83C98BB014A0F52DDEDAF3EA773C21E
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ....].%/....."#.D..I..<.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....+.....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .. .].%/....."#.D.....<.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....r).....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..6.].%/....."#.DJ^#..<.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.6469193432518585
Encrypted:	false
SSDEEP:	12:F8hRrROk/lSHe2f8hRrROk/+voe2k8hRrROk/fb7e20:UPJ/lS+2KPJ/u72lPJ/f+20
MD5:	43F798F2A0D713BA1EAC020699345D17
SHA1:	DA7AE2D4B32630619714DE40BFBF38539B20ADD2
SHA-256:	07D08586C89FDFC2C9CC63B41B50A7528D920AA92BACCFEA2B931ACC5A0841BA
SHA-512:	7CA1CE20136AFE9C5992B87748FFF91AF7A54970E1DB005D5EF89538377268A01F842E42E4E5D2AE119B7AB8429A115C8BD09E76B9ADBAB06340ABB6EBE2760E
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...u].%/....."#.D.....<.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..M.].%/....."#.D.....<.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....8x.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....].%/....."#.D.....<.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....J..4.....

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):	639
Entropy (8bit):	5.709541460179313
Encrypted:	false
SSDEEP:	12:ehRcveNrNJIC1uhRcS/jnDirNJIC1hRcyZqrNJIC6:ehJvJICAh5/jnDGJIC1hBlJIC6
MD5:	74974C22AADC85D980CB6317017C82B0
SHA1:	CF6558CAF9D3B77AB17874705D9E2378561B51FF
SHA-256:	D470F697E4949B4AE5BAE40FC761682FDEF20EF4916F72CF504E655067C46B8E
SHA-512:	D29129189DD09C355A7F6177C42D7644C4AD9BD421B8040581EB1229FF48CE58626C998158F27F7BA45635302ED2F2D7BD348E931AB5274F6F5977C598A52790
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .M.u].%/....."#.D.= ..<.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....p.f.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....].%/....."#.D.^...<.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..F.].%/....."#.D.C...<.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....p.O.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.627227455194031
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuBeeHhLzgm2d/1TK6tkOEYOFLvEWdrIhuBGVhLzgm2d/1TK6tI:0RSe5Re8RyLReLpReX8ReN
MD5:	4DD265C4E7C7401315C7013169037B7F
SHA1:	D24BAEB4F91FAC28A8763FF6847B0BC35E29E6DE
SHA-256:	8EEE493FB2A240442FC5C741D0336912E15123246C0556A37AA61D43ECBAD8FA
SHA-512:	7F728983FD19269072A654089DEE5C6EA745436F43EB0FA7D9AFA3A9C435CE9A5420B868B8E7D34BF9F9F428F7168BCC52FB7C8AE494DE60C62F42030AEA6FF
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .).u].%/....."#.DK"...<.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 ..3.].%/....."#.D....<.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 ....].%/....."#.DK....<.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....S.\.....

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):	564
Entropy (8bit):	5.637665100278707
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KveFkx56uvp1TK6tMAElVYOFLvEW1K34e+XqBkx56uvp1TK6tAg:6JJK2G6JJKoPXqq6wJJKaTo
MD5:	479222959953B04CB1FF9D705B8DD4E8
SHA1:	C62878441158B045DC091863B287668AAAB4C8CD
SHA-256:	782547B30E590C6AA956D131D01C81E8EAC49660695DA0F66F7848DDC05087FB
SHA-512:	219C98C7A1162E521185BC3B35375638DAF50AFAD5BE58A5DF9D978F3C21C4C787D9C1E3E172C2D3FCE529664344657D6E34AB56802784840C2D0E91BF0F253
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...a].%/....."#.D.....<.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....$..N.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..#.].%/....."#.D.d..<.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....i.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....].%/....."#.Dp....<.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....J4.....

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):	5.6572895384755695
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuq4/XtyhUDLYtmOZn1TK6ti:xRBJ54/RDcFZL
MD5:	6A42612B6E153DD4C92C77AB624FDC7C
SHA1:	23831E8C08108AFC6B84B15450DC897D3440C58E
SHA-256:	4D99EA4ADD1FF4468F05776F6A4376A076BD8A2DABDF33D448E7523C2066C513
SHA-512:	BE1827290E33F1E5DC4B168079514844AE94E1194F27388FA9C8F69D13B226F051B52C5CF8E2509CBAF8DEEE6DE95EA67FD168EC33F5E1B79485ED5DDDCAA9F
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..1.].%/....."#.D{.#..<.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.673181289325866
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7VdefYVPu1TK6trsRPYOFLvEWIa7zp7SARVPu1TK6tq/EsRm:BPHnYfYcaPHEicMrPHboN++RcS
MD5:	73305AB7302BD4B8478D95514C59DAE4
SHA1:	448CC0BC44E1B571C11EF740FDBBC2C716A799495
SHA-256:	9AB8D544F3CBE682A2EF5C5BB08CAEB04394B2287E7A5DBA14DD4D8E868AC556
SHA-512:	806E439A05F70F4AE0D9E57245220BAE940F65CD306551DD2D0DAC77152AD780A64DFD5180EF2BBFDEA406D270E8B7B1D41298ECFC90AAE42EFCABE9F9D2AC45
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...^].%/....."#.D....<.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....:..;.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....].%/....."#.Dx^S..<.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....>t.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .Q..].%/....."#.D.....<.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):	5.594079421597541
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVY25Aeps4XVAZ+8cV3vRm1TK5kf:mKPYOFLvEWdENU9Qj2ee9iM3Y1TK6t
MD5:	34024D9698E42A1E1ECEE2395914C561
SHA1:	F3D66FE323813A043F3373F73984612B0BE03979
SHA-256:	994C772DD945355E8C3F3C251099F7678A03AED3AD62DE8B2D09858529D9D122
SHA-512:	95C5972DE811B1627D6AE28F8EFF26C505F903491DB01CFD4DF92364716F81AEA4D7B8851C5F9FB93E70B6C445A881BFA41B07A13DD33A2B38D7D84FBB229A9D
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....].%/....."#.D$....<.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....jd4.....

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):	5.611433462340024
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQffk1QjBRCh/41TK6thgt:XRc94fk1QDi/E4t
MD5:	0B90E2AFAE74559EF3B07D2009AEEF0C
SHA1:	1069AD6F6617276FA293C36D00CFE9D15E4F4FBB
SHA-256:	7EDA4F947E1B1E2311AFF795458F1218838F81E4952EDC8B7A5BAE06375BDFAD
SHA-512:	F0745514472FC2744650C738A2BA189FD5E9CED1EFF748ED0FC057BAB99A203193D04299A1B5CA3AA88929831CE54C17FA50AD634502101EBCDAFEE8D2968DEA
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .mY.].%/....."#.Du.,..<.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....Q..M.....

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):	462
Entropy (8bit):	5.612111291310032
Encrypted:	false
SSDEEP:	12:bs6xRkiq8uM0LlF4nVhs6xRkionLlF4nZ:brxpDQoVhrxponoZ
MD5:	6877F57A822556D03B743FC8F1E56166
SHA1:	A1AF883DEF935E2A7B6ACE0B59EE2040C56E1C93
SHA-256:	95A3DCCCACD07E8D2AB9882FA6E47E4D3458CD3C50E15EB76F9F611F67555AE8
SHA-512:	41FB718DF8051C56C16A961A1C8FF6AC65E88CC47D0F046D733F7351661FA0CF5240965DA0EBA3E3CBD6644DFBE378B32389003E07BBBBC25477D3D1E501DC9
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .i.v].%/....."#.D..<..<.A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....<P.C.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....].%/..... "#.D.u...<.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....f.....

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):	5.501235112003061
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvH4PXB9Z9kfrcu1isLK5m1TK5kt7:mhYOFLvEWd/aFuq/B7Gw941TK6tjV
MD5:	987C414AE8973132FC89C616C804BCDA
SHA1:	BCFF1CA52FE83526DA4CBF4EB3E85AB4BF1862CE
SHA-256:	74C7D903DFDF8DC6F2EFF8EFAC8C6FEDC623B993E7E2AE04D5760889541FB8A1
SHA-512:	2C89E2996564DF85B53D7EE95F1414EE7528551CA0A1A3A9DCACDB2F92F2D0BF3526CB2B984C9C0F152033AB764942A2019CEDDCA4B40BA557908B5C7E0616D
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..H.].%/....."#.D{.$..<.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....k.a.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.529274736953949
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ/5v1oDw2oBMqVd3G4K41TK6t7:2DRuRcNUyB9Vd2k
MD5:	AA81F7C0F507C5E9FB838960C2A0874D
SHA1:	BD1E5077325E34C3AA176DE431DA20FFAB147F1B
SHA-256:	755FCCABF999CA45AAD2235CE25D189604F46B0E788E21F8EF6DCD3E4AB012C5
SHA-512:	3D5C525891B8EFF7257C060B8B33F1E803D1561DABD95941CC0AB8D6283EFE82F1A79242E5F64796DE8E323A05D718AB61507F29C36B6985C466C12EA8A4FDB
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....].%/....."#.D4.#..<.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. ....]..+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.629881707022122
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QP4eeRGtuA424r1TK6tAtMkqYOFLvEWd8CAd9QEpzgmuA42T:+RQP/Acrnmt8RQXdgZrnxRQXK1qrnB
MD5:	DC2BE45210B1F4702A7431EF81308C57
SHA1:	F6839D984D9A94ABED955E0E11C329F5EE10C139
SHA-256:	D2BF91233FBFB4EE5CFA6220164249291583 75F8DD8ACAA0743FCC56D05163F3
SHA-512:	3B22C666EBE420F25CDF276F01A71CC885E722EF1BF28DBD543746215F6E90AF2A8DD169446A62C5842B06893600223F871B52DA3211CD9197350083ECFA2EF9
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....].%/....."#.D..P..<.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... .....bu.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....].%/....."#.D;...<.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....].%/....."#.D..-..<.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo .....A..Eo.....*.O.....

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):	5.577999627407755
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuTTN6DAyC8n1TK6t:xhRTRTNh7Q
MD5:	4DFCC05F772EB8FDF7ED57AB266A20BC
SHA1:	76BD0AC2544EC33B722CB7D06618DAFFB7113B01
SHA-256:	8A0F3A76C395B4C757CF49AE286874CA0C5CAEC2258AE0AC6920A38CB78C335E
SHA-512:	DF50F532A47F82F3879C6D2033E7379C1D5D3C0368B692D9965AF01AF4FF06248E3FC00C5C123D41D9B894D3F0A68BC920FE73346307E08C61E3D3CAEF319BD
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ....].%/....."#.D\....<.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....Q..3 .....

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):	663
Entropy (8bit):	5.680431503192727
Encrypted:	false
SSDEEP:	12:nRrROk/VAX7+Vm5ItlRrROk/VxamOfRrROk/VEFm:nPJ/i7n5IPJ/LL+PJ/Kw
MD5:	74E10D5712FCE5FAF373CDDD356E1E4A
SHA1:	9E91C746DE9F507F37495F056B65780431AE967F
SHA-256:	E94CCA8EEB61B472597BAFA713587ED6E628A05B807D5C07E51B117E78514A30
SHA-512:	EB6F928C4470B5060A15B883AFD8D7D148245BA4422C882EEB3D24E356ECA11B561567E4ECE109122EA5EAD6B3E5DCDABF7EF424E6B84EC0C2D5604A056A17 F9
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .7Iv].%/....."#.D=.8..<.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....A.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....].%/....."#.D-x...<.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..H.].%/....."#.D.[...<.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):	5.574563992546808
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu+rdxAdm9741TK6tA:qxRcEjAdu7E
MD5:	D128DEBC01FA3D833B32E225117C56A6
SHA1:	8AA6C764AD899CABCC804B2238051A9B1DD3C468
SHA-256:	700848CBCD9B4C5627E6BA83107D36F39DC89AD95C5C148C8F8388CFACF4C282
SHA-512:	8ADDBDC4A1634E0A1294F33750170D5FB02F75DB52F84C4E2B8BF020815200C4D99C5D9350DC76A2BDE23EC6C88D313B15B4CEE0CEDC66019192E601370B7E5
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....].%/....."#.D^.$..<.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....p+.....

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):	5.5683273087969685
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvKXZiZB6shoq+Nem1TK5kt8tl:mMOYOFLvEWdwAPVugOkJn1TK6tU
MD5:	61983390686F65640FDF6167D19CC2B6
SHA1:	497C1739B7B8B4FB149623EBBF07C35943679DC6
SHA-256:	B0EAC93F9D2F58AA173F9FE104683AF8FCCDD480A9EE653B20C90DE6864E85F0
SHA-512:	3036FC364ACC70FC7FA2E7ACE5AD0643483F27EF91AC916603EBD6A65370875CDAD35DD90ABA1AC2D34E2B973BD868D710CCC3CB127D37C83971813BC336F6D
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .l..].%/....."#.D.....<.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.639301173461548
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQRXLzhcsBXIh1TK6t:mxRBJQiLDB0
MD5:	6FE2AC6CEF21641428D56F9CD3D102CD
SHA1:	06C98A9059E7F6ACE11FEC68632CCA42B6905800
SHA-256:	AB6E2A5014EA88C9978451F368ECDF157E42DDEE9DCDCCBD989F0E14F6D97E60
SHA-512:	812DFD75D1449BE7763C6EB255353FBFFCDFBE0202274177320B7672F716A2472941CDBD81F2A5561F036DD2CC6C4F8946D0A44B6A4C4370DBF350B394A80B1
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .;].].%/....."#.D~.$..<.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....). ?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	684
Entropy (8bit):	5.634529829650931
Encrypted:	false
SSDEEP:	12:3RrROk/sbDcvMcaRrROk/s235NecjlfRrROk/serMck:3PJ/aDWaPJ/f5N3JPJ/Tlk
MD5:	DEBECAEC9D4EEA1BF353CBB2DDB410AA

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
SHA1:	D9A3E83B9D41894A65D500BEBB8419B16D015426
SHA-256:	F41CDDCDC0CEA0B8AC0EF777CB45E1D7CDC583EAE9F5F3934C6DCDE1C52976D1
SHA-512:	80053694BDB077B2FF5866434D9BD38CD9A12B0712DEDBA7EF9533152748541BC90B7F303085239084B64B7E36E8629E935F7263BB7132083D1164C4E340CB4C
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..Pv].%/....."#.D..9..<.A....9Q].8O.z....=..:.N.{....N{. A..Eo.....A..Eo.....2.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .+..].%/....."#.D.... <.A....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....X.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-sele ct/js/plugin.js .{J.].%/....."#.D.....<.A....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....l..p.....

