ID: 682137
Sample Name: 35
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 05:06:22
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

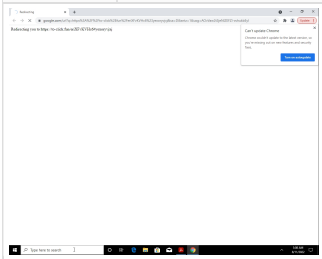
Windows Analysis Report

35

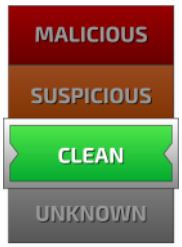
Overview

General Information

Sample Name:	35
Analysis ID:	682137
MD5:	aeada84492f831..
SHA1:	a24677f6a7549c..
SHA256:	e94b94022adbee.
Infos:	



Detection

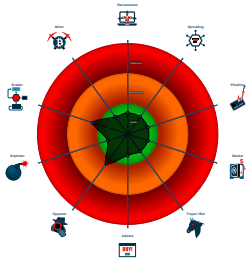


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- JA3 SSL client fingerprint seen in co…
- Queries the volume information (nam…
- Creates a process in suspended mo…
- IP address seen in connection with …

Classification



Process Tree

- **System is start**
- OpenWith.exe (PID: 1264 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: 5D37A62943F1071FFFFE1DE74B8F2778)
- OpenWith.exe (PID: 2972 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: 5D37A62943F1071FFFFE1DE74B8F2778)
  - AcroRd32.exe (PID: 2320 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\35 MD5: 0EAC436587F5A1BEF8AEB2E2381D2405)
    - RdrCEF.exe (PID: 5268 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 4AC861CBCAFA331A72C04BF35AE792E3)
    - chrome.exe (PID: 3932 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://www.google.com/url?q=%68%74%74%70%73%3A%2F%2F%74%6F%2D%63%6C%69%63%6B%2E%66%75%6E%2F%65%72%69%58%46%76%4B%56%48%63%36%23%79%65%78%6F%72%79%76%6A%78%6A&sa=D&sntz=1&usg=AOvVaw2t3jeNlZEFZI-xvhukbEyl MD5: 74859601FB4BEEA84B40D874CCB56CAB)
      - chrome.exe (PID: 6336 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1752,12796533771390455494,5363625801302401924,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2156 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

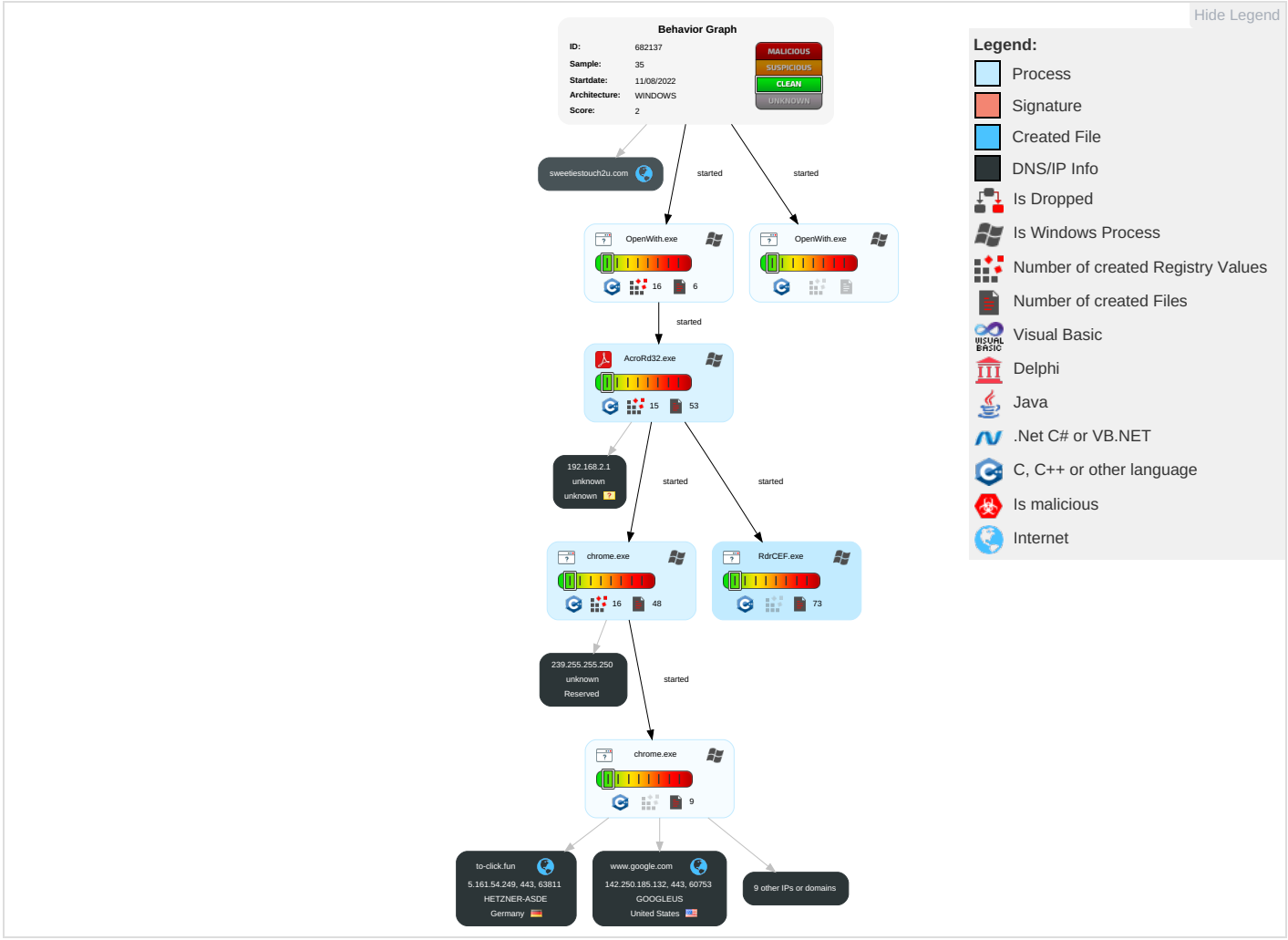
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 1 Process Injection	LSASS Memory	1 1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

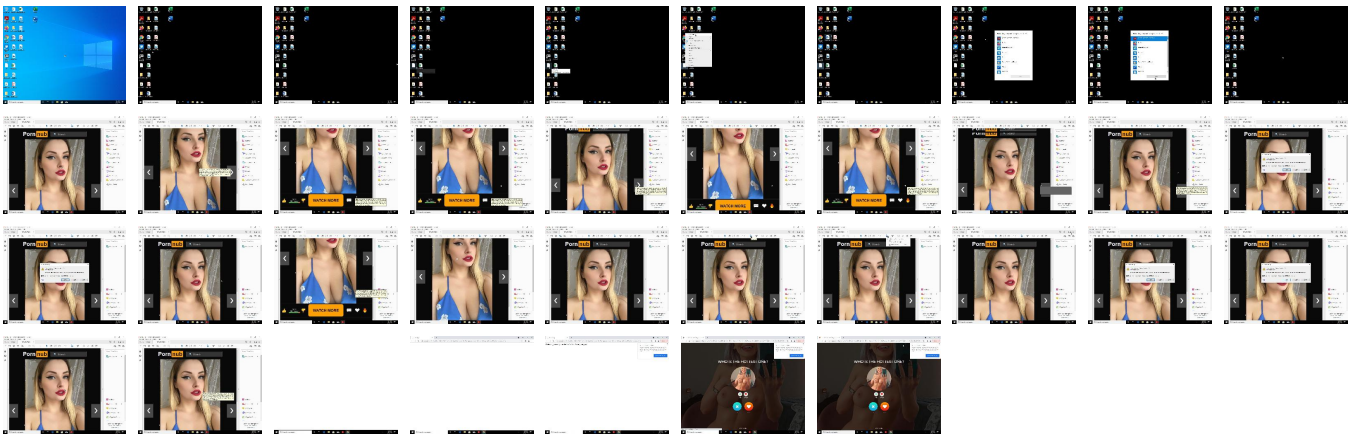
Behavior Graph

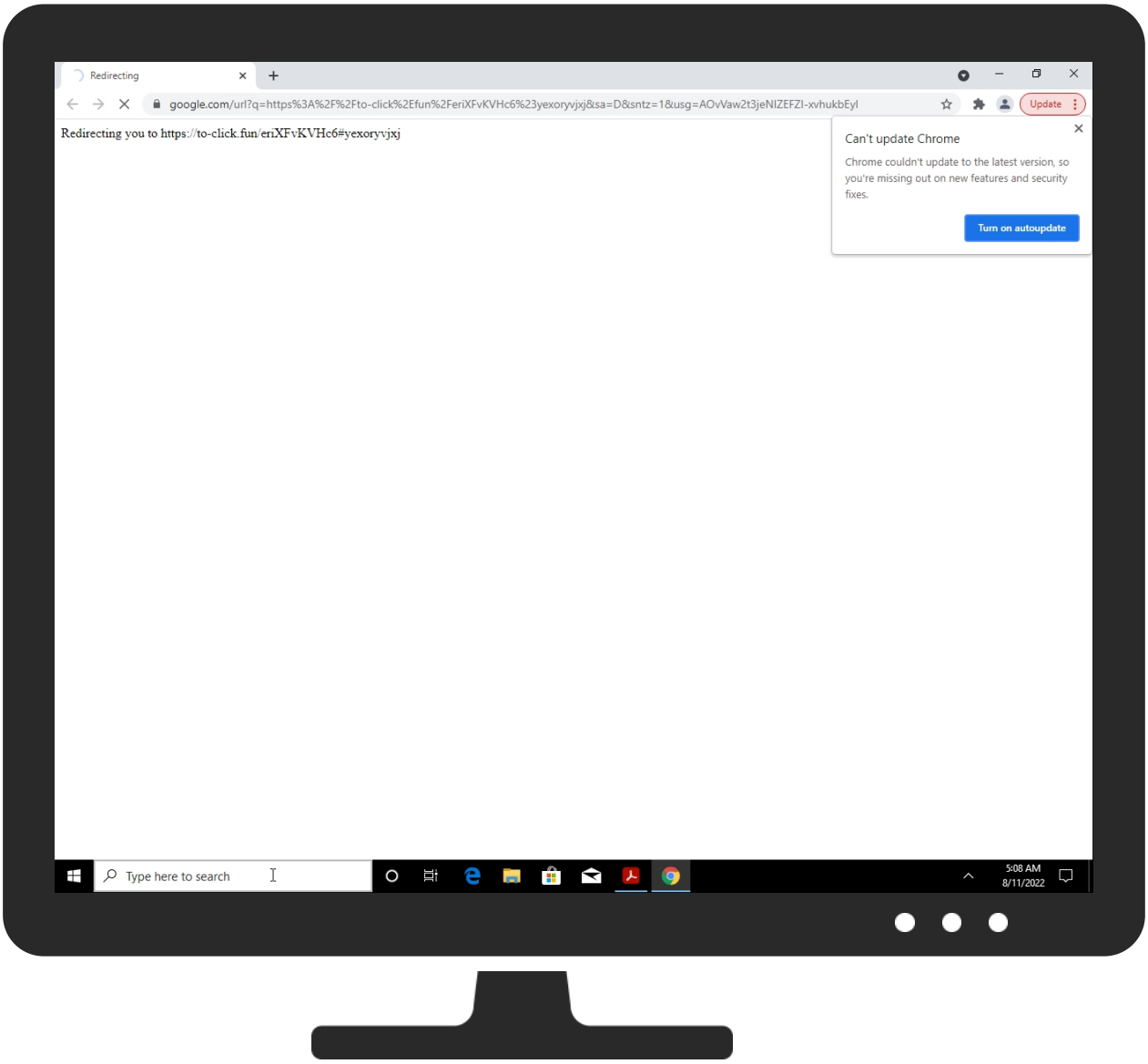


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
to-click.fun	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://to-click.fun/eriXFvKVHc6	0%	Avira URL Cloud	safe	
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart-red.svg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://sweetiestouch2u.com/?utm_source=g3Ase2bbTdNbHV	0%	Avira URL Cloud	safe	
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times.svg	0%	Avira URL Cloud	safe	
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart.svg	0%	Avira URL Cloud	safe	
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times-blue.svg	0%	Avira URL Cloud	safe	
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/m1.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