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):	5.214853352385442
Encrypted:	false
SSDEEP:	24:0l2bYdB8J6MbkeljKqRomvNA7tUDM0mhmpe8smw6l:t2kdhMkCqmvNA7G5ps6l
MD5:	00BB295B2129F5ABD121A738BC3F146A
SHA1:	9C6421F488656A35965AA110FF965E88838FC59A
SHA-256:	03F2409E0C35CF49A4F3BABA241840CCB4B01ADF0457D1A884C3D6EA298F76F1
SHA-512:	7BAB75829D5D742BA9E11315D3A02B5D9A4B8EC4E3029B8603B05FCEABF0D673DF161E7A4B4A2189270B258ED4D2EC4A1DC47F606FDAB4877A9A1BD84F9A3F 87
Malicious:	false
Preview:	.....goy retne....'.....'.....;.y~A.@.....*..@.....oB*.....#...(@.....k7A.@.....D.4.@.....[.i..%.@.....<...W..J..... ..,+...._.#@.....J..j...@.....6<|.....A?.2:..@.....+.{..'@.....*)....J:@.....2q....@.....P....V@.....+.U.!..V@.....P[. q@... .....!...0.o@.....u\]..q@.....@.....*....@.....o..k..@.....^.~..z.@.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@..... .....v...q..@.....C..M..@.....a.....~.,.4>.@.....&.S....@.....@..x.@.....=....m..@.....;/...@.....q.@.....MV3..@. .....:..N.A..@.....Z.....'1.oy 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):	291
Entropy (8bit):	5.173805976375338
Encrypted:	false
SSDEEP:	6:mgTbM+q2P92nKuAl9OmbnIFUtpTPXZmwPTPqMVkwO92nKuAl9OmbjLJ:jTbM+v4HAahFUtpTP/PTCMV5LHAaSJ
MD5:	A1B841FFD5C9976BFD96429A062299C9
SHA1:	CFB1DD9B0F3C758432037FBBF3FB4FB65391D676
SHA-256:	6A2BA8D83AB1478AE7D4EF4B1C68A09F3299D49C7D84880AA2FAAD5C769767CB
SHA-512:	52B672BB9A694BF78171523BE009D7AE0CFCA4F0412CAA93F765439D34FF7DCFE8134D40DB9E1CE06117ADD3B89C0ABFF574A7E1D16F780BA9ADA23D16D619 C4
Malicious:	false
Preview:	2021/07/16-16:38:16.001 46c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/07/16-16:38:16.002 46c Recovering log #3.2021/07/16-16:38:16.002 46c Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.0084423731585201
Encrypted:	false
SSDEEP:	24:T13rz13r+fUrjUVJjUVJjUVJjUVJjUVJjUVJjUVJ:T13/13KUvUvUvUvUvUvU
MD5:	20C2D53F3F6BF479288D699773FA372A
SHA1:	D18859D4EF1A2B4F96A6ACD1F09AB61AAAEB323A
SHA-256:	D6C5C9640C916DF6010AF982C733684606233C1632676FE69EA946B53C438E0F
SHA-512:	4A2A80FEAFDD414C93E701D268262C8F065DDFEC45211DA8A0A30762731DB0E7A21A44E9CEE09375C731C512652D5CFE20EE7821769E35AB95DF2563AB4493A 5
Malicious:	false
Preview:	VLnk.....?.....+.}.^1..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2107170127352-218.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	1.440007236641834
Encrypted:	false
SSDEEP:	384:w6vUcqyeXXKUmXyjXX9XrXXESXPbqvrXkuqkHuJdafA4:R1oo
MD5:	3084DB26F5CDEFA0A79BCE562600EC95
SHA1:	930E3A33550869DF7AB4510C947E7F61BB77E925
SHA-256:	58F5D44A7201116F4FA6CABD137A77CA8F88CFAF4AB918D803E51EEBB5FDE553
SHA-512:	11E7FB98CF0A0FB90461CB538C0BAB4F32D71D53A06963385918C0778D236C55BD61BAEEE22D0496BC5E25459C3F58C0FF8F3BA17673086E97213A198D61E0C
Malicious:	false
Preview:	BM.....6...(...u...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:	modified
Size (bytes):	32768
Entropy (8bit):	3.388850501981248
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQOOhFVCsL49IVXEBodRBkRWOOhAVCs749IVXEBodRBklWOOh+Y:iGedRB6edRB/edRBDedRBc
MD5:	9032E659D6A1B676197D6F919666B645
SHA1:	0BE77D58B9C811A8B0F2101D953B82F9CAE6C28C
SHA-256:	136057138C23255324BD8173234FB10934A05BE9A55A23FDE88A992EF9D380DD
SHA-512:	39FC349D7418A82D8CA4F53301D18A8A462633AB98CB32AC8993BA951DDA993742FC4DB516F5F3088C34BDB705CE097476B37E40E46C18022C5BD3D737A6800
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.2022612289364374
Encrypted:	false
SSDEEP:	96:m7OhFVCPh949IVXEBodRBkBOOhFVCsyLR49IVXEBodRBkKWOOhAVCsnd49IVXEB0:mdiedRBXLGedRBPCedRBXyedRB9
MD5:	93AB3D893E2B435B7BF85DD8768A632C
SHA1:	305E9273FB3EF7D62D4CEB5FC21D0FAE1AF8AF27
SHA-256:	AFB77F00097E52A6EC8A407D10A046CFFA4D80EE9F117DD18798C31F22E1E992
SHA-512:	3568D29732CD769AD73E3E57A60E3AF504083658CA000714022F86CB794F0D7489353F1D3FE632C180644E9DBFDF2D65CA5FED0960E27B8654DD2BC7CA33B86
Malicious:	false
Preview:	.....D..... .....X.. .h...y..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.304248760879033
Encrypted:	false
SSDEEP:	48:panitqAtg0KUNFeYnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWAtXKokTz1+boavLJpu5
MD5:	202F2D29B3E8C798A335CDBFA528CA26
SHA1:	27CCBD68F9EBEA6D255967A47EDC59196A31C85F
SHA-256:	03BF005BA66C5693387352136F127279DF5858255D016ABCBF90D7849573BCDB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
SHA-512:	1A2CB656B02EE0008C071F1F16C7A774EE0C522A279680FE82C52264B94CDA60242D6F042695655A06B8E11CA86F57F476FB509DCF38549CAF223ED078D5C0E7
Malicious:	false
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20210715193819Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20210715193819Z....20210717073819Z0...*.H.....M..".o...M..6.k.n~.X;.....q..f.3..3..1.a....`..e=!@-..:.O.*....C(.d.....t:...6...3...@...x...._..a...8...Q.)=...".`#8....u.,bn.=..s....;..2.eJ.X.Aw...F..^J.dEp... .].A.g.F.....c..QwIQ....c$.hF2,..Vn.G..E.f.0ly..C.....!....Z.6.r...3m.&...HV....0...0...0..g.....f...p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..210909070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20.."0...*.H.....0.....'.....^Y.u..U.qU..."......-]XG(qk#.+....J...G.3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	183060
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGbrec7VDBGm
MD5:	7DAFFD77F2D6E43937A4AF91891D572A
SHA1:	B00718D20556FAB59D4F815460CE0E657707B125
SHA-256:	D9A5468356659DD4E681FBBEC4EBFECDE08400FC5432BAF92553813A62336A3D
SHA-512:	7E8C0EA36B41D44B914D409F9FD2B1E8BB0F0BD617670E274452E7CF56E61CEC68CC550BA817D9654B6F5C85A0135C45B5ECECC73E61EA0A4D2642D89723198
Malicious:	false
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t.z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.`=*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.304665468482358
Encrypted:	false
SSDEEP:	48:snitqJSTXORuVnitqsXA49e5REMeZ6+23wQ:UJmtsw49eEMeZ6+Y
MD5:	9A74E06FED8E6D15EC1C4C67C8E1DEB1
SHA1:	061DD4B990C802C096FB57099054A9C935D7A2EC
SHA-256:	91A83F6E51E8C00851757C6740427E13B9BEB3B11F9AEBBC1F9C834F51112912
SHA-512:	415B8A9B87B1A39C734368C8A03378E745934E7240016877513A40B613B787E8EA1A7791B877DD2EE3EBEC2E40441BD8811303EF032F2B48B006683BE46C24D2
Malicious:	false
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G1..20210716014216Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....20210716014216Z....20210717134216Z0...*.H.....|.....b.....\b....Y....A..d.U.xk..[.a.b ..X...Y.....S-Z_..)W..C...]..9..A..B.....!..\t.z..PrC.@Gr..a3^._1V.D..{....|.R.....8.|.X..~.~ S..2...!j...S.B.....V...p.;...I.....g.|!R.q-.~'..2(r)2....Z.....6MKj.....D..8. ..-.....b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c....'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.778031175513724
Encrypted:	false
SSDEEP:	12:5368rQESIgsFFV13Mz1mySGqWvXQj39lJ8rQESIgsFFV13Mz1mySGqWvXQB:FTwyPV13MhmyFqWK98wyPV13MhmyFqW0
MD5:	4A8492564EB9177B57673FF0BAC4CBF4
SHA1:	22067D689345A76296F626FC05723DF4C6D9711B
SHA-256:	60D3C81F304E7C5CD5BE04996AC829D1B535F65E52EFE1B02CF45D7C2A784307
SHA-512:	BB0FBB1ED5FFE6F47B62A4C6D32144A79460BDFFCEBBF1DDFF9D5CB6AF8906EF5B9111C65571B9260E35495DA6E7EA47A0C8BFB8E4645B3E43F8F0CE331E2F70
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Preview:	p..... .....5E..z..(..... .....y.....V.....h.t.t.p.:.//./.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".2.7.c.c.b.d.6.8.f.9.e.b.e.a.6.d.2.5.5.9.6.7.a.4.7.e.d.c.5.9.1.9.6.a.3.1.c.8.5.f."...p..... .....5E..z..(.....y....D..z.....D..z.. .....y.....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".2.7.c.c.b.d.6.8.f.9.e.b.e.a.6.d.2.5.5.9.6.7.a.4.7.e.d.c.5.9.1.9.6.a.3.1.c.8.5.f."...

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):	978
Entropy (8bit):	3.1474961458003774
Encrypted:	false
SSDEEP:	12:C5kPlE99SNxAhUe0eI5kPlE99SNxAhUe0en05kPlE99SNxAhUe0et:C5kPcUQUfeI5kPcUQUfe05kPcUQUfet
MD5:	11B320858A3C92EE1E947B5D79276806
SHA1:	660A2058637A191AE9EA6002B8B1A0B4EA6AE60D
SHA-256:	BBBF3F47A51F73D59491E4562E06A07C90D21090E6BBC716D84FEA63659BA18A
SHA-512:	5D2BC15E52BF609D12CEC647BC86B2E95528D5155BB2B500C3D8FD5B345AB24E240943AD4A960E448929CFD92D6D6713D0CDEC7840F072EBBF35AA8BE00047C
Malicious:	false
Preview:	p..... ..... 7.z..(..... .....T'._.....$.....\...h.t.t.p.:.//./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....6G7.z..(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....F..z..(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	3.7442787132937903
Encrypted:	false
SSDEEP:	12:uOcj+rQEFDsFrvgxE0P6GANMmZ0jrrL+rQEFDsFrvgxE0P6GANMmZB:uOXV4xaVSGAmmZ0jXSV4xaVSGAmmZB
MD5:	875D72A1C0E024930A288372F090DC58
SHA1:	4D66592032EC9CC14675975C2927052695A89482
SHA-256:	CA0DDBEB71E9B13F103ED41C5E46D2DA2D0468BCAFF497C516DA7AA73A92CD82
SHA-512:	4975524917EF90ABC8EC50F990168438B06899ECF7A088EC76B8B97374D7BFDE28BEE640F92DEFC3F698A096C3BF5BF491E0BC17EDD0E3AFDF29B9CEE4924CE8
Malicious:	false
Preview:	p..... .....=..z..(..... .....y.....V.....h.t.t.p.:.//./.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.I.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".0.6.1.d.d.4.b.9.9.0.c.8.0.2.c.0.9.6.f.b.5.7.0.9.9.0.5.4.a.9.c.9.3.5.d.7.a.2.e.c."...p..... .....=..z..(.....y...l"..{.....l"..{.. .....y.....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.I.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".0.6.1.d.d.4.b.9.9.0.c.8.0.2.c.0.9.6.f.b.5.7.0.9.9.0.5.4.a.9.c.9.3.5.d.7.a.2.e.c."...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZsNSjIXKkMan2T/rPINA/MsuENYyu:J0GpiyVFiBswjIXKkMuI/rg5SK
MD5:	AFF35D42BBE7B71FE5941DA59BE223AB
SHA1:	916A2740D369BCBA1BDB26EBCD08298924EDACFC
SHA-256:	4ED10091C6A36EA520CD1FE5C6CDB16C31DEF8958B58126C34479F94908023B8
SHA-512:	97C483D140F5496714C8E55932C5D9AE3356BABC0D2418771AF2A9B1CCC321583523B740336EB63D5363A8C19F197D70648E14FA883E76C94D4584C384F4FF2A
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:AIgerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Google\Chrome\User Data\039a6783-f6d0-40e0-80b4-8b3cf82f54a6.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):	364342
Entropy (8bit):	6.015258461027268
Encrypted:	false
SSDEEP:	6144:tgHbsLZIdF21L48Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBs:y7a6F21BxzurRDn9nfNxF4ijZVtilBs
MD5:	3389E1967B9A02DDC0A16B8F5068CF80
SHA1:	3488BCC95270710A891C087579709ABE25C8A0EF
SHA-256:	7AC17BEF2F678212D965C02FBE095A8EA10BC11A02CEE549826AAACFA237C354
SHA-512:	2C4D9C828ECEF1BED593EAFB9FA0E2E8D6BECB3CA66CF7479A0296920FC914890956085A8A057DABCF4ABAA6E26D0ED57BE25650A7E5E92276252319A39365BA
Malicious:	false
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":1.626478767897632e+12,"network":1.626446368e+12,"ticks":6754138896.0,"uncertainty":2697373.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327095236564

C:\Users\user\AppData\Local\Google\Chrome\User Data\15ab1e42-1b9d-47fd-a6d5-6d21c46b0116.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):	367926
Entropy (8bit):	6.0277259258771805
Encrypted:	false
SSDEEP:	6144:/gHbsLZIdF21L48Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBs:o7a6F21BxzurRDn9nfNxF4ijZVtilBs
MD5:	2D20808D31638C30668F942F6DA2D794
SHA1:	378678507DEDD0CCFCBE431E5993F31573C1CC9B
SHA-256:	AF849D9C3AAC81DF033F6D82DA65B2E8C020858E0EFCFDA5A3ECB9979502A10F
SHA-512:	C216D99B75966AF48E0A351024C8E3F5AC82395AD13C918F559C7C51074E192285B621F3CE3CCE3465C496E01FC292EC2C22D1BA3F1EF75EE6D5E05CE29AB9
Malicious:	false
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":1.626478767897632e+12,"network":1.626446368e+12,"ticks":6754138896.0,"uncertainty":2697373.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075757673"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\24f81939-edbe-490f-b63d-4f96e8757db5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7516032324174002
Encrypted:	false
SSDEEP:	384:Hjfe1Bf4WLjM54NZryvdn3GJjiHz6Gq9rIbxpxWrvTursBmc/43JJh2OH/JNM1xJ:m2Bt2v2eke3BLLIfTCHKh39Fm
MD5:	F7B78AC5A34A5F80288A0B6EF11C0442
SHA1:	B5151B632B740182CB78C404E0E8760CB4AF119B
SHA-256:	8FA89949D9764F9A2D068DAA4884C7C8E687DF10E92DE591B0BD230AA2955290
SHA-512:	85EA39CAAECF4F414983C0BB7140DE5A8C6BA96736900A7AB7F5DB5D56C7A9C3393A01DDD8C2A88EFE22E78B84E63F168C863509E091DCA8595475B83A95B3E1
Malicious:	false
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\3a08b007-379e-4ed7-90f0-fd256b03f394.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\3a08b007-379e-4ed7-90f0-fd256b03f394.tmp	
Size (bytes):	368010
Entropy (8bit):	6.027845073772459
Encrypted:	false
SSDEEP:	6144:5gHbsLZIdF21L48Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBs:+7a6F21BxzurRDn9nfNxF4ijZVtilBs
MD5:	E228AD0CBF5CBC5F0A265958B24778C0
SHA1:	5F99452EEF5214BAA521CEAF64B85795C42E6E8A
SHA-256:	39AE0CD591B99864F492FE40F7C2EBC235D1277DC6C9F5C261F62E1E11E2AE85
SHA-512:	E4E5177F49EF8C1C10055CECE058551167FAF760CAC050B7436B20658809DE89AE00FF96744A4E24F7BA4137FCEBA8E9B71B09C54C252D7D5EDFD772AF1A0B9 4
Malicious:	false
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":1.626478767897632e+12,"network":1.626446368e+12,"ticks":6754138896.0,"uncertainty":2697373.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075757673"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\504ae7d7-22d1-4168-8a98-6c19f512bf6b.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):	364341
Entropy (8bit):	6.015258531472639
Encrypted:	false
SSDEEP:	6144:9gHbsLZIdF21L48Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBs:C7a6F21BxzurRDn9nfNxF4ijZVtilBs
MD5:	C92EB9546680367BF4D9348A54476D3C
SHA1:	6681B8B60DE518B5C659772BF600AE150C072C12
SHA-256:	DD0AAAF502718AB256594F88FEA7F7A447B8BA3E25CF93EAA79915525F23B83C
SHA-512:	3B9E9464A6595A60B1B992314ABCEB42F5A62D506828DAAE110ED16F4F4BBD055AF649F2753985517A664991CBCA761F52C5DF3382E1831FE6323F6F8A4E402C
Malicious:	false
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":1.626478767897632e+12,"network":1.626446368e+12,"ticks":6754138896.0,"uncertainty":2697373.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327095236564