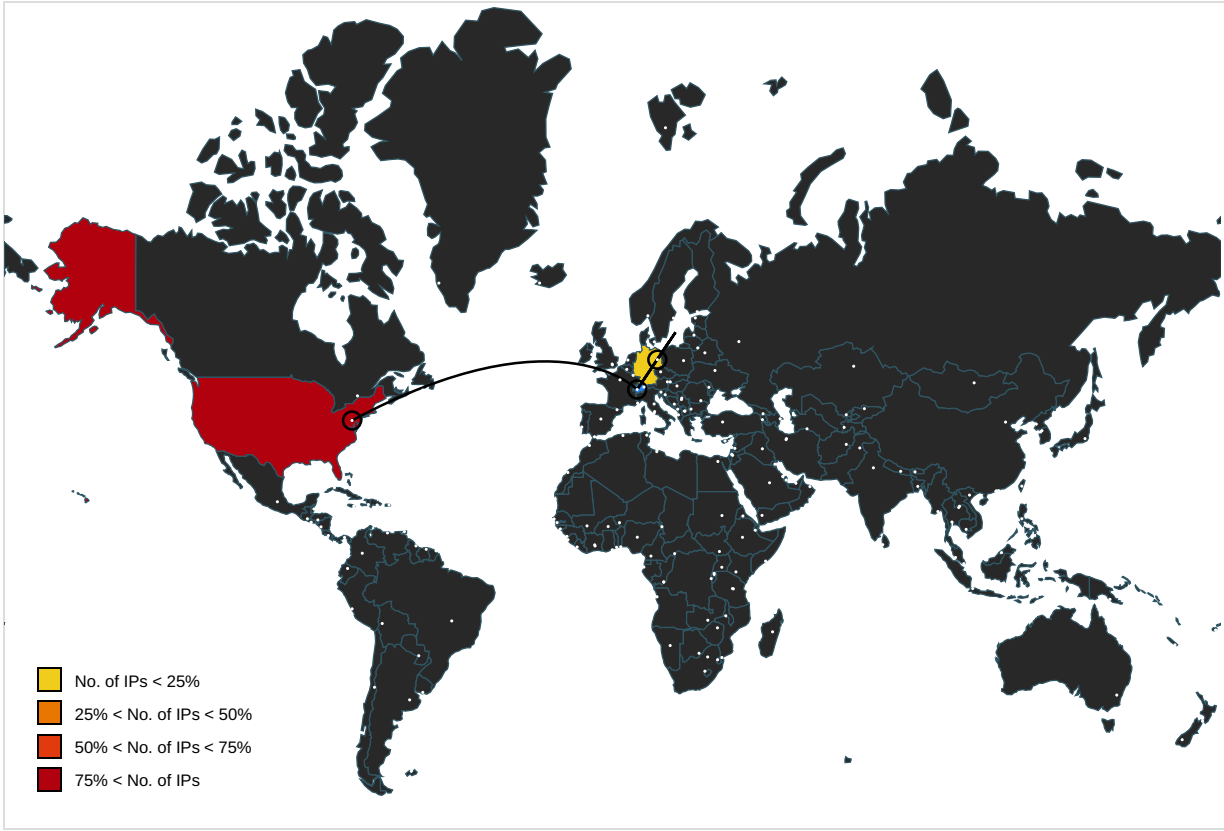
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.67	true	false		high
example.org	93.184.216.34	true	false		high
accounts.google.com	172.217.16.205	true	false		high
to-click.fun	5.161.54.249	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.250.185.132	true	false		high
clients.l.google.com	142.250.185.142	true	false		high
sweetiestouch2u.com	188.114.97.3	true	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://to-click.fun/eriXFvKVHc6	false	• Avira URL Cloud: safe	unknown
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart-red.svg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/url?q=%68%74%74%70%73%3A%2F%2F%74%6F%2D%63%6C%69%63%6B%2E%66%75%6E%2F%65%72%69%58%46%76%4B%56%48%63%36%23%79%65%78%6F%72%79%76%6A%78%6A&sa=D&sntz=1&usg=AOvVaw2t3jeNlZEFZI-xvhukbEyl	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=92.0.4515.107&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://sweetiestouch2u.com/?utm_source=g3Ase2bbTdNbHV	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/url?q=%68%74%74%70%73%3A%2F%2F%74%6F%2D%63%6C%69%63%6B%2E%66%75%6E%2F%65%72%69%58%46%76%4B%56%48%63%36%23%79%65%78%6F%72%79%76%6A%78%6A&sa=D&sntz=1&usg=AOvVaw2t3jeNlZEFZI-xvhukbEyl	false		high
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times.svg	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart.svg	false	• Avira URL Cloud: safe	unknown
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times-blue.svg	false	• Avira URL Cloud: safe	unknown
http://https://sweetiestouch2u.com/?a=1868012&cr=57748&lid=19953&mh=TWpVZHNsdmF5SEF4eWJmcm9BaGdMV1Z6cEVXeE54YXRRUndzRU8tMzU4NzU%3D&mmid=2760&p=0&rf=uu&rn=zc4ZodGUys4WmdeVEhG&t=notrack	false		unknown
http://https://sweetiestouch2u.com/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/m1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://example.org/media.ext	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.67	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
93.184.216.34	example.org	European Union		15133	EDGECASTUS	false
172.217.16.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.185.132	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
188.114.97.3	sweetiestouch2u.com	European Union		13335	CLOUDFLARENETUS	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
5.161.54.249	to-click.fun	Germany		24940	HETZNER-ASDE	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682137
Start date and time:	2022-08-11 05:06:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	35
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	14
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:	clean2.win@31/65@9/10
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

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, CompPkgSrv.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 92.123.224.208, 92.123.224.225, 2.21.22.179, 2.21.22.155, 23.3.108.167, 88.221.168.141, 23.54.113.182, 23.22.254.206, 52.202.204.11, 54.227.187.23, 52.5.13.197, 142.250.179.163, 34.104.35.123, 142.251.39.106, 69.16.175.10, 69.16.175.42, 104.16.87.20, 104.16.85.20, 104.16.89.20, 104.16.88.20, 104.16.86.20, 92.123.195.35, 92.123.195.73, 20.223.24.244
- Excluded domains from analysis (whitelisted): e4578.dscg.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, cdn.jsdelivr.net.cdn.cloudflare.net, slscr.update.microsoft.com, e4578.dscb.akamaiedge.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, arc.msn.com, acroipm2.adobe.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, ssl-delivery.adobe.com.edgekey.net, a122.dscd.akamai.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, client.wns.windows.com, google.com, fonts.googleapis.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, fonts.gstatic.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, p13n.adobe.io, ssl.adobe.com.edgekey.net, armmf.adobe.com, edgedl.me.gvt1.com, geo2.adobe.com, nexusrules.officeapps.live.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:06:52	API Interceptor	2x Sleep call for process: OpenWith.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.635434451938335
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QfPu/wZx9tFflBi7Z+P41:vDRM9YPuIZx9nfuZi
MD5:	0FC1648A0D19CDD69F1792624A33FE7C
SHA1:	EFF08B65B1FF7183FA66F11175A9DA4C75BF9AC3
SHA-256:	10DAD571F7116A7D9ED43F2AB3C4831BC012D9FF5C86C76D55A693151885DBB8
SHA-512:	A81526D3AFBC08A52D0CCA5F05BB5FCAB546FCCC09C27E69CAD62EB78CBF1FDEB723467614A955C39EBAC81107687B9B0C9A69FC3AAA9BD371F198B1E8EE E1F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .(.L.D/.....*. (.G<..A.A..Eo.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.562019634990087
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVyjtzkZQdvRktJTf/e98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEk0tTdatdfy8Be7Ywcr1
MD5:	E372CA140FC18C013D32E8B8C61D0820
SHA1:	147AABD6A034E0B20288647E42B5718CAC474582
SHA-256:	E57DC27FCA6646F3C4168C48097451514721A08FB633F2F6A670472B03E7B647
SHA-512:	584E75219B3EF7C03DF774FA91572C21AEE916CE40334A6B59E323A1ED8572EF130FC3C700FB1A172660BE6652742AE86CE7286535E4903C6379D947F2EF4484
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..&.K.D/.....*...xC<..A.A..Eo.....6.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.5823577315703625
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuZNt/T+jtZt/RlUoSjGY1:DyeRVFAFjVFAF/t7e7tZlUo6
MD5:	08BBA5D6FA3685E725A8A85A791942E0
SHA1:	3901CE7FD8E97E6A09F2BBD65D03D67005BB9E44
SHA-256:	AA72B6018B7ADC65960FD071A184431D6C95A734991C84EE200196851B39E2C4
SHA-512:	70DDEF0F65B21B9860E9D776BBE31A292C0D22A5AC7FEDAB9CDDCED09F01DAB7733E04C56612399AF7BFC378F2BFA470820EFF455D4653ED3EABE4757608A D9C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....L.D/.....*.W..G<..A.A..Eo.....; ;.....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.6824521753619335
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsformfat6zuiWulHyA1:IbRkiD7rmS0zjWus
MD5:	FEAC663BC48FEFD5D95C21F063B18B4B
SHA1:	35A2583B0822F2F27C5F635B52764F28E48C2779
SHA-256:	951B8829C7C98B44DCDE6F1ABDB71C5E16A4F59DD049CF8B369A9DC402B82B4C
SHA-512:	F32E59F0B2A67C75F6FC2888F177C813B4CD759C1134B6CF8112D625F9A525AE93B772944DE3465017706F7A0B07C87C20011BE60CD0F88D32342DFFBCE8FD2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .;..K.D/.....*..8.C<..A.A..Eo...../.^.....8 P..a...R..Y ....7.@..2Dm{..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.55763845470418
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuTf0/ag9jtpXcVyh9PT41:pyixRulsN97cV41T
MD5:	279185060F98815F1EF432CEF7EE7268
SHA1:	32B5A27781F7DFF1B492D37352055394591830D3
SHA-256:	5BB2E85F7CABF8F1CEB77DB6007CD773117DD242C6CB39CBEA4242FEFA50FCB2
SHA-512:	D34C5349C7E20955855DCEA8CFDBE412D737DAFF10AF76C7AEDD10F107D9E8816B34EB84491ADF84761CCE69659923F653744ADE5E387FF7158891AE1FCE9D D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....L.D/.....*..^.G<..A.A..Eo.....t.i.....k.Q.....-_..y.....O...>..1....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.621647904682762
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVcbl/3aj1kRktVBlYo2sZI8xeGvA:mvYOFLvEWdhwjQ3B/8t13ZIl6P41
MD5:	17123792B5E686EE68BAD37FCE5F60E3
SHA1:	EE4C9255DBD6EFF2E25E1EFD4F6A73DAF83712C4
SHA-256:	E1B0E5F3FA9365FC605A8B6DDDFD42CF02309E4685371E5DC1F064A207BBCD00
SHA-512:	16C9230E5F97C5BF3B67F40C7F489A2E050A6A4FB6FCA6783A8F011DFAA54D3F67D67E3A1C23B5F2F887FB01BCB62F6B88E4EDDC44A8AED45C6FE06FC0DE7 474
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .Q@}L.D/.....*..7.F<..A.A..Eo.....m.....].>....uUf..N...k.....c..l.A. .Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.542909074501603
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVJm0//G1zqkRktp9rcyxMtv9G:mJYOFLvEWdGQRQOdQZU/G4jtp1D6g1
MD5:	93FF0FFE0D609077BE05E1C5D1366EA0