C:\Users\user\AppData\Local\Google\Chrome\User Data\5fabf9fe-7ebd-4194-8b22-5a4c1c1f595c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7518450859757655
Encrypted:	false
SSDEEP:	384:Bjfe1Bf4W/gjLVkq54NZryvdn3GJjiHz6Gq9rIbxpxWrvTursBmcIa43JJh2OH/H:de2Bt2vseke3BLLIfTCHKh39Ff
MD5:	B1ECC2EDABCC2766E02EB6D69B80B19A
SHA1:	04B40BB19B2015F404F931AB825838C311A1A2CB
SHA-256:	46A2801512276330693E485D9D6F3F87F63DCA6AC13A72620DFCC7F63C5565A8
SHA-512:	5B40C45133FED96DD59BE05949987ED820A00172F22E30B3091173CA37E9FF5DE490A1328226985D7C64D74A843BADBD6E23D94F567E6287CCB69DD7833267A
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....?8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d2bedab-e802-4292-bf14-c909a907efa7.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):	364342
Entropy (8bit):	6.015258217565408
Encrypted:	false
SSDEEP:	6144:9gHbsLZIdF21L48Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBs:C7a6F21BxzurRDn9nfNxF4ijZVtilBs

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d2bedab-e802-4292-bf14-c909a907efa7.tmp	
MD5:	51D4D0A7843BA78B0DB94C082CB8F8C7
SHA1:	50DE2EB3F4A8580864E29627926AC9281754323D
SHA-256:	501F4BF926801E0586AF8C02EFA6718336A1C1D9FC4FB6E6E6D640A888FA2310
SHA-512:	27618F0F47111E6B68B1B651EA06B0BD1411B99AE7B463EEC84B0C06B6C1B872AE442D36E75C6E8396E8CACCD071A810E61C8BA37815B8937AC5D9A757467E8 2
Malicious:	false
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":1.626478767897632e+12,"network":1.626446368e+12,"ticks":6754138896.0,"uncertainty":2697373.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075757673"},"policy":{"last_statistics_update":"1327095236564

C:\Users\user\AppData\Local\Google\Chrome\User Data\8de20485-ffbd-4b25-ab0b-62997c7ae843.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.752323312286085
Encrypted:	false
SSDEEP:	384:xjfe1Bf4W/gjLVkq54NZryvdn3GJjiHz6Gq9rIbxpxWrvTursBmc/43JJh2OH/Jb:Ne2Bt2v2eke3BLLIfTCHKh39FJ
MD5:	207C05405D62B92B349A7CD513054008
SHA1:	2035783D9FA89240326A404930433E9160577F41
SHA-256:	B40665B72C0144C58DA0BD32785761E484F126B147AB453396AF1DC6C01440E6
SHA-512:	23B9F500F290EFE36264B751C0E6D1A1016B8A332BA4464E375325885BBADD9898C03457904F3671C346F06F3512FCC53C8DA6D952661433C42333F74304E23D
Malicious:	false
Preview:	.q.....*...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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04b39dac-68e4-4b5f-87f8-38d43207136b.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):	1710
Entropy (8bit):	5.563236357814097
Encrypted:	false
SSDEEP:	48:YQaU4Q6UUhrwUk/gUkNDKUeuGEdUEUoUrUeCgpwUbUeh:QU4ZUUyUkYUUDKU7dU7oUrUHgqUbUc
MD5:	63C8169B62F1D8117E623FF8426BA3DE
SHA1:	1E6E6750F17EC3C0B95B241B1454148BAD3D5FDE
SHA-256:	0D1649C448F0C9F88DAE6555CFFCDF407DF1283C598808517B332676FC14AA01
SHA-512:	33D6B0834D22D2B08ABC89CAE40EF1B661A1D7C22C0692E425CA59189622470F380FE0A9656FE05F6589420D0DBB81ECA66D69868732CBF19C9B3422DA5914E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04b39dac-68e4-4b5f-87f8-38d43207136b.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478771.354716},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658014803.213169,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478803.213175},{"expiry":1658014769.098694,"host":"avI6i3zd7b3vW8lj9ClOwYk+RSTKrstFmJ6VHx5gYrI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478769.098702},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1626565233.441218,"host":"yHr6+fG7cib6pk4E9Q3y3Xbu14sGfVO0fAjZ+dCCQg0=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\060b1c6b-fc0a-438c-9009-eaff5c628800.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12f78126-a422-4f21-b413-1d14830fdaa6.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):	2211
Entropy (8bit):	5.570191687689346
Encrypted:	false
SSDEEP:	48:YQaU4Q6UUhrwUkjjUnbAUdgUkNDKUe8wU20Ub0UoU7UeCgpwUbUeh:QU4ZUUyUkfU8USUUDKUwU3UbLoU7UHgN
MD5:	D45A37D7E26BF82D880D5B5A3C5072F2
SHA1:	82ACD427906205D579EBEA73C6076787C5EAFAC4
SHA-256:	2245678D026DBBC47474BDDFBF9DAA105A1EF477FE545100894A497C2273F59B
SHA-512:	4548029EE05DBCAAA1100D2ECEB65D6C8D14B731CB98594C437ED12DF3E8F4BAFB426C9DE808C26861AA09984032C7582EAAA6154EC4202B6A667023F7B33E0
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478771.354716},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658014803.213169,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478803.213175},{"expiry":1658014865.343747,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478865.343752},{"expiry":1658014864.894378,"host":"YuJ8GecMGWmVSo9vXGXsc5KAROjJs5y8X2yABohamr4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478864.894383},{"expiry":1658014769.098694,"host":"avI6i3zd7b3vW8lj9ClOwYk+RSTKrstFmJ6VHx5gYrI=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1a1e459d-a967-46dc-897d-fd7305c61dc1.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\23c084fc-bcf8-4f02-bf19-2bbc9c088ac4.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):	2379
Entropy (8bit):	5.571294112202221
Encrypted:	false
SSDEEP:	48:YQaU4Q6UUhrwUkjjUnbAUdgUkNDKUe8wU2CrUFvwU6SUoU7UeCgpwUbUeh:QU4ZUUyUkfU8USUUDKUwUBUWU6NoU7UU
MD5:	F8AF76A9DF800B6F9736D0E406836828
SHA1:	DE07751DA27890768B273D82A9824F269AB469DC
SHA-256:	34AFFC67DD3F801D0F355CB76E6F156FF59F28312C3C03443362EF98092BC68D
SHA-512:	19C453FEC8FAEACB513E21382767C6350FE5F150D92C8A912BFE27C202258683772830CB9FE0757E505360AB683ED0DD755A442FB081B3FCDAB6A7B8A2ACDD 7
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478771.354716},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658014803.213169,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478803.213175},{"expiry":1658014865.343747,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478865.343752},{"expiry":1658014864.894378,"host":"YuJ8GecMGWmVSo9vXGXsc5KAROjJs5y8X2yABohamr4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478864.894383},{"expiry":1658014769.098694,"host":"avI6i3zd7b3vW8lj9ClOwYk+RSTKrstFmJ6VHx5gYrI=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2e7676b1-acb5-4368-a098-b2f84c227168.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):	2837
Entropy (8bit):	4.858788685785592
Encrypted:	false
SSDEEP:	48:Y2ntwTCXDHz5sXRLscTsGrrshMsIMHKsciyvOsW3zsrAkq6qm6K2XZ7NiYhbxD:JnOTCXDHzAfXrshsGei+Ihjxm67XZ7Nn
MD5:	4E0F296839DE4134B75579E59FE3196E
SHA1:	18D6932059FC3941D4E05426614DE8ECE42E58D6
SHA-256:	38358C460A8502619EDA1DE7A5E337F913C8536ABE6713AC7CC3D42C02F42061
SHA-512:	04CFB4293C9FECD751772FED81DD997CB12B59A93A2D87BA2DD451889A77E488B912CE6279ED30E8D6EB933768B052E507BED21017D3505DC43672B1BBED00 8
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273544368598000","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273544368620762","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4307a062-8872-4482-a81f-1d02927d294a.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):	2323
Entropy (8bit):	4.856330737775205
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zsXRLscTsGrrs4sOkqMs86XZ7UYhbxD:JnxOTCXDH+zMGfXrsOjo6XZ7lhVD
MD5:	0D481074465523B8C428E7C8F64D5EDD
SHA1:	656F6CE10973976BC4BC23C0BB32832626C6EE41
SHA-256:	630284F6E592CB618DFB5C797E90BF452B47AFFE0077DC27FE1795C42236FB9D
SHA-512:	C6F866B69DA2ADF8EBE7521E799414CF1BD7AE8ED2B439A1208F17F400DC0E315EFF3A32DE0E0F32950AAEF2EFD9F50A0A172AA2CFEE083633396E1E963D40 CD
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273544368598000","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternati

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\435970f7-28d0-4441-a6ad-ba452ba17d7a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\435970f7-28d0-4441-a6ad-ba452ba17d7a.tmp	
Size (bytes):	5718
Entropy (8bit):	5.187164507016659
Encrypted:	false
SSDEEP:	96:nZrfs5Ms/SKICRDIk0JCKL84kP11XAbOTQVuwn:nZrMMmS8dC4KtkPy
MD5:	E75B795F73D7C14454B260C20886F20F
SHA1:	27EC8921CDE296F9F1483EFDC4D97EE952502244
SHA-256:	4CC02F160FDECB3E38F6CA32569E82397F76A1077C86829BAAE3176417C72661
SHA-512:	C866D5327890FF695293E561C011E6F9AF83DEEB85CE739130566BED8CB9E1421C4AB4A018009CC356F8EEDD94D0B5818211B55DDE7E80B2B61B9E79E8EFAB 3
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270952366235342","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5009922b-7845-4aeb-b685-0433f5c50ae7.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):	3882
Entropy (8bit):	5.586928408943983
Encrypted:	false
SSDEEP:	96:QU49eUUieUogUSUU7UnUAU4UsUjjUBDKUh2UihUvUWU6RU7hUEloULBiUQPUHgqk:QUYeUEUlUSUU7UnUAU4UsUjjUBDKUoU1
MD5:	81BA60005E056AAA8EAC510F335B54F3
SHA1:	BB12F5B80D5E6E414DDCE6A5DA7A4B069FF05BE0
SHA-256:	D0E506EF1652957BAF89D6E816CA9C0D04AEC1DA787D8EDCA0E18AD9826AE4FA
SHA-512:	48FD0428D2AFA3C019C25EFF98BEBD844E4257905AF200AA2279C09FA7C71BA22618DC4C6D22183630817D0363E9099DFBBBBA2EC758C848C9BB5B5329422A2 E
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478771.354716},{"expiry":1637365359.544711,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478959.544719},{"expiry":1658014958.778805,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478958.778812},{"expiry":1658014959.160691,"host":"M8FCPDx/iztAurBHj5rqTMZrfy6572JZu9VqQVWm2Dc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478959.160698},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658014958.806147,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\53e67d93-8196-4ab4-b4c2-e08bf6328ca0.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):	5122
Entropy (8bit):	4.97165218024737
Encrypted:	false
SSDEEP:	96:nZrcl5MpSKICRhIk0JCKL84kP11XAbOTQVuwn:nZrKMpS8/C4KtkPy
MD5:	B3881D33110D5D120CFEB194A753690A
SHA1:	F8B630AAB33FF42780CFDFEB85A6AEC69E61487C
SHA-256:	CDC86ADCC5FCADC489E2277CAEE33209A7740BA187BF202130687496E2D58D3A
SHA-512:	B3DB8D5C56218130C933BECAB4945E5FD2B9493D5D9BF011702516B60105A290E92F5C421E4C52995458EDD43C0A1F77C7C1301529249CB9531365CC1D8BE56
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270952366235342","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\56a8493e-81b2-4f1e-a241-f71f69d4e7b7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	18940
Entropy (8bit):	5.568857279599955
Encrypted:	false
SSDEEP:	384:xJotaLlNLXM1kXqKf/pUZNCgVLH2HfDNrU1XUHG8VzYaJ4+:dLlpM1kXqKf/pUZNCgVLH2HfZrUCGqln

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\56a8493e-81b2-4f1e-a241-f71f69d4e7b7.tmp	
MD5:	5AFD70F9C88F2813F4EC11002325EF58
SHA1:	75F42EAAC2F9D8C196B9A34B0F449D6830486F4E
SHA-256:	EAC62BE401CF95329C51AA265BD73C76AE7BB3FB8EB48B80737F13FDCC4C938E
SHA-512:	C9A58D876587D543C5F7D03CABD88E8306FEECFE64AC0C58E88D78159AC7D0A0FAA64C2B8BFFE7FA94EE2F3191226C4DB164477C82886210658B79B3C820993 0
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13270952365760680","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7483e886-0bdf-4ae8-bc97-1cdaeaae2bee.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):	2379
Entropy (8bit):	5.571380939619547
Encrypted:	false
SSDEEP:	48:YQaU4Q6UUhrwUkjjUnbAUdgUkNDKUe8wU2dUrvwU6SUoU7UeCgpwUbUeh:QU4ZUUyUkfU8USUUDKUwUWUcU6NoU7UU
MD5:	A32E277CD1D061ABD8C09E93083BD718
SHA1:	BF05E4D6C3C4C68A97CE66EBF93FE48AA02B1BAB
SHA-256:	2A1A9B931067F1DED7B8E3D116B1B2658FEB6342327BC69121FEEA61C90F1694
SHA-512:	D053FB6C93208DBE3341A2C1A36AB432F1613FFD6E12ED189DB06A790BDEA6228A638509A99967AC9BDA0B8DEC7CDBA1E9B94A19A5B2CE35E3067374D3652C 13
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts _observed":1626478771.354716},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subd omains":true,"sts_observed":1601477028.822838},{"expiry":1658014803.213169,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https", "sts_include_subdomains":true,"sts_observed":1626478803.213175},{"expiry":1658014865.343747,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnX wn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478865.343752},{"expiry":1658014864.894378,"host":"YuJ8GecMGWmVSo9vXGXsc5K AROjJs5y8X2yABohamr4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626478864.894383},{"expiry":1658014769.098694,"host":"avI6i3 zd7b3vW8lj9ClOwYk+RSTKrstFmJ6VHx5gYrI=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80498f5b-7cfb-403a-8070-013b8a06c7ba.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):	1710
Entropy (8bit):	5.563635920380592
Encrypted:	false
SSDEEP:	48:YQaU4Q6UUhrwUk/gUkNDKUeu4DUn+UoUrUeCgpwUbUeh:QU4ZUUyUkYUUDKUGUZoUrUHgqUbUc
MD5:	BE0EE760F6DABD2369C7946A9B29609E
SHA1:	306AB6926E84B43252EF27435C62DD9369EC663A
SHA-256:	6E3569327878CFE0D665CEE62503FE53D74E5176DC9AD5DE6DFB5962EC544FBA
SHA-512:	0A6A9AD93CB17020E998E937B66FB5F8FEA3895FE9BD991C71CA29BE683C0AF4AD148D41F432EBF3489D07E3463D06F7ED81635B1509A7E92420E63466C6BC3
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658014771.354711,"host":"BTtEjYMbtYABz8gwxxxVqV8ObprI35xLPv9i6s2tyw4=","mode":"force-https","sts_include_subdomains":true,"sts _observed":1626478771.354716},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subd omains":true,"sts_observed":1601477028.822838},{"expiry":1658014803.213169,"host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","mode":"force-https", "sts_include_subdomains":true,"sts_observed":1626478803.213175},{"expiry":1658014769.098694,"host":"avI6i3zd7b3vW8lj9ClOwYk+RSTKrstFmJ6VHx5gYrI=","mod e":"force-https","sts_include_subdomains":true,"sts_observed":1626478769.098702},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm 38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1626565203.273462,"host":"yHr6+fG7cib6pk4 E9Q3y3Xbu14sGfVO0fAjZ+dCCQg0=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9cba95a4-1b9c-428b-9534-2c070e04d38d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536081263927109
Encrypted:	false
SSDEEP:	384:xJotHLlNLXM1kXqKf/pUZNCgVLH2HfDNrUvXUHGANTnTpzY+J45:OLlpM1kXqKf/pUZNCgVLH2HfZrUQGANE
MD5:	59F2051BF7ECB010ADE9B5519F6A791B
SHA1:	B0FB1155257FDCFFC4CC0BE50DC3665F6BE3A86F
SHA-256:	CAAA3A358FDDE9E039AA5965B01B8CA7F0D5BEDD6A8A7AE46E2CAD42C68B4333

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9cba95a4-1b9c-428b-9534-2c070e04d38d.tmp	
SHA-512:	466DB33E00D5D437FB3A5849DA6B762D70E4901411486F662F2E8E59EE1EF6FDFF6DE8B08C9325B6A6E29AE4A55CFA1265B83256771D902BFC4ED2EC79519AD5
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13270952365760680","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9e8324a4-d448-4cc1-83a9-d2829a019220.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535985506484641
Encrypted:	false
SSDEEP:	384:xJotHLlNLXM1kXqKf/pUZNCgVLH2HfDNrUvXUHGJNTnTpzYHJ4jd:OLlpM1kXqKf/pUZNCgVLH2HfZrUQGJNX
MD5:	92250A9F79F6B33CAD8879EA979177E6
SHA1:	777A0AF8565A2DE03A788AD1ADC9D961ECA655ED
SHA-256:	E05671278141439D0D99C701E9DF806BCD32EFB294C9B36C5590129E0D740410
SHA-512:	50A1EFCAAD17A0587CD6784100B1EEAD3D370D2826634335BE019CFE69B9AD5CDAE337EC032BA0B12822540491F160FFBA73D28E76842F271FDFAC78F3EF84F
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13270952365760680","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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):	336
Entropy (8bit):	5.26098963200569
Encrypted:	false
SSDEEP:	6:mnU7jyq2P923iKKdK9RXXTZIFUtpV1ZmwPQmlRkwO923iKKdK9RXX5LJ:P7jyv45Kk7XT2FUtp3/PJR5L5Kk7XVJ
MD5:	00D4EECF2D5B6EEC192EFD1E51CE2871
SHA1:	DE3D13961510E44FBCD063D1287706817DC8AF74
SHA-256:	D6D4807270ECF7FB4D5B2C09FA53C8F0EEC488B2422C1C0BBF68606808BD4A48
SHA-512:	9B83FA43CA063B78D3E15A0DD16A1357D4DADCDE46D3678709D7EFB81B642AEA450A29F9F1408F92C6CD0E7AEF43A6FF8DF8203607824A65D798EEAF81B806E
Malicious:	false
Preview:	2021/07/16-16:39:35.949 1374 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/16-16:39:35.989 1374 Recovering log #3.2021/07/16-16:39:35.990 1374 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):	320
Entropy (8bit):	5.2471151443130095
Encrypted:	false
SSDEEP:	6:mR3yq2P923iKKdKyDZIFUtpt1ZmwP7lRkwO923iKKdKyJLJ:Qyv45Kk02FUtp//PxR5L5KkWJ
MD5:	C5FAE99B61BD3445058AA79E1F9ACF01
SHA1:	B8947CB8A716F8213DC946F63637DB4215C0FF6A
SHA-256:	0551E11BE953A54A1B1BBD87E6C520491324D354F23EC787795A25312D97156F
SHA-512:	22D95D66BA69543A23FF2578DB6FC8960A50055A63FD74BF90D524421B0670B63776A17F975965DA9F8F308922F804F3660A50F514BD32A2F4F0814296B41B3C
Malicious:	false
Preview:	2021/07/16-16:39:35.908 1374 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/16-16:39:35.909 1374 Recovering log #3.2021/07/16-16:39:35.910 1374 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\0396d3d509d4a2cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9197
Entropy (8bit):	5.568120614574528
Encrypted:	false
SSDEEP:	192:pr7DluBlMxi4tplEiqixrl58ipQYJeMxu/p0GYt:p/hpD5cYoVyGk
MD5:	48F528B1892798C017D2386DB088AFF6
SHA1:	1042B804A53A3C6C8C295E37BC8CED1AC3819D24
SHA-256:	62999417B75203C2D63DA7393238F56430DB1D9D8B7BB3E62C09216754402456
SHA-512:	C9D3D10C1DC1B46B83F763011F34CECC75C4B0B99D4CCD3CBD7A10E35C7673BB5B814D62894C726CA4FC84D488C94C1893A06828875630BDE04D68C3C6058B
Malicious:	false
Preview:	0\r..m.....]..........._keyhttps://service.force.com/embeddedservice/5.0/utils/inert.min.js .https://salesforce.com/eLml.%/.....tW.....O.5....OT....N...c.T...ZTw.P..A..Eo.....x.....A..Eo.....'.f ....O....h"...Hqa.....(S.<..`2.....L`.....(S.\.`t.....L`.....Q.@"..H....exports...Q.@.....module....Q.@.....define....Qb.....amd...Qc.....inert.....K`....Dq.....s.....s...\...'...s.....&.(.....&...&.^.....\.....(Rc.....I`....Da.....@...P.....@.-....LP.!.....@...https://service.force.com/embeddedservice/5.0/utils/inert.min.jsa.....D`....D`*...D`.....`v...&...&....&.(S..`>....`L`,....pRc4.....Qbj.D.....e.....Qb.(g.....f.....Qb.i.....k.....Qb.....l.....Qb*.g.....m.....Qb.....h.....Qb.Z&.....p.....Qb.3.....q.....Qb2Ci;....r...h.....I`....Da,....@...(S.....Ia....6.....1.....d.....(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\093e8d39c8dba529_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92528
Entropy (8bit):	5.660709883914733
Encrypted:	false
SSDEEP:	1536:qfjKK5W7ftB42PKJhE/MXcsq8EMPI3+WeCrsa6:mfYDt+2yc9svZQ6
MD5:	7F0ACCADA97E56D1067C105BA0CC2C2A
SHA1:	5368EB1CBD50814DE5EFE3206F0B72B91F6EADD0
SHA-256:	0044B8DECE5671B9E19952C3030AC147B7F44C5576A1F64B43170B95804354D2
SHA-512:	5FFCE993B37133B8EF8D8380BCCA8290E81C350D2EC95C880AA64BF51A0155CA6535E06A634276FF7CC80B15E9D1E701295DDE148F10940D5EC11A8800CCB6B7
Malicious:	false
Preview:	0\r..m.....@.....8A7EB8912CA07CFF16A55D77F2D4C0DA81E8E1B9BF8E2080C149BEFF0BAE9540.....'.....O.... h....P.....(....?.....d.....x.....(S....?..`.}.....L`.....$L`..... Qf>.....generateURLSignature.(S.....la....y.... ..e.....*.....(.g.....2.....@.l,.....5p.....e.....d.....$QgF.8.....initializeTeaserLoader..E.@.-.....P.A.....https://www.salesforce.com/etc.clientlibs/cq/personalization/clientlib/personalization/kernel.min.015ac4f9d569ca6cc01b4c370c725560.js...a.....D`....D`....D`.....`....&...&.(S.(.`.....L`.....(S.....lab...f...IE...,d.....K`....Dd.....(Rc.....I`....Da.....a.....d..... .....&...%&.(S.U...`d.....L`j....dRc.....Qc2c u....mapping...Qd..!...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ab3e4edf4747545_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.954546955426353
Encrypted:	false
SSDEEP:	6:mkkYGLqdIbgHKoRHTUjsRTLl5qKH2dgdIvlS7jKRyZK6taJO+nxxUJRyl:TYbgHnZ4yvl5qKWdgK9op8txxUq
MD5:	27AF21467C6B86ACCD5CA24B8D0E2729
SHA1:	81D5C2015BE56D4203F81CC43F3A627DC6644262
SHA-256:	B468824724F766E1DD2F1C5A093AF26AF4AC207A17F1F68C17A3DD12140D2ED2
SHA-512:	7D123FE5306A64B6E6CBFB1D236EDAEBB45D91BD97E5F4AE2E13411FE84768AF74801E2EB0F63C7A0497A266EE46451B597CFAA076DBD264B6648200220057E8
Malicious:	false
Preview:	0\r..m.....~/...._keyhttps://www.salesforce.com/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_login_bottom.min.9c3f2d6d381f893dbb9767b9db33d6af.js .https://salesforce.com/...c.%/.....OFD....+.w..d...@5!.....L.]....A..Eo.....|-.....A..Eo.....c.%/....6CD4EE0BB9EEF4F0177B99713463489148B1D6B4826F79E28887AD3A1B2E6A69OFD....+.w..d...@5!.....L.]....A..Eo.....%S..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b7793b866733cfc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11644
Entropy (8bit):	5.686144666620173
Encrypted:	false
SSDEEP:	192:gkc/8rMaFCxXvUnoSKJ5x9BFld4wfaIUqgrl1JeKaE5imIqUWbpvWyty88I+2Pm/:g9baFCxX0oSKJr9oMdUqg51sKaCuybpW
MD5:	667E372D67B7FDC636BB2027D0820F4B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b7793b866733cfc_0	
SHA1:	713C1533A91DD8BD1FA0536401EB4631B320038F
SHA-256:	D803E80D671D7E5B7756F8BA2900087E8DEAD360D1273C5B4A9E20C4CAA2E7F4
SHA-512:	9A518C1BEEA4FF68A586EDBB8AE047914BC658F4FFACACE6C2B6E8FDB310F741813A959A7AE19F73CCB5D0B5FAED9A64BD61E90266650ABE8669E89101162948
Malicious:	false
Preview:	0\r..m.....S2....._keyhttps://www.salesforce.com/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_bottom/js/platforms/adobeAnalytics/VisitorAPI.js .https://salesforce.com/..mg.%/....._..F....'...&.,.J2u.@.L...8.A..Eo.....W.0.....A..Eo.....'.....O....+...{s.....(S....`.....lL`2....(S.x.`.....L`.....PRc$.....Qb.Y.....n.....S...QbN.u.....t.....Qb..S....r.....M.d$.....$.....QbNl.6....e...`....Da....h....(S....`.....4L`.....4Rc.....Qb.....s...`$.....`....Da:.....A...Q.@&.YU....require..... Qf...8....Cannot find module '..Qb~.....'.....Qen.....MODULE_NOT_FOUND.9.....a.....Q.@.....exports....a.....Qb.....call..A..(S.P..`\...]..K`....Dn.....&...*..&...*..&.%.*..&.....&.%...%.&.].....,Rc.....I`....Da(...p.....a.....c..... .....@.-.....P.!.....https://www.salesforce.com/etc/clientlibs/sf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bc875f6b0dba4f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1894
Entropy (8bit):	5.5759385315652725
Encrypted:	false
SSDEEP:	48:msM+87m8cpyAUuiPlXEXXBtUpfmH7HMGn:Yk8cpwXExAC
MD5:	B4B1B951D72CE96208258441F20D1445
SHA1:	FBCAE7371BCCC3E37A24A7D35E056375165EA68D
SHA-256:	7FA1276045B38AF12D2ED9D8FA927726F15C0682AF30871A432B5AA772C3B6D1
SHA-512:	6857645C3D9164C1CCE4170383695A7DCA9ED49A16FBC6224990E6EB6D070AF3691E096C9761B7ED692A3D44031D3819901B0149DFE0EB57F15A794DCADEAD2
Malicious:	false
Preview:	0\r..m.....f...8.T....._keyhttps://service.force.com/embeddedservice/5.0/client/liveagent.esw.min.js .https://salesforce.com/q.cl.%/.....U.....}.<.;....Gb.e.I2...| ....L.{..c.A..Eo.....a'.....A..Eo.....q.cl.%/.8.....'..N....O.....F.F.....(S.@..`<.....L`.....Q.P:P.L....embedded_svc..Qe.<.5....defineFeature.....Qd"er<....LiveAgent....(S.....Ia/....N...y.....8.....=[...e.....&....&.(....).+....+.,.....,-....-./..../.0....0.1....1.1....2.6....7.9....9.;....;.<....<.=....=.?....?.@....@.D....D.M....M.O...O.R....S.V....V.X....X.Y....Y.Y....Y.Z....Z.[....[.\....\.]....].^....^._...._.`....`.b....b.g....h.m....m.n....n.}....}.....*...<.l,.....d.....(.g.....!."....#.#....%.&.....|...d.....".".... .....d.....'.'.....e.....-.....d.....<.=.... .....d.....D.M.....d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c9ed63e22aa523f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	464
Entropy (8bit):	5.424579608083673
Encrypted:	false
SSDEEP:	6:m29YEu21DhSagdI4JN/SxfltoCRc9rTO2VjqDK6tW29YEu21DhSagdIPlSjwCRc1:77IK4fCfltoCRcNyh7IKPljCRcbj
MD5:	2478D511411493358DCD11EBB28C8FE6
SHA1:	7B23339AB687E3D2D5602AC315D47DD144869330
SHA-256:	3465F81378F6166169D7923E839A2D7A2A61FE4008BC11317E151C1AFFDEEE31
SHA-512:	C2100FA0D89D576A2A5446B60594645EC539430BFE0C109BBD5CB2F482633E585C2BCE56AE85477AADEC3C5BEA3ED5C615BF9A230EE1C78ACEB43DAA237489E
Malicious:	false
Preview:	0\r..m.....d....F....._keyhttps://cdn.evgnet.com/beacon/salesforce/sfprod/scripts/evergage.min.js .https://salesforce.com/!^Ql.%/.....Q.....E..=.....[.y..3I.N.9?.qj..-..A..Eo.....A..Eo.....0\r..m.....d....F....._keyhttps://cdn.evgnet.com/beacon/salesforce/sfprod/scripts/evergage.min.js .https://salesforce.com/.N.n.%/.....E..=.....[.y..3I.N.9?.qj..-..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fe58cb23543dcad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.499659817440876
Encrypted:	false
SSDEEP:	6:mGeYN4IIxSzgAq3JodIh9SIlwul4jhPB/ZK6t:Nb41x0qZoKb+y2JR
MD5:	24A26E76469B94E6693273EB1A3BD2FF
SHA1:	1AFD4BC8470C5144AD6E1BD288A1695FC186E061
SHA-256:	39C1F40FD0F93B4E9287206307D98881B890894BDB3AC474B467BB1C91E05455
SHA-512:	3505177468AB4E08E52AFE4472A16515A14615E8785C4347958634871B6A59CDAA16D1604A5C9CAAF9E06CA24C0A3DE662205704B411F6291F9E629F875B460B
Malicious:	false
Preview:	0\r..m.....r.....:...._keyhttps://milehighunitedway.my.salesforce.com/jslibrary/LoginMarketingSurveyResponse.js .https://salesforce.com/.@.a.%/.....WZ.t.feD....P.e..H%n....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\132f97af514833fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.921843704971907
Encrypted:	false
SSDEEP:	6:mm/LVYcvnAN6UxnX5/OcvSrDbO41/hK6tr1nxxqlKv9gDbO4h:/4Jpmc2PN/751n3qlKlgPZ
MD5:	6C84CA6FF018DFBAECB40F079F51324D
SHA1:	A6D92D698049B9281748379A4E555753DA802B98
SHA-256:	7E884E39C4A3EF6EADE8CAFBC90D6FF272047D1C138CB0F96B1D1B78A7B590E8
SHA-512:	54ED7DE8A7C5B78FB7168DA310E398BBF64F8F3902C0217523822AEC1B35F5AE9472C8417383DBAE8F880518A2B3AE67DB3D910C4205278A85E12195BF1F63F0
Malicious:	false
Preview:	0\r..m.....e...vVg....._keyhttps://assets.vidyard.com/share/webpack/js/0-c3cdc926d9ed4a3714fd.chunk.js .https://vidyard.com/[.km.%/...../.....o!./C...El.....<KL..].n*.. .@H.A..Eo.....c.....A..Eo.....[.km.%/.....FB7AF220AB1697365CEFBD44163698386BD922E9837DAC35726DD3880C4BD18A.o!./C...El.....<KL..].n*...@H.A. .Eo.....Fw'L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bc531e21a30a47b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	400
Entropy (8bit):	5.917996803737954
Encrypted:	false
SSDEEP:	6:m++Y34d2WOgZAURmIsnRnudIfWlSWMxYCQK6tJQjnqyNzcnLCWjwXkVSR0xYCp:ougaUR/qgKaRTXQjqysL3EXX
MD5:	48838B60A15A1FAD0CF2FDA9783F79B0
SHA1:	16D83D554D4882EEB968063CC4283E03E27B563C
SHA-256:	222D8D89CB6B1C6BDA903ADA43740D0E5701FE1FD2C948EAA21C9E1F5F2DE239
SHA-512:	1A7EB1C4AF6E0AB54B404CA12788F8FCEC5E7CABE79E3956016CCF75C10EFECA41F4A9030CAB2E732E1AC86D7DD285D86434E769602274E4E38B0DEF023E47 19
Malicious:	false
Preview:	0\r..m.....q....._keyhttps://a.sfdcstatic.com/enterprise/salesforce/prod/6140/v12/oneTrust/scripttemplates/6.14.0/otBannerSdk.js .https://salesforce.com/j..c.%/..... .....+.f.....dP{.....73..TB...Pg...A..Eo.....).....A..Eo.....j..c.%/.xG..C55B7A25304FE28C9CEA78108F0F56A9B17D1595DC111D043ED628F52D6B2A07.+.f.. ...dP{.....73..TB...Pg...A..Eo.....$`6.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c26761dbfc2c2a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31879
Entropy (8bit):	5.823486831493443
Encrypted:	false
SSDEEP:	384:WFh3VAdrlsnwSFyzHG34Df2yrQioJIcoXy0wVXhAbvXBwdC8QBI:WFrq+y6s/UrXExI
MD5:	D6957E109B563BB3FC11F12A7DDF3FC7
SHA1:	4A0FF42FB88AC449F3428564EAD438E8446C2D62
SHA-256:	BC78741242D2BA72189EAF736D06B70C05A55972C110A5E9C989AF41C8E84495
SHA-512:	B56F048871BB8365B73579274BF92495564CA769E91B090629A602B3F6A44F93884E29267AA3130D6A1AF786E31986A263E4C2C9E3ACAC0766091BCDD52D10A6
Malicious:	false
Preview:	0\r..m.....p....._keyhttps://www.salesforce.com/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_top.min.301d6a760140b020516d3cfffac8a128.js .https://salesforce .com/5N.h.%/.....J.....3E..U{..=..&T.(...h....<.^.#.A..Eo.....*A7t.....A..Eo.....'..h....O.....z...J`_.....(S.....`..... L`D....<L`.....QdJ..I....SfdcWwwBase...Qb..W9....Url...Qc../.....Base64...(S.P.`Z....0L`.....4Rc.....M.a.....Qe...c....CookieHandler...`....Da2I..FQ...(S.\.`n.... L`..... .Qc61f.....document..QcZ.?[....location..Qc..m....hostname..Qcj..,....indexOf...Qe._.....salesforce.com.....K`....Dq .....&.(...&.(...&...&.Y....&...j.....&.%.4..... ..,Rc.....`....DaXJ.."K.....#....c.....P.....@.-.....P.....z...https://www.salesforce.com/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_top.min.301d6a76014 0b020516d3cfffac8a128.js..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ce0eabb8db46424_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.49269445048484
Encrypted:	false
SSDEEP:	6:mNYN4IIxSzt3FV5dICaS0d68oH4h/ZK6t:V41xmFV5KCavdnoHa/T
MD5:	FC389605177C8D7C23C743B0AD0F6958
SHA1:	24D7E613C854B2762399B3A7FA17210B0DEDE031
SHA-256:	5EA3B6CF77F4318F16C5704B67CEE1E6A404FAD76188AE86E3BA30080474A005