SHA1:	FB92DBD0936A856DC290466BDF6E92DB8FC6E31C
SHA-256:	E321FF3BD29429BFD218F9B9E5B978168CA002D5289CBF23AC0AA392C9B0669F
SHA-512:	E4211705A2BEC7AD98A9DD510533FAD8D03E6AC387908EF15663AA4BF0BAAD7A104BADA5D1355CDA48D6621850F8230D8B5E67557CA4C7A71B64B7F66DB36A8
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...L.D/.....*.I..G<..A.A..Eo.....O.J.....c..y/L....|y.n..C/I.....X7-ne.A..Eo.. .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.545880624952299
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVTTN1SGvRkthyQMWqg4nRb7om5m1:mOYOFLvECMLV1SGathruR/41
MD5:	CF63BD82677A14078BB3EAF9BD25534C
SHA1:	FB0A00B86C2984A3127DDABD6C92185B9D6B1724
SHA-256:	6DDE2AF6768EEF51A4F0F91E2CA498AC328F89722FB618D55FC1D187C510E767
SHA-512:	E6407A87379A51BE4BEA5B09588144D472FB076C907B71DD4BA353E11C8748632DA1D6A301712FC54A529D0195052681F1C99C21585BABA6D8427A38FF0A306D
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....K.D/.....*...xC<..A.A..Eo.....=1Z.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.527446012505621
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvfW/9kGvRktL8d1dn76KohyP5m1:md4HXXYOFLvEjMSWFvfW1kGatL8jUdyA
MD5:	050A3FF476D0CFD850A1B1EB965545BF
SHA1:	FBC39A1E39BF83F66DCE4D94F63E71001CD0ED6D
SHA-256:	6626DC26B1A21F35CF8C6B16A0CD8A6560AFC5ED4479C68BFBF1A4DBCD453FC0
SHA-512:	1AF7E8124C97F99AE9A860D1B7DB3E3691F6DADF5F27D7523766A8D501198FC0DB376A5A73049BAAF591385C57419AB79F985AD40FE350A16A24FD8A83FA685
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ....K.D/.....*.7.xC<..A.A..Eo.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4ca3cb58378aaa3f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.57850199545023
Encrypted:	false
SSDEEP:	6:msNXYOFLvEWdpJWNKjQt/ASt0m8E+IUGkA1:BjRpJWNKjeoSN8NID
MD5:	6D57656762F19871944A8E3EFFD5E92E
SHA1:	558B692C025BF35B43AEEF8C797AA8540A528185
SHA-256:	59F7810B9BBF423402D7EA87E7A7504F360941AF713C60A02DB08867DE453439
SHA-512:	EFD4A797CE853687AF01B7E74BF5D23E5BD6D17D536A3E55A6D6B797DBCA2F79783026B532DAFDF938DB20553FFED46E87679F86B26A09F83690EA176AE8D61
Malicious:	false
Preview:	0\r..m.....S...9O....._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/plugin.js ..B}L.D/.....*....F<..A.A..Eo.....E.n.....e.....@-H.>a..o..sh.5.A.x ..C..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

Size (bytes):	187
Entropy (8bit):	5.547910091960451
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLUvKlX/5m9JRktee9t/RUPqf9tsDMaPV4B:mkl9YOFLvEWsfOLceRm9QtzCPqVyM+VI
MD5:	53FFAFEE67839E964C651E060E4170D0
SHA1:	B7BEAA5D18AE683DC27D71C8CBEDCF712B627954
SHA-256:	DD5B0B4084D0B046C545238A4DD4906A53BA7DADD52FCD64AF3D1EB10242B2B8
SHA-512:	8E80D33048BE38B38F6B407E5BF71353569A10D071B406829D1D72D695FB89B21B2A93F900F4A4249A2A8867E5697D5D1B42F2324154AC71FDAB33C9509B476C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .z..K.D/.....*.qW.E<..A.A..Eo.....k.....q.O...j...._y..L^z...?..@N..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.620507343590824
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyzmpm/f+jtttwSeKaT9pr1:URVFAFjVFAFrUeTtwSeKaTL
MD5:	56E7594227269EB5F9575AF4737BDF03
SHA1:	A3DE4E98100B1AD294899562F451051F0E320054
SHA-256:	632F17675075BB32DB5AD941403464B63A9A2CE34D4AF332787E34BB0F7BA895
SHA-512:	AE5F4EFE77455E9BD1A329B2241869BE0E4EFFA3DF211940D0ED27108D2DA9408E0727C860443935476B1A61203B29A95EBAA8BCD858A947CDE4AF0B375E3C1 6
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 .|..L.D/.....*....G<..A.A..Eo..... .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\64766d63a539c3ca_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.586576635498904
Encrypted:	false
SSDEEP:	3:m+lUZHWK8RzYOCGLvHkWBGKuKjXKKINiB4KPEEKPWFvnBK/l/Q/9kRktE01iwIQi:m8nYOFLvEWdfNBHYuut/wjtE0kwU1
MD5:	6B67AA9A50531FE12101D86D84F5E0DB
SHA1:	D1091EA58694809521AEF3E87486441EB969F6F3
SHA-256:	9B969760ED0BF9A494EE2178D6487B825537F034FF4F366F38DCA412813E6272
SHA-512:	0D2767E372350CF7BF47EB5FC2781838FA0FE905CD0A4AD10F5E7F736130B73D5C85F99800050CE0D5ABC7EE904C1B33A2FD1BF89632A5B004D680FF8C5919C 5
Malicious:	false
Preview:	0\r..m.....T....."...._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/selector.js ..*)L.D/.....*.(eUE<..A.A..Eo.....4p#W.....8U-....a=...`#..VT.k.....A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.522001356179088
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuR/kmqjtaq11:BsR2EseQEj
MD5:	65DC11945D7836CAC42CFA8F256933A8
SHA1:	FE5A72CBDABED8766C8E0AC24E328E1019C52F3E
SHA-256:	CD3971E75F8993C731C10C333BF6C7147E50B78A42764DE7390243E9CB8F47FE
SHA-512:	8F16C95F413805D6B9E86D19A6E00B9DD00C1C3FC92E86FDA6740033BC36CF2467D56EEFD0293FB6814A374C80FEC6773880436BBF6DF8BCE2132E3ECEEEC7 7D
Malicious:	false

Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .9..L.D/.....*....G<..A.A..Eo.....A.o]@r..Q.....<w.....].n\....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.655335360298566
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQnB/S/9tN1xm7OhKlvA1:RbR16KalZxmJ
MD5:	B835E31DA7ADA47B408AB8DC3C558EC5
SHA1:	D4EC7607D4AB348C34C66572AD78B08CE282EB32
SHA-256:	ABD7B44C81EDDCB7C1CAD12001D79F3056C1FB11EBF6BA87FC61CE8C12C27DC5
SHA-512:	314714255EFA0FD27628054AB1ABDF070D88C716670D0D3383699AA4EBF3EC60B65522BC4CFFFCF52BB16A42A8A684D730CE291F0B95027F57752B666CAAB20B
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..>}L.D/.....*...F<..A.A..Eo.....~1M".....4T].....Tw.....(..b...EO....9.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.5591350195137785
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVueF/b+jt/nHlPdFt1:B2geRHRQLze
MD5:	1ED295D15027AE22D929F2780953AA93
SHA1:	A2962D40D3F0F5904723EEE7721D93975DC95972
SHA-256:	23DC6307997EC1D2BB263E011144B54666F329B898D318E51B19910180AFC6AC
SHA-512:	F057351D266E751444DBB5A8E9B7DF10B8464CE55471FC3A1568CC81D8A93A9E73F74B3AA1A2484C7FA6CE037CAF5F7CA0D81FA9D62D272723DE262656422EE
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .B..L.D/.....*.c).G<..A.A..Eo.....Y|.....@..{o]...9o|..qY....T....{ ..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\72d9f526d2e2e7c8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.552235842120562
Encrypted:	false
SSDEEP:	6:m+8nYOFLvEWIAuELZRudyPGXuy1079tT9/N0KGkTqcY1:1StuEH2DuyGRX/p
MD5:	706690C90B7750765E419D45A5A17983
SHA1:	B962353A69397EEFB55AE87CD04BFA7D2D21C6E4
SHA-256:	B100CECBBBE9279E9EE179AAD4C27149DF38B30DA3A63F2A4804DF37661D7A66
SHA-512:	E4A02322C53B158E7241FED649E9DD1D939479DEE356F34D1FBB33BCAA6F373752A3BC2F7F5B4B1931EF07D931E3ED4DB803ED82E639145264D2EA779A9A1A4C
Malicious:	false
Preview:	0\r..m.....b.....6...._keyhttps://rna-resource.acrobat.com/static/js/libs/microsoftGraph/microsoft-graph-js-sdk-web.js .G}.K.D/.....*....D<..A.A..Eo.....C.....-.... .5p9o..k#.}..6(..*A...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\78bff3512887b83d_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.594367788571492