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ce0eabb8db46424_0	
SHA-512:	2A57CD7A6212B121224E82181CE36B31ADE5339701184AD693ECC01E30777C636C5B77CDC5726308CD405DB41D2238DD55311F3F01EA7AFF2BF179BFC7EA1F5
Malicious:	false
Preview:	0\r..m.....b.....!...._keyhttps://milehighunitedway.my.salesforce.com/jslibrary/LoginHint208.js .https://salesforce.com/.F.a.%/.....BA..*.J_hiF0.=.M`...1.I.....n ..A..Eo.....^R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\25654a32fd1008c8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3182
Entropy (8bit):	5.261888777703263
Encrypted:	false
SSDEEP:	48:wVpiThVtVBopBkDZI7VjRSWyfKjocGCzOPZBPa/RIwpsoXlpG:4SA/kNlxjfocGbW/RfdTG
MD5:	E71AA5C4362FABA72F8139B13A633859
SHA1:	B2777989380221BAF7ADC057428878340702870B
SHA-256:	0EA8C48E69183F81652644BD53FD2E3383D79660674CBCB23B5E6E9E2703A817
SHA-512:	AA7DD36D90C0E1089E3A64AF0F668843193C3618C74AA9FEAFA584D07CA60B5CCBD709FE58A53905A07DD4EB466460623A07712E7EEA9A8E4AB7CE6905DDA0 4F
Malicious:	false
Preview:	0\r..m.....^...,.L...._keyhttps://service.force.com/embeddedservice/5.0/utils/common.min.js .https://salesforce.com/..`l.%/.....T.....0Q]f.?d1!Z.?..I...\..l.V.R@..f.-.A. .Eo.....A..Eo.....`l.%/.H.....'.....O.....6.....(S.0..`.....L`.....(S.=..`4.....L`R....(S.,.`.....L`.....Qe.Z.....eventHandlers.....K`....De... .....~-.....,Rd.....Qb..^.....d...`....Da,...^.....b.....@.-....PP.1.....A...https://service.force.com/embeddedservice/5.0/utils/common.min.js...a.....D`....D`* ...D`.....l...`2...&...&....&....&.(S.....Pc.....d.getOS.al...~...IE....d.....&.(S.....Pd.....d.isDesktop.a.....IE.d.....&.(S.....5.a.....a.....Qe.!W. ....outputToConsole.a.....IE.d.....&.(S.....Pc.....d.log...a.....IE.d.....&.(S.....Pc.....d.error.a2.....IE.d.....&.(S.....Pd....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2914ffb6a4f6449d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.918863830424976
Encrypted:	false
SSDEEP:	12:4bgHnZ4aSK3NVHmGrGh22SDS4Ah99s1rGh:4bgHnZ4YDfq22V3TYq
MD5:	FE680B21FDFB5D596CFEB4A0BC72B435
SHA1:	5388FF29E032FB7BF31A581E5696E2C1B59B2D79
SHA-256:	E929F9E4C5DE82297FF66AC30621A63BD5FCBB0795711D63106B259941103D8A
SHA-512:	E596780570C6059B9AC55B7945DBE9BCAF6452F799C538C89EE239D261023FFE87AD9A02CC5634C7A7269BE7EA3C074697B70818618D852D19A9D7B58B65891D
Malicious:	false
Preview:	0\r..m.....pfT...._keyhttps://www.salesforce.com/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_bottom.min.5f37c69aa514d6e3c200b2781a9f1435.js .https://salesfo rce.com/@g.h.%/.....P.....f..B.S|k...E.]0O.....7....@..A..Eo.....M.....A..Eo.....@g.h.%/.....034B64C2971DD32B48840566C716E6AE532D90B53F27C 45F229AB792D0B07BF8.f..B.S|k...E.]0O.....7....@..A..Eo.....p\@.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b2eec19ea6624dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	65310
Entropy (8bit):	5.780021496366131
Encrypted:	false
SSDEEP:	1536:K2J/n3Bl1MquJwOx8k0PW6hXkmXRHwopT4yt:J1nx7quJwfk0PW6hXvwo7t
MD5:	0E994AA2380974EE3FCB2E335E831C74
SHA1:	2BF592B245988CFD6DD137053234344BFFC3C860
SHA-256:	B27F4FD527EED12366366AE256B8BE7D6E11197809D4555F5D4EA010D37FA732
SHA-512:	3C08BBE2F9E0F89331126220234D50862C59743EADFFDEBAB3EAC4F55F503144C4FDCC60FC6F8E13FE36E94BEE7BE863075D07845621BCF9C77BF87DC59CCC 7
Malicious:	false
Preview:	0\r..m.....g...._keyhttps://www.salesforce.com/etc.bundles/sfdc-www/bundles/webpack-script-manifest-formContainerV2-js.bundle.52bc5e074c2de27d5cb2.js .h ttps://salesforce.com/N.UI.%/.....LR.....g."....%...m....AO.b..-.!Q..A..Eo.....a..S.....A..Eo.....'..l....O.....o.....$.....,..... ....(.....(S....`.....L`<....Q.@.i.....window....Q.P.v.....webpackJsonp..Qb.Fn.....push.....`.....L`.....`.....Ma....D...`.....bh.....C`....C`....C`.. ..C`....C`....C`....C`....C`"...C`<...C`>...C`....C`Z...C`\...C`^...C``...C`~...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....(S.....Pc.....push.100aF.....d.....m.....Qb .....100.E.@.-.....P.1.....https://www.salesforce.com/etc.bundles/sfdc-www/bundles/webpack-script-manifest-formContainerV2-js.bundle.52bc5e074c2de27d5cb2 .js...a.....D`....D`l...D`.....`....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3246e51d8c77b25d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3246e51d8c77b25d_0	
Category:	dropped
Size (bytes):	856
Entropy (8bit):	5.514313088429757
Encrypted:	false
SSDEEP:	12:nNHMaK91/wxXNy7JNHMaKUKH/xXNYNJNHMaKzltCxXNI/NJNHMaK73lRnxXN1:NCzey7C3YN7Cz4I/N7CTPL1
MD5:	F8445B9E4A935E6E9443EE7FE3D47A80
SHA1:	59878FB65D155EE13412DABA7613939A901C1962
SHA-256:	E3E60880B25A10A3036C88C80A61128AF2989CB8D727B28194C63355EF26647E
SHA-512:	69A180117BAD368AEFA7680ECFA52791A8B99A1E31AB369E2D5C45315FA8E6C0CA7EAEB1C77EC99F0EE4053F0BE5606E679A36842F01382E772D11B805254C75
Malicious:	false
Preview:	0\r..m.....R...N....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://salesforce.com/.-dl.%/.....U.....om.c....X.b'.[.....H....L0.l..A..Eo.....\..E.....A..Eo.....0\r..m.....R...N....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://salesforce.com/.. m.%/.....om.c....X.b'.[.....H....L0.l..A..Eo.....y|.....A..Eo.....0\r..m.....R...N....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://salesforce.com/.u.n.%/.....om.c....X.b'.[.....H....L0.l..A..Eo.....k~.....A..Eo.....0\r..m.....R...N....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://salesforce.com/-}.n.%/.....1.....om.c....X.b'.[.....H....L0.l..A..Eo.....|/8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\327c4c88ec613485_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.403875306451186
Encrypted:	false
SSDEEP:	6:mmEYwU5IIx6JyLRsdIXSKHSElfmP4MK6t:FAYxtL2KXZFlfG
MD5:	080AD24C1ADB48FFCC059EA5EA5E574B
SHA1:	9DAC9095DB308C061F6DD0D5F135F56F3AA9B9E6
SHA-256:	EF84A3F3E327650B34C9F13FEE5404CF3A221878EBDD3D320D6B530F51DE1C8B
SHA-512:	552EC09F1B404699A9A5FEBF286EBD131662C6F2D65CD6785EB582D03F0D89C665981E7F8ECCCFDABC08E1FC82C95FAB458AE7AE02CC271EDB99C4D8E4A4ECBA
Malicious:	false
Preview:	0\r..m.....P.....(l...._keyhttps://test.salesforce.com/jslibrary/baselogin4.js .https://salesforce.com/i0.m.%/.....Iv....<J.k..!k.}...]..$.A..Eo.....p.e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3abc09c1ee5bab79_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.700297465103879
Encrypted:	false
SSDEEP:	12:FvypEHKNodAQ7arPvypEHKylZidAQ7E//7PvypEHKP1l4dAQ7F1:8nVIarKnyjpIEX7KndhIF1
MD5:	1AC3C0B8123AEF72812C616BACA33C7D
SHA1:	57A94A8584A83C6379B09F4B400BE276F205901B
SHA-256:	CE666E9B640E3B2AF784E5A39C75DC5A8F8DBC38844BCEABE136D7BCCBE9C4CB
SHA-512:	432799E9A88B670FB03C1913D7D42FC83F1CB339684668EC4E05560DA8215A3E42C6589C452A55348154A8E5F3E987E256785AE3DE8F05D5DED07DB64D93A641
Malicious:	false
Preview:	0\r..m....._....;....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N4QVCLK&l=dataLayer .https://salesforce.com/.Yl.%/.....R.....@..f....>x....@.....>F.d...A..Eo.....'A8.....A..Eo.....0\r..m....._....;....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N4QVCLK&l=dataLayer .https://salesforce.com/.H.n.%/.....@..f....>x....@.....>F.d...A..Eo.....=.....A..Eo.....0\r..m....._....;....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N4QVCLK&l=dataLayer .https://salesforce.com/...n.%/.....".....@..f....>x....@.....>F.d...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cac65354664bc92_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1555
Entropy (8bit):	5.80189008302492
Encrypted:	false
SSDEEP:	24:YbFIK3gqr7H36YL2Abe+vmp4Y+sslhYidduUbFnW0h5exuukg+X:AXgqr7H36+2D4mp+3XAzkg+X
MD5:	DB3D2F68383352CEBAFA3D0AABA46AD3
SHA1:	EAD0F2E27FF59BD58893C18EE35DDF71C3F6EA91
SHA-256:	77B4583683B854E5CD6E12D5229E96A90ED5902F471AE353DBF3540E909A7F04
SHA-512:	277B1C22F755F76FC5192C0FEBB484C8FA080F5BD798E1DE5D5B8FD604A1A73672A69DD76FDD40739AF843268167B66B4E7ED0D322DFE067AAEC12F60410AC2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cac65354664bc92_0	
Malicious:	false
Preview:	0\r..m.....c....y.%...._keyhttps://service.force.com/embeddedservice/5.0/client/invite.esw.min.js .https://salesforce.com/.lll.%/.....W.....kT!.&.#.=Y.)5...9.....V..c.. .A..Eo.....KE.....A..Eo.....lll.%/.....'..l....O.....<.....P.....(S.@..`<.....L`.....Q.P:P.L....embedded_svc..Qe.<.5....defineFeature.....Qcf2*;....In vite...(S.....Ia,....I...U.....+.....:.....".....'....'.(.... (.)....).*....*.+....+.2....2.3....3.3....3.4....4.6....6.B....C.D....D.G....G.R....R.S....S.V....W.Z....Z.[....j.k....k.n....n.p....p.q....q.s....s.t....t.v....v.w....w.x....x.x....y..... .....*.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4227dc6a3fddee79_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.570333316201845
Encrypted:	false
SSDEEP:	6:mP/XYcvnAN6VoGOC6S/eJpaSVnANZJx4XDl/hK6t:KyaoIN+pamnqZCD1
MD5:	682ABFA9ECE632A020AD4A708A3C8178
SHA1:	F5E16AB9DDEFE5CED493E680C4DEAEE21BD0C948
SHA-256:	5959C62526C5E3A84F31735B5BADF676E71701E8FA6AD55ECE394BFAB8B904EE
SHA-512:	89B2C18148314D260322DFB6BDE0246F99DE4366645ED3BF9D003240E5B5913D1EC0FCAB0F0163690EAF060955DFC0D10C5E4D9A8C0F229A23877D97BFD7DC3
Malicious:	false
Preview:	0\r..m.....g....U....._keyhttps://assets.vidyard.com/share/webpack/js/335-0cd57ad1abce82796388.chunk.js .https://vidyard.com/..lm.%/.....0.....5.Sq..Y.L...o.r..h..l... .....A..Eo.....8.U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42c6ff745afae2c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	173912
Entropy (8bit):	6.141976416109377
Encrypted:	false
SSDEEP:	3072:QsKa6cGnLvZCjbSQeAi0ARHn3ji/Ux5XqKC:rhCl+e3Hne4C
MD5:	D0AA420E32700B7EC1921BE116E209BB
SHA1:	DF174E50DB7226E52E631039E5D0F93C7A2DB54B
SHA-256:	E33638707C096D33E9B378BE6867C8AF454456B3D9576201533EE0F759099181
SHA-512:	7D01F98DA2F84BBB4C37039CFF5AB2881BB0F9A93B93CA12D4B9598EA3378ECFC8AA423B36178CD01F9B03A2A8FDE613C8CB29A8891F80CB278F78B0D76988 2
Malicious:	false
Preview:	0\r..m.....@...h.....034B64C2971DD32B48840566C716E6AE532D90B53F27C45F229AB792D0B07BF8.....'.an....O9.....9.c.....(..... .....@.....x.....|.....|.....(S.....`b.....L`.....xL`8.....Qb.^.....vp....Qb:.....Pag e...2.....Qd.Rm]....digitalData...Qe..q....siteCatConfig.....Qdnu.....s_account.....Qb..."....s....(S.....Ia.....Qdz..1....s_doPlugins.E.@.-.....P.!.....}...https://www.salesforce.c om/etc/clientlibs/sfdc-aem-master/clientlibs_analytics_bottom.min.5f37c69aa514d6e3c200b2781a9f1435.js...a.....D`....D`"...D`.....`....&...&.(S...`.....DL`.....A2.(S...`..... (L`.....Qd.-.U....getActivity...Qc.....l_vdays.....Qd.....First Visit...QeB.=.....Less than 1 day...Qe../....Less than 7 days..Qe.+.....More than 7 days. Qf.....More than 30 days ....$QgJQ.g...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\508bf6a9bb984fde_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7134
Entropy (8bit):	4.980857086775019
Encrypted:	false
SSDEEP:	96:LDr/VDob3x5B4CrWOFs6d9yNC+c2/QnmPN9P/dIMkwUpthj:LDr9Dep4CSM/QCJmP3eb3X
MD5:	B3EFB5A1BA5CAE2779DBCBBD047A1AAF
SHA1:	FD38EFECF40903D73F23976A0208AABA606B5FB9
SHA-256:	129E250377F4B59B3871844679EC100591C01C439F2CF8951D349111BA103F4F
SHA-512:	73BCE5CB44FC457243AA420E87278454D6B35E930C20D9E5ED9B38E87534F136E9E8387E652A62771E6AB9614C24FD153835EEC6E985BD6A56E12711F9E03D7C
Malicious:	false
Preview:	0\r..m.....P..8...._keyhttps://www.salesforce.com/etc.bundles/sfdc-www/bundles/vendors~scriptloader~utils.bundle.52bc5e074c2de27d5cb2.js .https://salesforc e.com/v..b.%/.....!$g/.TS..=..._'ed...O.X.6NB...A..Eo.....fV.....A..Eo.....'.J<....O....(.. .....(S.....`.....%.L`.....Qc...Q....win dow....Q.P2.M....webpackJsonp..Qb...+....push.....`.....L`.....`.....Ma.....`.....`....Y.L`(...Eh.....Em.....E`....E`.....Ek.... .....Eb.....E`....Ed.....Eb.....Ea.....Ea.....E`....E`.....E`....E`.....E`....E`.....Ec.....Ea.....(S....IaB.....d..... .....IE.@.-.....P.....q...https://www.salesforce.com/etc.bundles/sfdc-www/bundles/vendors~scriptloader~utils.bundle.52bc5e074c2de27d5cb2.js..a.....D`....

Static File Info

General

File type:	PDF document, version 1.4
Entropy (8bit):	7.200680444429164
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Denver Water COVID-19 Response _ City of Denver.pdf
File size:	184034
MD5:	a7bcca2fdf7e02497eea284f085340d9
SHA1:	ecd2f0ba7b1e5f99a3fd7310e2c12c07f68fbe69
SHA256:	3495047623e0f3271699945ab0018b8b83c55128afb028e e3a07f8f6dfaa6f88
SHA512:	b56234d8fc314fc06dcbb1a528d877f28c093049d0b75ad 008ccf6dec13f24c0623e990516b38974d215299269f0a1 4d318b554119aa1704512aa90cba867a4f
SSDEEP:	3072:uThlxnrmRF3OgYKqxLZHzOl1r45G9l1BR78kB6z bkVgH:w7rma/ilKkl1TByQgH
File Content Preview:	%PDF-1.4.%.....1 0 obj.<</Creator (Mozilla/5.0 \(Windo ws NT 10.0; Win64; x64\) AppleWebKit/537.36 \(KHTML , like Gecko\) Chrome/91.0.4472.124 Safari/537.36)./Pr oducer (Skia/PDF m91)./CreationDate (D:20210715194 102+00'00')./ModDate (D:20210715194102+00'00')

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.200680
Total Bytes:	184034
Stream Entropy:	7.997100
Stream Bytes:	96849
Entropy outside Streams:	0.000000
Bytes outside Streams:	87185
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
8	0071e8c4c4e87100	a055fa61a0d695c66d8caa7e6d9ad900	
9	0000404040400000	986a9da71e7a861fc6ab81304c327543	
19	00c8e96961696900	b160bb3b3828c8866b85d80f3a11d344	