Encrypted:	false
SSDEEP:	6:mgEYOFLvEWdpJWNKyunpU/xb9tn21R/xXj1:neRpJWNKnGDaRp
MD5:	BB35E5628B951A95D3672E1FB6D7CC77
SHA1:	C670F4637D2E256370CB7329F15F93867C433F38
SHA-256:	0F3719B410E1C1609C207A8D571790F64ABDB558AA757F1137D4C907491FD263
SHA-512:	93DDAB271E08FAA5E3DB563D3DBA31B8FF94A95DB9ABC44EB3F6FBCC7FB8105FE29766D1542D2C884998AEB53A24A145D907C54BF6C3EC4FA5F12A8888A3D2EC
Malicious:	false
Preview:	0\r..m.....U...r.L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/selector.js .(.|L.D/.....*...F<..A.A..Eo.....=.....U.....&.Y|.. . .&.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.583312616585357
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVa/l/yRktjltuEnNWQ1SUm1:mzyEYOFLvEWdrIOQ5/ltjlIEt1S/1
MD5:	B4A156565B030FBF2E8CEAD01FF85510
SHA1:	34C13731E7D1FFB567ED44F50065CB3E89EC1886
SHA-256:	7110640CFBFE8BA37A3B2EDBC2DED7409484F73EDE9EA6B08E1E43C1619ED1CF
SHA-512:	AD97B39ABED2A5112C7FDF7D534D884AC1FE149A6A8D5B9B260EA1585FA6913E8E4BA561C7B4BDFE7277F73387B107AD41D3E16B1B4E661F0319D1A9D393181E
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...?L.D/.....*....F<..A.A..Eo.....6.....t\a.....x5.'OuE.C..@.....x..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.57819777498227
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyub8l//8StftKlwrqwK+41:wRhE8tLjKqGwK+
MD5:	195E00579710CABF758B1F5A61F56E9B
SHA1:	A07C25C010AADC873D7261408B1ED5B57AE1A8E9
SHA-256:	9D34D4D524997C3A484E665B521C0CB82EB4D4152456A8526E73743B4FBF81AC
SHA-512:	5C2F7F19635C7374620ABBE26D1BAB5B323087D18103F364B5E5B02DCAAFAE90F55F0A2F7FBD99FE82F6DC19284ED529BC77C4FC7D1A1D161CE9A545F3A137CE
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...|L.D/.....*....F<..A.A..Eo.....7.....7...o..a=.98I.....(3.$G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.572460583056192
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuYr/bQtwfO441:/RrROk/FrzQmfL
MD5:	390836E201CC7D88E0959FB5F9D9E6C9
SHA1:	DE99CCDDD4DF9083DAA866AED3F5C5AE7CF28102
SHA-256:	F0CE44E8F13310C26DD19684C136B554DAC7771B7CB62E7BEEE08160500E9646
SHA-512:	D25E09132183C385ABBA84E539F5E49206EA05B6025BDCA41ACB95CDF148B3AECF2821C86F66BB4C71209FADC1F196DCCD3185E7DCE0961B35FC16C44084846
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...?L.D/.....*.V..F<..A.A..Eo.....rd>.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.526781977017839
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVVJUXV1kRktOllRzoIN1OFPL4m1:mmDEYOFLvEWXlsV1jtO/RzV1QPLr1
MD5:	30CA0345342B8B7BE39E192AF6D75702
SHA1:	614614917968FA857440D1DD39DC103DB1FB19B3
SHA-256:	B6DA6D08EA5CA0D2761F2784D8CAABB5A3F2978FB335188B9FF45ECB9179BEC9
SHA-512:	39A12CC6C9545FF2E9C75CC817EEA852477EBD02C7EFE0DAF2C43B405B410A02EBB9AF7524E02DE365CFCB40C7739C74B931CFF84E6E9949372D36F3DAC4C DB
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .IQ.K.D/.....*.)..E<..A.A..Eo.....E.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.61595679962136
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAud4u/TmqjtvFluEvsEJ41:zRMwub1jdvs
MD5:	8C7C1ED241A452EC5BD562069FEF991E
SHA1:	A63FDE23AD76E6E4C9A501E87F466524BE46300F
SHA-256:	1F6DADE0FBCBC0D0D1D59FD23A85BE24D229271CDCB41A8D1153B24AB0772935
SHA-512:	F65931359674F66551BE98C4953B43748DCC5635A31CD48916B73A779995616A3CBC4E897DD8CD89C4F67840DC589BB1971782B6024EDC24BE5E6485905BF7C
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...L.D/.....*....G<..A.A..Eo.....Po.H.....z._a...'.v.....4p3..1.']...A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.580403783519067
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuf/6x9jtIyong1:6lJRWq9uyo
MD5:	8E794FCED23D980D64F125498EF93EC9
SHA1:	AD01B1A525B08B96318C7BEA6A2B3A21AC3A1463
SHA-256:	A4F7EE6CB6E9FF011368CF8BD7A5AD57C2EF9F7F6BEA1E722D220295EB580A1A
SHA-512:	4F1E29F802EF786FFB22F28B5CD47B4EABCF8EB71036CD69328F17C75723DDAC9D9C017F22C793D867153A20BF08D38260EF1E668C95AA27986A1675AB7F0F4 A
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...L.D/.....*..:.G<..A.A..Eo.....L.....c}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.569551435228624
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/lu4/WYStr1N16wG1:F8hRrROk/eufhP
MD5:	6DC3621BD62F7709719BDA86EF57D533
SHA1:	302D67ADD60C75FC3D37965072A2B54B9CA57419

SHA-256:	C3E0EBC75F0A8E55C98CB9084119D41A333BF23689EEC88FD69781165AB80CA6
SHA-512:	C5BFE7DFB6E960AF4BB4E452ABBA7B8CE74766F7DC20A4B0EAE19DBFC11294D60DCC7CBB4D80D70AB9E7A088B01C795B9EA8A490392B1CB4801862A29B721D48
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...?L.D/.....*.:[nF<..A.A..Eo.....%.k.SZ..~W.....:)'B..ad.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.668873581676799
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQVH0/Kst//QeJIi1:ehRcE0zp/QeJI
MD5:	839649E9C0240218E5052D68033DD4A8
SHA1:	769996247EE753009AFA72C588C856CBE643FF9E
SHA-256:	EBEB4DBA13AF9ADDA59717B6C2BBA40D962EA86942D0385CAF8EB6EFB42CEA89
SHA-512:	E3D8AD1FC72E3B8975DB1A48AEE472EE5605E5E6959CE06D5DAD33E84D1A75268406807724F67A1B77A56DCC713E13C872D8125D8B65D28DA3134D3BA887E0D
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...?L.D/.....*....F<..A.A..Eo.....T''.....;"./N_.,.:C..2....9L.H...3:...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.590082967511287
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvKcCl/F0kRkt/mtP6mgmOZLhT79:mOEYOFLvEWdrIhu8/6t/szgm2d/1
MD5:	8C13744E08A423AA6DDBEC08730265C3
SHA1:	34A5A4D71D15FBEADAC7B0CF314030B08654CDB0
SHA-256:	0E13EDD53705B1FBCADE5F89C2D88818006E87F2CB0E199A75F90319FC704CEC
SHA-512:	2576209F48147D58187EC73AA4436E2DA87262B78ED002402061CB6CE0A09DCCD517D6A9B1D8354398CE23A7DF390699EE6189AE45EE446D49C03DAC507FDD3
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...?L.D/.....*...SF<..A.A..Eo.....5*.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.595682095033529
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cvuhe8gvRktf90BiaQ562HvpMm1:mAElVYOFLvEW1K/UBatfjx56uvp1
MD5:	7E9109EDB73E8CEAF50220E94F9F4F49
SHA1:	790D6935AF93D0D229476AE4428B4583267C3112
SHA-256:	497BA6662D2780F261751DC5A6A6B179C6D8BBAA431C3D74C35588281A64C8C9
SHA-512:	A6CF1FCDB585B1192A6B15AD0322B1C3CC4788784C183CC39E30F35FD4908448FFE674E0400A931301EBBEC68BC326F22B97AE7B322BD407A8A803186C159A1B
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .8..K.D/.....*.m.C<..A.A..Eo.....E.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.636307178682704
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuhmKt/yjtlUDLYtmOZn1:xRBJFKtCgDcFZ
MD5:	C29F2044C1981D5381E6A8A9E823344A
SHA1:	569775C5CD26F9DE067EB4FBB646F639ACA9F7AE
SHA-256:	47927D938543A71FA7B855A55AFB710BED3CDC403648227CB8401D3AED492CFC
SHA-512:	628E5D9CA647E457303C5D5ACE572519284ED4489FB4CD2D467B7ED16FFD72E0B84F47C930E85F429004F4EE6640916F79B353E910820D76631EA93CC9C7EBA
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...L.D/.....*....G<..A.A..Eo.....m.....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.600234493840769
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFv+c1mXuvRktaH//npSKGoS6:msRPYOFLvEWIa7zp7TUmXuatCX8VPu1
MD5:	E7D279DFA39305E28BDD93110806EF57
SHA1:	C91BA68F80EB14CE7918FA7AA7D1AFD77B0EB4F9
SHA-256:	16F08A54EE9A7669FF688B4C56F69941A985FA706133B9FFF2612D1564D9F4D1
SHA-512:	5DBA09C9C7E5A7C8A76B9B8257F2CEBBF5983BE09B7763CDA4C748B86DC6C1AC354A64EBC2909641E66ED1979E52C2D1BE02EBA10CAFADA6192B298E925F3 27F
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .:..K.D/.....*.{.yC<..A.A..Eo.....L...Im.@.....E.nW...IP..A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.642636467126913
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQjU/aetljBRCh/41:XRc9WUSevDi/
MD5:	01A3C06868C8270E2D89AB5765BC2C5F
SHA1:	D2A448D684FA0C1751C5C4E67815312F3865D01E
SHA-256:	4FCBCFFEEF5E8D6BC9A3CE03C2102A53706BB3F89B4CF042956129 91C2EDFE13
SHA-512:	61CBE5910973A2DC82B76F14956F1E11ADBAE95ECB4E4C372AF53BD9C3F8C4DDDFCB5E95C7BCA0536DE2A56976F47075C20473395B3A00C06B3D9B7161BDC 4BB
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....L.D/.....*....G<..A.A..Eo.....(.4.....PJm...0x.x..RD...BB!@5..<..]. ...A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.607121931276159
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu7hWNkatokULlF4r1:bs6xRkiZAe7LlF4
MD5:	000925A60CA011E904F39C0EDFEC4214
SHA1:	9151BEA33E8E7143C0454099F1EFA41494A9F592
SHA-256:	DFAF167FB5910856AFED8AFD70CCB208AC044F582E216510B239ABA5D978C626
SHA-512:	F033B749870CFEE614A8A19A23C985A5A1C6F1A768CFF5FA0279A4E21362571700C0EE08567C9D2FCD4C4BF961BBD2016CC46CFE5831768AE777B9E538A042A 0

Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..u.K.D/.....*.a..C<..A.A..Eo.....S.....P...#4..l....5...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\e58e492b0f04240a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.639082445030783
Encrypted:	false
SSDEEP:	6:maJYOFLvEWdfNBHvdQ9/Uz7jtnMzPne7cV6gr1:v/RfTHlm8zfhgPneYU
MD5:	DA36C2643C7733D19F2BA281720A5B87
SHA1:	373AC6FB69D32E3DB614C9BB465276BD17F11D99
SHA-256:	E979043A5B5DFE69C1BA1A67F409D3FED6B1CEFB75BD3D715186BB5376E8DC11
SHA-512:	D37EAC1F2FF853FC4A632950F9BDF904E9D103DA4A6D905A4CAD4A9F5896F30ADBD24F182AE7B2AD966796BEDCD9B659204F32D55F5BEBAAAFEFF6AF7C6A8885
Malicious:	false
Preview:	0\r..m.....R..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/plugin.js ..B)L.D/.....*...UE<..A.A..Eo.....-.6.....E*).*^.!..C.....G..#.&)A..Y..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.603369443093073
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Qf20/IzltN/TuA424r1:+RQn0gzlGr
MD5:	22308FCD38E6D4B13CF07BBBC4F00906
SHA1:	0EE4B2E4CE95C74123D0DCDDB3D110AC642B4E5A
SHA-256:	96CA11F0C3F9A4295AFF62DEEFA7ACA2E289EDACB8753BC7D9FF9917497FAE48
SHA-512:	41B36ED6EA10FEB325BB24668F0A59B36D235FA9143140883B7F92F8D639EB0ED66ED4CAD604807AA5CC76DC7E14CEA7C7ECC2ED5851546EA30F243F058870FD
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .`.L.D/.....*..t.G<..A.A..Eo.....}Q.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.607621556385136
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQ6Pu/T/9tn/sLmB41:nRrROk/VZuT91N
MD5:	D2F9687B611CA6C6890F121E29CE6A7E
SHA1:	E5939D3CA495C99B99C6D9FC2806ACCF84FA65A2
SHA-256:	3B21CBCADF763958AAF52C9467819B7ACE75B09FB169C4C254532F7CF976D313
SHA-512:	D60312FA9542B786C093E9DC2BD5FD5B10A5B2D1FD4C682A722DF895383955A3D21E330D3F26A9FDBC903CA683163BC61C515E098AF90EAB32D6241C82ADA1D
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...@L.D/.....*...zF<..A.A..Eo.....~.(..... ./.ev.....N~..6.b.....$.j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210

Entropy (8bit):	5.597206313985681
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuvDpm/X7jtkDdm9741:qxRct1mPfuDdu7
MD5:	873D0B25AA40C41A7397589C450C97A0
SHA1:	894AAAFBAE8C1532D949CF90B73E68EE7856BD40
SHA-256:	CD15C568E5E7E02092DD0E4C0FBA015EF835028EE3E26F9843031A0765AEC810
SHA-512:	E284A528350A93D62302CB1818EE2457F90C21EF1ADB04115C154FCBFFB96F9D64A9758AAFA84CF0DD6F8D8200FD38D8114A480FE642BDF35EE406024529B10A
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js . ..L.D