ID	DHASH	MD5	Preview
20	0000402020480000	02511ced1155463264a7ac1bd75abb07	
21	40b0f269f4b05024	c38be4fb8c419f23c6879bc75fb03d0f	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/16/21-16:39:34.446596	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61585	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 16, 2021 16:39:14.210187912 CEST	192.168.2.5	8.8.8.8	0x5e90	Standard query (0)	force.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:28.211425066 CEST	192.168.2.5	8.8.8.8	0xa0ea	Standard query (0)	milehighunitedway.lightning.force.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:29.172324896 CEST	192.168.2.5	8.8.8.8	0x7a5e	Standard query (0)	milehighunitedway.my.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:31.081058979 CEST	192.168.2.5	8.8.8.8	0xc185	Standard query (0)	login.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.100406885 CEST	192.168.2.5	8.8.8.8	0xdd60	Standard query (0)	c.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.370102882 CEST	192.168.2.5	8.8.8.8	0x75dc	Standard query (0)	cdn.evgnet.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.370744944 CEST	192.168.2.5	8.8.8.8	0xa71a	Standard query (0)	salesforce.us-1.evergage.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.375431061 CEST	192.168.2.5	8.8.8.8	0x2071	Standard query (0)	a.sfdcstatic.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.375648975 CEST	192.168.2.5	8.8.8.8	0xfcd	Standard query (0)	www.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.808172941 CEST	192.168.2.5	8.8.8.8	0xd5ef	Standard query (0)	milehighunitedway.my.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:33.090857029 CEST	192.168.2.5	8.8.8.8	0x9f18	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.047305107 CEST	192.168.2.5	8.8.8.8	0xed64	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.635565996 CEST	192.168.2.5	8.8.8.8	0xdbef	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.924534082 CEST	192.168.2.5	8.8.8.8	0x1237	Standard query (0)	www.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.995759964 CEST	192.168.2.5	8.8.8.8	0xc1c0	Standard query (0)	salesforcecom.demdex.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 16, 2021 16:39:34.997960091 CEST	192.168.2.5	8.8.8.8	0xeb89	Standard query (0)	omtr2.partners.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.003062963 CEST	192.168.2.5	8.8.8.8	0x8074	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:44.030108929 CEST	192.168.2.5	8.8.8.8	0xb467	Standard query (0)	milehighunitedway.my.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.059966087 CEST	192.168.2.5	8.8.8.8	0xaa25	Standard query (0)	www.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.375201941 CEST	192.168.2.5	8.8.8.8	0x7ba9	Standard query (0)	a.sfdcstatic.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.376835108 CEST	192.168.2.5	8.8.8.8	0x92d8	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.394750118 CEST	192.168.2.5	8.8.8.8	0x8ce2	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.560816050 CEST	192.168.2.5	8.8.8.8	0x1e	Standard query (0)	salesforce.us-1.evergage.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.562454939 CEST	192.168.2.5	8.8.8.8	0x9605	Standard query (0)	cdn.evgnet.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.751992941 CEST	192.168.2.5	8.8.8.8	0xb58d	Standard query (0)	org62.my.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.752229929 CEST	192.168.2.5	8.8.8.8	0xcc30	Standard query (0)	a10681260716.cdn.optimizely.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.337188005 CEST	192.168.2.5	8.8.8.8	0x8a6f	Standard query (0)	cdn.krxd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.337450981 CEST	192.168.2.5	8.8.8.8	0xcaba	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.337601900 CEST	192.168.2.5	8.8.8.8	0x80a1	Standard query (0)	service.force.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.043036938 CEST	192.168.2.5	8.8.8.8	0xcda5	Standard query (0)	cdn.evgnet.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.044368982 CEST	192.168.2.5	8.8.8.8	0xa75e	Standard query (0)	privacy-policy.truste.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.255655050 CEST	192.168.2.5	8.8.8.8	0x2df8	Standard query (0)	a10681260716.cdn.optimizely.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.503506899 CEST	192.168.2.5	8.8.8.8	0x7fa4	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.764148951 CEST	192.168.2.5	8.8.8.8	0xd14d	Standard query (0)	salesforce.us-1.evergage.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.963886023 CEST	192.168.2.5	8.8.8.8	0x1d5c	Standard query (0)	service.force.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.425084114 CEST	192.168.2.5	8.8.8.8	0xa637	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.547463894 CEST	192.168.2.5	8.8.8.8	0xee9a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.883198023 CEST	192.168.2.5	8.8.8.8	0x3c80	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.951903105 CEST	192.168.2.5	8.8.8.8	0x64e7	Standard query (0)	d.la2-c1-ia4.salesforceliveagent.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.004822016 CEST	192.168.2.5	8.8.8.8	0x36af	Standard query (0)	trial-eum-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.006069899 CEST	192.168.2.5	8.8.8.8	0xcb86	Standard query (0)	trial-eum-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.247283936 CEST	192.168.2.5	8.8.8.8	0x6d9d	Standard query (0)	kqitim5n3zwnuyhrti7a-pinofr-89940bd62-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.248061895 CEST	192.168.2.5	8.8.8.8	0x8f18	Standard query (0)	84-17-52-51_s-80-67-82-83_ts-1626446398-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.593508959 CEST	192.168.2.5	8.8.8.8	0x201a	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642673969 CEST	192.168.2.5	8.8.8.8	0xe3b4	Standard query (0)	d.la2-c1-ia5.salesforceliveagent.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.835752964 CEST	192.168.2.5	8.8.8.8	0x4098	Standard query (0)	1737ad5b.akstat.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 16, 2021 16:39:59.118799925 CEST	192.168.2.5	8.8.8.8	0x5bce	Standard query (0)	privacy-policy.truste.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:08.062321901 CEST	192.168.2.5	8.8.8.8	0x1e10	Standard query (0)	test.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:09.036859989 CEST	192.168.2.5	8.8.8.8	0x8f78	Standard query (0)	www.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:09.567296028 CEST	192.168.2.5	8.8.8.8	0xd815	Standard query (0)	test.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:11.943944931 CEST	192.168.2.5	8.8.8.8	0xea0b	Standard query (0)	salesforce.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:14.551315069 CEST	192.168.2.5	8.8.8.8	0x2b94	Standard query (0)	assets.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:14.555058956 CEST	192.168.2.5	8.8.8.8	0x318	Standard query (0)	c1.sfdcstatic.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:14.948591948 CEST	192.168.2.5	8.8.8.8	0xaaaa	Standard query (0)	play.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:15.514595985 CEST	192.168.2.5	8.8.8.8	0x7554	Standard query (0)	cdn.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.126163960 CEST	192.168.2.5	8.8.8.8	0x387	Standard query (0)	raw.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.612281084 CEST	192.168.2.5	8.8.8.8	0x2b6a	Standard query (0)	salesforce.vidyard.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.282321930 CEST	192.168.2.5	8.8.8.8	0xb134	Standard query (0)	vfhbo3jsnvrutdkuee1akd0lj.litix.io	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.235372066 CEST	192.168.2.5	8.8.8.8	0x4c28	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.238065958 CEST	192.168.2.5	8.8.8.8	0xd460	Standard query (0)	a.sfdcstatic.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.565220118 CEST	192.168.2.5	8.8.8.8	0xce3	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.623236895 CEST	192.168.2.5	8.8.8.8	0xdb61	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.641225100 CEST	192.168.2.5	8.8.8.8	0x12ef	Standard query (0)	org62.my.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.644010067 CEST	192.168.2.5	8.8.8.8	0x53a7	Standard query (0)	cdn.krxd.net	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.725491047 CEST	192.168.2.5	8.8.8.8	0x9d1	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:34.505635023 CEST	192.168.2.5	8.8.8.8	0x9d6e	Standard query (0)	omtr2.partners.salesforce.com	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:38.534806013 CEST	192.168.2.5	8.8.8.8	0xa48e	Standard query (0)	kqitim2qinjecyhrtjsa-f-61be14707-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		23.1.35.132	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		184.31.10.133	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		104.109.11.129	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		104.109.10.129	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		23.1.106.133	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		184.31.3.130	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		23.1.99.130	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:14.273256063 CEST	8.8.8.8	192.168.2.5	0x5e90	No error (0)	force.com		184.25.179.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	milehighunitedway.lightning.force.com	na136.lightning.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136.lightning.force.com	na136.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136.force.com	na136-ph2.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136-ph2.force.com	na136-ph2.ph2.r.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136-ph2.ph2.r.force.com		13.110.37.182	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136-ph2.ph2.r.force.com		13.110.36.54	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:28.425654888 CEST	8.8.8.8	192.168.2.5	0xa0ea	No error (0)	na136-ph2.ph2.r.force.com		13.110.39.54	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	milehighunitedway.my.salesforce.com	na136.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	na136.my.salesforce.com	na136-ph2.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	na136-ph2.my.salesforce.com	na136-ph2.ph2.r.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.39.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.36.53	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:29.383783102 CEST	8.8.8.8	192.168.2.5	0x7a5e	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.37.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:31.131093979 CEST	8.8.8.8	192.168.2.5	0xc185	No error (0)	login.salesforce.com	login.l2.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:31.131093979 CEST	8.8.8.8	192.168.2.5	0xc185	No error (0)	login.l2.salesforce.com		85.222.155.195	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:31.131093979 CEST	8.8.8.8	192.168.2.5	0xc185	No error (0)	login.l2.salesforce.com		85.222.153.67	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:31.131093979 CEST	8.8.8.8	192.168.2.5	0xc185	No error (0)	login.l2.salesforce.com		85.222.155.67	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.159926891 CEST	8.8.8.8	192.168.2.5	0xdd60	No error (0)	c.salesforce.com	c.salesforce.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:32.422811985 CEST	8.8.8.8	192.168.2.5	0xa71a	No error (0)	salesforce.us-1.evergage.com		34.192.141.216	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.422811985 CEST	8.8.8.8	192.168.2.5	0xa71a	No error (0)	salesforce.us-1.evergage.com		52.1.220.4	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.433067083 CEST	8.8.8.8	192.168.2.5	0x75dc	No error (0)	cdn.evgnet.com		151.101.0.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.433067083 CEST	8.8.8.8	192.168.2.5	0x75dc	No error (0)	cdn.evgnet.com		151.101.64.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.433067083 CEST	8.8.8.8	192.168.2.5	0x75dc	No error (0)	cdn.evgnet.com		151.101.192.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.433067083 CEST	8.8.8.8	192.168.2.5	0x75dc	No error (0)	cdn.evgnet.com		151.101.128.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.434685946 CEST	8.8.8.8	192.168.2.5	0xfcd	No error (0)	www.salesforce.com	www.salesforce.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:32.437314987 CEST	8.8.8.8	192.168.2.5	0x2071	No error (0)	a.sfdcstatic.com	a.sfdcstatic.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	milehighunitedway.my.salesforce.com	na136.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	na136.my.salesforce.com	na136-ph2.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	na136-ph2.my.salesforce.com	na136-ph2.ph2.r.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.39.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.36.53	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:32.872862101 CEST	8.8.8.8	192.168.2.5	0xd5ef	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.37.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:33.149096012 CEST	8.8.8.8	192.168.2.5	0x9f18	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:33.149096012 CEST	8.8.8.8	192.168.2.5	0x9f18	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.211.113.33	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.211.62.226	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.153.45	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.168.191	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.168.199	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.16.73.168	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.109493971 CEST	8.8.8.8	192.168.2.5	0xed64	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.706017971 CEST	8.8.8.8	192.168.2.5	0xdbef	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:34.706017971 CEST	8.8.8.8	192.168.2.5	0xdbef	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:34.985310078 CEST	8.8.8.8	192.168.2.5	0x1237	No error (0)	www.salesforce.com	www.salesforce.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	salesforcecom.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.76.54.153	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.243.30.18	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.16.73.168	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.101.97	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.106.150	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.052839041 CEST	8.8.8.8	192.168.2.5	0xc1c0	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.154.124.189	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.064451933 CEST	8.8.8.8	192.168.2.5	0x8074	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:35.065136909 CEST	8.8.8.8	192.168.2.5	0xeb89	No error (0)	omtr2.partners.salesforce.com	partners.salesforce.com.ssl.d2.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:35.065136909 CEST	8.8.8.8	192.168.2.5	0xeb89	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		15.236.176.210	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.065136909 CEST	8.8.8.8	192.168.2.5	0xeb89	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		13.36.218.177	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:35.065136909 CEST	8.8.8.8	192.168.2.5	0xeb89	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		15.188.95.229	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	milehighunitedway.my.salesforce.com	na136.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	na136.my.salesforce.com	na136-ph2.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	na136-ph2.my.salesforce.com	na136-ph2.ph2.r.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.39.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.36.53	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:44.091275930 CEST	8.8.8.8	192.168.2.5	0xb467	No error (0)	na136-ph2.ph2.r.my.salesforce.com		13.110.37.181	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.121916056 CEST	8.8.8.8	192.168.2.5	0xaa25	No error (0)	www.salesforce.com	www.salesforce.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.436907053 CEST	8.8.8.8	192.168.2.5	0x7ba9	No error (0)	a.sfdcstatic.com	a.sfdcstatic.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:54.439102888 CEST	8.8.8.8	192.168.2.5	0x92d8	No error (0)	api.company-target.com		99.86.162.22	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.439102888 CEST	8.8.8.8	192.168.2.5	0x92d8	No error (0)	api.company-target.com		99.86.162.29	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.439102888 CEST	8.8.8.8	192.168.2.5	0x92d8	No error (0)	api.company-target.com		99.86.162.95	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.439102888 CEST	8.8.8.8	192.168.2.5	0x92d8	No error (0)	api.company-target.com		99.86.162.70	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.453921080 CEST	8.8.8.8	192.168.2.5	0x8ce2	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.619858027 CEST	8.8.8.8	192.168.2.5	0x9605	No error (0)	cdn.evgnet.com		151.101.192.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.619858027 CEST	8.8.8.8	192.168.2.5	0x9605	No error (0)	cdn.evgnet.com		151.101.64.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.619858027 CEST	8.8.8.8	192.168.2.5	0x9605	No error (0)	cdn.evgnet.com		151.101.128.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.619858027 CEST	8.8.8.8	192.168.2.5	0x9605	No error (0)	cdn.evgnet.com		151.101.0.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.634404898 CEST	8.8.8.8	192.168.2.5	0x1e	No error (0)	salesforce.us-1.evergage.com		52.1.220.4	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.634404898 CEST	8.8.8.8	192.168.2.5	0x1e	No error (0)	salesforce.us-1.evergage.com		34.192.141.216	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.812299013 CEST	8.8.8.8	192.168.2.5	0xcc30	No error (0)	a10681260716.cdn.optimizely.com	wildcard.cdn.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	org62.my.salesforce.com	na128.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	na128.my.salesforce.com	na128-ia5.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	na128-ia5.my.salesforce.com	na128-ia5.ia5.r.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.46.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.43.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:54.899667025 CEST	8.8.8.8	192.168.2.5	0xb58d	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.44.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.397944927 CEST	8.8.8.8	192.168.2.5	0x8a6f	No error (0)	cdn.krxd.net	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:55.400913000 CEST	8.8.8.8	192.168.2.5	0xcaba	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.400913000 CEST	8.8.8.8	192.168.2.5	0xcaba	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	service.force.com	location.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.force.com	location.l.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l.force.com		161.71.8.169	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l.force.com		161.71.11.44	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l.force.com		161.71.8.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l .force.com		161.71.10.172	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l .force.com		161.71.10.169	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:55.401282072 CEST	8.8.8.8	192.168.2.5	0x80a1	No error (0)	location.l .force.com		161.71.8.41	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.100162029 CEST	8.8.8.8	192.168.2.5	0xcda5	No error (0)	cdn.evgnet.com		151.101.0.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.100162029 CEST	8.8.8.8	192.168.2.5	0xcda5	No error (0)	cdn.evgnet.com		151.101.64.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.100162029 CEST	8.8.8.8	192.168.2.5	0xcda5	No error (0)	cdn.evgnet.com		151.101.192.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.100162029 CEST	8.8.8.8	192.168.2.5	0xcda5	No error (0)	cdn.evgnet.com		151.101.128.114	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.104259968 CEST	8.8.8.8	192.168.2.5	0xa75e	No error (0)	privacy-po licy.truste.com	d2pj9rkatqbt38.cloudfront. net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:56.104259968 CEST	8.8.8.8	192.168.2.5	0xa75e	No error (0)	d2pj9rkatq bt38.cloud front.net		65.9.66.106	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.104259968 CEST	8.8.8.8	192.168.2.5	0xa75e	No error (0)	d2pj9rkatq bt38.cloud front.net		65.9.66.105	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.104259968 CEST	8.8.8.8	192.168.2.5	0xa75e	No error (0)	d2pj9rkatq bt38.cloud front.net		65.9.66.8	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.104259968 CEST	8.8.8.8	192.168.2.5	0xa75e	No error (0)	d2pj9rkatq bt38.cloud front.net		65.9.66.54	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.327815056 CEST	8.8.8.8	192.168.2.5	0x2df8	No error (0)	a106812607 16.cdn.opt imizely.com	wildcard.cdn.optimizely.c om.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:56.573539972 CEST	8.8.8.8	192.168.2.5	0x7fa4	No error (0)	s.go-mpulse.net	ip46.go- mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:56.821301937 CEST	8.8.8.8	192.168.2.5	0xd14d	No error (0)	salesforce.us- 1.evergage.com		52.1.220.4	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:56.821301937 CEST	8.8.8.8	192.168.2.5	0xd14d	No error (0)	salesforce.us- 1.evergage.com		34.192.141.216	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	service.fo rce.com	location.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.f orce.com	location.l.force.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.8.169	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.11.44	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.8.44	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.10.172	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.10.169	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.034529924 CEST	8.8.8.8	192.168.2.5	0x1d5c	No error (0)	location.l .force.com		161.71.8.41	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.489547968 CEST	8.8.8.8	192.168.2.5	0xa637	No error (0)	c.go-mpulse.net	wildcard46.go- mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:57.596494913 CEST	8.8.8.8	192.168.2.5	0xee9a	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:57.596494913 CEST	8.8.8.8	192.168.2.5	0xee9a	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.596494913 CEST	8.8.8.8	192.168.2.5	0xee9a	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.596494913 CEST	8.8.8.8	192.168.2.5	0xee9a	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.596494913 CEST	8.8.8.8	192.168.2.5	0xee9a	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:57.940542936 CEST	8.8.8.8	192.168.2.5	0x3c80	No error (0)	www.google.ch		142.250.185.131	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.063721895 CEST	8.8.8.8	192.168.2.5	0x36af	No error (0)	trial-eum-clienttons-s.akamaihd.net	trial-eum.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.063721895 CEST	8.8.8.8	192.168.2.5	0x36af	No error (0)	trial-eum.cname.clienttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.068471909 CEST	8.8.8.8	192.168.2.5	0xcb86	No error (0)	trial-eum-clientnsv4-s.akamaihd.net	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.097107887 CEST	8.8.8.8	192.168.2.5	0x64e7	No error (0)	d.la2-c1-ia4.salesforceliveagent.com	la2-c1-ia4.salesforceliveagent.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.097107887 CEST	8.8.8.8	192.168.2.5	0x64e7	No error (0)	la2-c1-ia4.salesforceliveagent.com	la2-c1-ia4.ia4.r.salesforceliveagent.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.097107887 CEST	8.8.8.8	192.168.2.5	0x64e7	No error (0)	la2-c1-ia4.ia4.r.salesforceliveagent.com		13.109.191.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.097107887 CEST	8.8.8.8	192.168.2.5	0x64e7	No error (0)	la2-c1-ia4.ia4.r.salesforceliveagent.com		13.110.57.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.097107887 CEST	8.8.8.8	192.168.2.5	0x64e7	No error (0)	la2-c1-ia4.ia4.r.salesforceliveagent.com		13.110.56.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.330265045 CEST	8.8.8.8	192.168.2.5	0x8f18	No error (0)	84-17-52-51_s-80-67-82-83_ts-1626446398-clienttons-s.akamaihd.net	84.17.52.51_s-80.67.82.83_ts-1626446398.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.330265045 CEST	8.8.8.8	192.168.2.5	0x8f18	No error (0)	84.17.52.51_s-80.67.82.83_ts-1626446398.cname.clienttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.350034952 CEST	8.8.8.8	192.168.2.5	0x6d9d	No error (0)	kqitim5n3zwnuyhrti7a-pinofr-89940bd62-clientnsv4-s.akamaihd.net	kqitim5n3zwnuyhrti7a-pinofr-89940bd62.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.350034952 CEST	8.8.8.8	192.168.2.5	0x6d9d	No error (0)	kqitim5n3zwnuyhrti7a-pinofr-89940bd62.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.225.136.92	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.235.253.93	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		34.201.191.168	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.55.122.255	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.55.235.182	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		34.232.172.2	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		3.224.117.145	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.642741919 CEST	8.8.8.8	192.168.2.5	0x201a	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.44.89.131	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.699923992 CEST	8.8.8.8	192.168.2.5	0xe3b4	No error (0)	d.la2-c1-ia5.salesforceliveagent.com	la2-c1-ia5.salesforceliveagent.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.699923992 CEST	8.8.8.8	192.168.2.5	0xe3b4	No error (0)	la2-c1-ia5.salesforceliveagent.com	la2-c1-ia5.ia5.r.salesforceliveagent.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:58.699923992 CEST	8.8.8.8	192.168.2.5	0xe3b4	No error (0)	la2-c1-ia5.ia5.r.salesforceliveagent.com		13.110.41.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.699923992 CEST	8.8.8.8	192.168.2.5	0xe3b4	No error (0)	la2-c1-ia5.ia5.r.salesforceliveagent.com		13.110.66.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.699923992 CEST	8.8.8.8	192.168.2.5	0xe3b4	No error (0)	la2-c1-ia5.ia5.r.salesforceliveagent.com		13.110.43.111	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:58.894931078 CEST	8.8.8.8	192.168.2.5	0x4098	No error (0)	1737ad5b.akstat.io	wildcard46.akstat.io.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:59.181302071 CEST	8.8.8.8	192.168.2.5	0x5bce	No error (0)	privacy-policy.truste.com	d2pj9rkatqbt38.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:39:59.181302071 CEST	8.8.8.8	192.168.2.5	0x5bce	No error (0)	d2pj9rkatqbt38.cloudfront.net		65.9.66.106	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:59.181302071 CEST	8.8.8.8	192.168.2.5	0x5bce	No error (0)	d2pj9rkatqbt38.cloudfront.net		65.9.66.8	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:59.181302071 CEST	8.8.8.8	192.168.2.5	0x5bce	No error (0)	d2pj9rkatqbt38.cloudfront.net		65.9.66.54	A (IP address)	IN (0x0001)
Jul 16, 2021 16:39:59.181302071 CEST	8.8.8.8	192.168.2.5	0x5bce	No error (0)	d2pj9rkatqbt38.cloudfront.net		65.9.66.105	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:08.119538069 CEST	8.8.8.8	192.168.2.5	0x1e10	No error (0)	test.salesforce.com	test.l2.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:08.119538069 CEST	8.8.8.8	192.168.2.5	0x1e10	No error (0)	test.l2.salesforce.com		85.222.152.194	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:08.119538069 CEST	8.8.8.8	192.168.2.5	0x1e10	No error (0)	test.l2.salesforce.com		85.222.154.194	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:08.119538069 CEST	8.8.8.8	192.168.2.5	0x1e10	No error (0)	test.l2.salesforce.com		85.222.155.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:40:09.094033003 CEST	8.8.8.8	192.168.2.5	0x8f78	No error (0)	www.salesforce.com	www.salesforce.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:09.624427080 CEST	8.8.8.8	192.168.2.5	0xd815	No error (0)	test.salesforce.com	test.l2.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:09.624427080 CEST	8.8.8.8	192.168.2.5	0xd815	No error (0)	test.l2.salesforce.com		85.222.153.66	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:09.624427080 CEST	8.8.8.8	192.168.2.5	0xd815	No error (0)	test.l2.salesforce.com		85.222.155.194	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:09.624427080 CEST	8.8.8.8	192.168.2.5	0xd815	No error (0)	test.l2.salesforce.com		85.222.155.66	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:12.004009008 CEST	8.8.8.8	192.168.2.5	0xea0b	No error (0)	salesforce.vidyard.com		54.205.5.87	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:12.004009008 CEST	8.8.8.8	192.168.2.5	0xea0b	No error (0)	salesforce.vidyard.com		52.205.54.201	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:14.611517906 CEST	8.8.8.8	192.168.2.5	0x2b94	No error (0)	assets.vidyard.com	p.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:14.625035048 CEST	8.8.8.8	192.168.2.5	0x318	No error (0)	c1.sfdcstatic.com	c.sfdcstatic.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:15.005613089 CEST	8.8.8.8	192.168.2.5	0xaaaa	No error (0)	play.vidyard.com	p.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:15.578571081 CEST	8.8.8.8	192.168.2.5	0x7554	No error (0)	cdn.vidyard.com	cs6.cn.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:15.578571081 CEST	8.8.8.8	192.168.2.5	0x7554	No error (0)	cs6.cn.wpc.omegacdn.net	cs6.wpc.apr-17a6a-2.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:15.578571081 CEST	8.8.8.8	192.168.2.5	0x7554	No error (0)	cs6.wpc.omegacdn.net		93.184.221.26	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.187036037 CEST	8.8.8.8	192.168.2.5	0x387	No error (0)	raw.vidyard.com		34.234.32.98	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.187036037 CEST	8.8.8.8	192.168.2.5	0x387	No error (0)	raw.vidyard.com		44.194.2.86	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.670679092 CEST	8.8.8.8	192.168.2.5	0x2b6a	No error (0)	salesforce.vidyard.com		54.205.5.87	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:16.670679092 CEST	8.8.8.8	192.168.2.5	0x2b6a	No error (0)	salesforce.vidyard.com		52.205.54.201	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	vfhbo3jsnvrutdkuee1akd0lj.litix.io	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		3.227.80.201	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		3.212.116.77	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		3.211.86.125	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		3.224.91.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		50.19.68.215	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		52.87.9.202	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		3.214.163.16	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:21.345416069 CEST	8.8.8.8	192.168.2.5	0xb134	No error (0)	a9010d017688211ea9afe0620acb249f-596514373.us-east-1.elb.amazonaws.com		52.71.207.95	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.295815945 CEST	8.8.8.8	192.168.2.5	0x4c28	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.302165031 CEST	8.8.8.8	192.168.2.5	0xd460	No error (0)	a.sfdcstatic.com	a.sfdcstatic.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.628416061 CEST	8.8.8.8	192.168.2.5	0xce3	No error (0)	api.company-target.com		143.204.205.100	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.628416061 CEST	8.8.8.8	192.168.2.5	0xce3	No error (0)	api.company-target.com		143.204.205.98	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.628416061 CEST	8.8.8.8	192.168.2.5	0xce3	No error (0)	api.company-target.com		143.204.205.84	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.628416061 CEST	8.8.8.8	192.168.2.5	0xce3	No error (0)	api.company-target.com		143.204.205.53	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.156.174	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.243.30.18	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.233.208	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.153.45	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.219.200	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 16, 2021 16:40:32.682895899 CEST	8.8.8.8	192.168.2.5	0xdb61	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.44.171	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.707768917 CEST	8.8.8.8	192.168.2.5	0x53a7	No error (0)	cdn.krxd.net	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.786720037 CEST	8.8.8.8	192.168.2.5	0x9d1	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.786720037 CEST	8.8.8.8	192.168.2.5	0x9d1	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	org62.my.salesforce.com	na128.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	na128.my.salesforce.com	na128-ia5.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	na128-ia5.my.salesforce.com	na128-ia5.ia5.r.my.salesforce.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.69.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.70.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:32.791412115 CEST	8.8.8.8	192.168.2.5	0x12ef	No error (0)	na128-ia5.ia5.r.my.salesforce.com		13.110.65.75	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:34.568871975 CEST	8.8.8.8	192.168.2.5	0x9d6e	No error (0)	omtr2.partners.salesforce.com	partners.salesforce.com.ssl.d2.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:34.568871975 CEST	8.8.8.8	192.168.2.5	0x9d6e	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		15.236.176.210	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:34.568871975 CEST	8.8.8.8	192.168.2.5	0x9d6e	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		13.36.218.177	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:34.568871975 CEST	8.8.8.8	192.168.2.5	0x9d6e	No error (0)	partners.salesforce.com.ssl.d2.sc.omtrdc.net		15.188.95.229	A (IP address)	IN (0x0001)
Jul 16, 2021 16:40:38.631874084 CEST	8.8.8.8	192.168.2.5	0xa48e	No error (0)	kqitim2qinjecyhrtjsa-f-61be14707-clientnsv4-s.akamaihd.net	kqitim2qinjecyhrtjsa-f-61be14707.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 16, 2021 16:40:38.631874084 CEST	8.8.8.8	192.168.2.5	0xa48e	No error (0)	kqitim2qinjecyhrtjsa-f-61be14707.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- salesforce.vidyard.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49913	54.205.5.87	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 16, 2021 16:40:12.167887926 CEST	14076	OUT	GET /watch/MxeeKTO3x5oMx4jNVWWX4w HTTP/1.1 Host: salesforce.vidyard.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
Jul 16, 2021 16:40:12.392962933 CEST	14077	IN	HTTP/1.1 302 Found Date: Fri, 16 Jul 2021 14:40:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Referrer-Policy: no-referrer-when-downgrade X-Content-Type-Options: nosniff X-Robots-Tag: noindex Strict-Transport-Security: max-age=31556952 Location: https://salesforce.vidyard.com/watch/MxeeKTO3x5oMx4jNVWWX4w Cache-Control: no-cache Content-Security-Policy: default-src * mailto: tel:; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline' X-Request-Id: 2f3bd9ee-35e4-4c6a-93eb-81584b6a27aa X-Runtime: 0.054526 Data Raw: 37 64 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 61 6c 65 73 66 6f 72 63 65 2e 76 69 64 79 61 72 64 2e 63 6f 6d 2f 77 61 74 63 68 2f 4d 78 65 65 4b 54 4f 33 78 35 6f 4d 78 34 6a 4e 56 57 57 58 34 77 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 7d<html><body>You are being redirected.</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
Jul 16, 2021 16:39:28.775032043 CEST	13.110.37.182	443	192.168.2.5	49746	CN=*.na136.force.com, O="salesforce.com, 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	Fri Aug 28 02:00:00 CEST 2020	Fri Aug 27 14:00:00 CEST 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
					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		
Jul 16, 2021 16:39:28.775079012 CEST	13.110.37.182	443	192.168.2.5	49747	CN=*.na136.force.com, O="salesforce.com, 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	Fri Aug 28 02:00:00 CEST 2020	Fri Aug 27 14:00:00 CEST 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
					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		
Jul 16, 2021 16:39:28.779479027 CEST	13.110.37.182	443	192.168.2.5	49748	CN=*.na136.force.com, O="salesforce.com, 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	Fri Aug 28 02:00:00 CEST 2020	Fri Aug 27 14:00:00 CEST 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
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:39:29.733500004 CEST	13.110.39.181	443	192.168.2.5	49751	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:29.770757914 CEST	13.110.39.181	443	192.168.2.5	49753	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:30.621341944 CEST	13.110.39.181	443	192.168.2.5	49757	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:30.868350983 CEST	13.110.39.181	443	192.168.2.5	49758	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:31.218091011 CEST	85.222.155.195	443	192.168.2.5	49762	CN=login.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:39:31.347224951 CEST	13.110.39.181	443	192.168.2.5	49760	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:31.347333908 CEST	13.110.39.181	443	192.168.2.5	49759	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:31.348797083 CEST	13.110.39.181	443	192.168.2.5	49761	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:32.535665035 CEST	151.101.0.114	443	192.168.2.5	49770	CN=cdn.evergage.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 28 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Apr 28 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	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
Jul 16, 2021 16:39:32.755556107 CEST	34.192.141.216	443	192.168.2.5	49769	CN=*.us-1.evergage.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	Fri Oct 02 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	Mon Nov 01 13:00:00 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		
Jul 16, 2021 16:39:33.268650055 CEST	13.110.39.181	443	192.168.2.5	49774	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	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=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		
Jul 16, 2021 16:39:33.268748045 CEST	13.110.39.181	443	192.168.2.5	49775	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	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=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		
Jul 16, 2021 16:39:34.248372078 CEST	52.211.113.33	443	192.168.2.5	49786	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 16, 2021 16:39:35.192650080 CEST	54.76.54.153	443	192.168.2.5	49791	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 16, 2021 16:39:54.807164907 CEST	151.101.192.114	443	192.168.2.5	49828	CN=cdn.evergage.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 28 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Apr 28 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 16, 2021 16:39:55.042015076 CEST	52.1.220.4	443	192.168.2.5	49830	CN=*.us-1.evergage.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	Fri Oct 02 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	Mon Nov 01 13:00:00 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Jul 16, 2021 16:39:55.468502045 CEST	13.110.46.75	443	192.168.2.5	49835	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:39:55.607800007 CEST	161.71.8.169	443	192.168.2.5	49837	CN=*.um1.force.com, O="salesforce.com, 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	Wed Mar 31 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Thu Mar 31 01:59:59 CEST 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		
Jul 16, 2021 16:39:56.195765972 CEST	151.101.0.114	443	192.168.2.5	49839	CN=cdn.evergage.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 28 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Apr 28 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 16, 2021 16:39:57.146698952 CEST	161.71.8.169	443	192.168.2.5	49848	CN=*.um1.force.com, O="salesforce.com, 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	Wed Mar 31 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Thu Mar 31 01:59:59 CEST 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Jul 16, 2021 16:39:57.196178913 CEST	52.1.220.4	443	192.168.2.5	49844	CN=*.us-1.evergage.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	Fri Oct 02 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	Mon Nov 01 13:00:00 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		
Jul 16, 2021 16:39:57.341373920 CEST	52.1.220.4	443	192.168.2.5	49846	CN=*.us-1.evergage.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	Fri Oct 02 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	Mon Nov 01 13:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:39:57.491981983 CEST	161.71.8.169	443	192.168.2.5	49851	CN=*.um1.force.com, O="salesforce.com, 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	Wed Mar 31 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Thu Mar 31 01:59:59 CEST 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		
Jul 16, 2021 16:39:58.353833914 CEST	13.109.191.111	443	192.168.2.5	49867	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:39:58.354335070 CEST	13.109.191.111	443	192.168.2.5	49868	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:39:58.459656000 CEST	13.109.191.111	443	192.168.2.5	49869	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:39:58.966083050 CEST	13.110.41.111	443	192.168.2.5	49877	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:39:58.966301918 CEST	13.110.41.111	443	192.168.2.5	49878	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021	Fri Feb 25 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 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		
Jul 16, 2021 16:39:58.970612049 CEST	54.225.136.92	443	192.168.2.5	49876	CN=logx.optimizely.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	Mon Sep 21 02:00:00 CEST 2020	Thu Oct 21 14:00:00 CEST 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
					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		
Jul 16, 2021 16:39:59.271012068 CEST	65.9.66.106	443	192.168.2.5	49883	CN=*.truste.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	Tue Feb 16 01:00:00 CET 2021	Fri Mar 18 00:59:59 CET 2022	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		

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		
Jul 16, 2021 16:40:08.205993891 CEST	85.222.152.194	443	192.168.2.5	49896	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:08.206517935 CEST	85.222.152.194	443	192.168.2.5	49895	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:08.528745890 CEST	85.222.152.194	443	192.168.2.5	49898	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:08.650626898 CEST	85.222.152.194	443	192.168.2.5	49899	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:08.656364918 CEST	85.222.152.194	443	192.168.2.5	49900	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:08.740516901 CEST	85.222.152.194	443	192.168.2.5	49901	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:09.764702082 CEST	85.222.153.66	443	192.168.2.5	49905	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	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=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		
Jul 16, 2021 16:40:09.764986992 CEST	85.222.153.66	443	192.168.2.5	49904	CN=test.salesforce.com, O="salesforce.com, 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	Wed Sep 30 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 29 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	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=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		
Jul 16, 2021 16:40:12.857906103 CEST	54.205.5.87	443	192.168.2.5	49914	CN=*.vidyard.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	Mon Apr 26 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	Thu May 26 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:13.953530073 CEST	54.205.5.87	443	192.168.2.5	49915	CN=*.vidyard.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	Mon Apr 26 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	Thu May 26 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		
Jul 16, 2021 16:40:16.532341003 CEST	34.234.32.98	443	192.168.2.5	49937	CN=*.vidyard.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	Mon Apr 26 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	Thu May 26 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:16.997284889 CEST	54.205.5.87	443	192.168.2.5	49942	CN=*.vidyard.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	Mon Apr 26 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	Thu May 26 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		
Jul 16, 2021 16:40:21.678436995 CEST	3.227.80.201	443	192.168.2.5	49947	CN=*.litix.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 Nov 27 01:00:00 CET 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	Mon Dec 27 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:22.249758005 CEST	3.227.80.201	443	192.168.2.5	49948	CN=*.litix.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 Nov 27 01:00:00 CET 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	Mon Dec 27 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		
Jul 16, 2021 16:40:22.390233994 CEST	3.227.80.201	443	192.168.2.5	49949	CN=*.litix.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 Nov 27 01:00:00 CET 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	Mon Dec 27 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:22.559830904 CEST	3.227.80.201	443	192.168.2.5	49950	CN=*.litix.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 Nov 27 01:00:00 CET 2020	Mon Dec 27 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
					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		
Jul 16, 2021 16:40:33.049267054 CEST	13.110.69.75	443	192.168.2.5	49974	CN=*.my.salesforce.com, O="salesforce.com, 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	Thu Sep 17 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Sep 11 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Jul 16, 2021 16:40:35.184498072 CEST	13.109.191.111	443	192.168.2.5	49978	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021	Fri Feb 25 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 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		
Jul 16, 2021 16:40:35.200506926 CEST	13.109.191.111	443	192.168.2.5	49979	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021	Fri Feb 25 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 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 16, 2021 16:40:35.227864027 CEST	54.225.136.92	443	192.168.2.5	49976	CN=logx.optimizely.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	Mon Sep 21 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	Thu Oct 21 14:00:00 CEST 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		
Jul 16, 2021 16:40:35.714951992 CEST	13.110.41.111	443	192.168.2.5	49985	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:35.730007887 CEST	13.110.41.111	443	192.168.2.5	49987	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:36.426409006 CEST	34.248.156.174	443	192.168.2.5	49994	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 16, 2021 16:40:38.889941931 CEST	13.109.191.111	443	192.168.2.5	50001	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:38.914752007 CEST	13.109.191.111	443	192.168.2.5	50002	CN=la2-c1-ia4.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:39.440033913 CEST	13.110.41.111	443	192.168.2.5	50003	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:39.455190897 CEST	13.110.41.111	443	192.168.2.5	50004	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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		
Jul 16, 2021 16:40:50.347223043 CEST	13.110.41.111	443	192.168.2.5	50038	CN=la2-c1-ia5.salesforceliveagent.com, O="salesforce.com, 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 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Feb 25 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 4532 Parent PID: 5520

General

Start time:	16:38:02
Start date:	16/07/2021
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\Desktop\Denver Water COVID-19 Response _ City of Denver.pdf'
Imagebase:	0xce0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 4440 Parent PID: 4532

General

Start time:	16:38:03
Start date:	16/07/2021

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\Desktop\Denver Water COVID-19 Response _ City of Denver.pdf'
Imagebase:	0xce0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6132 Parent PID: 4532

General

Start time:	16:38:09
Start date:	16/07/2021
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:	0x50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: RdrCEF.exe PID: 3488 Parent PID: 6132

General

Start time:	16:38:12
Start date:	16/07/2021
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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12047842394824068586 --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=12047842394824068586 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6048 Parent PID: 6132

General

Start time:	16:38:14
Start date:	16/07/2021
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=1716,18340769791588095283,14740429863509864490,131072 --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=16938848815433914037 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x7ff797770000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 5316 Parent PID: 6132

General

Start time:	16:38:18
Start date:	16/07/2021
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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=787724751391022994 --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=787724751391022994 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 5884 Parent PID: 6132

General

Start time:	16:38:20
Start date:	16/07/2021
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=1716,18340769791588095283,14740429863509864490,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16674541699487182290 --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=16674541699487182290 --renderer-client-id=5 --mojo-platform-channel-handle=2128 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x50000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6268 Parent PID: 4532

General

Start time:	16:39:24
Start date:	16/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'https://milehighunitedway.lightning.force.com/lightning/r/Account/0014T000004o6JxQAI/view'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6812 Parent PID: 6268

General

Start time:	16:39:26
Start date:	16/07/2021
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=1560,8292458995521785639,16987803382321267150,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8

Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis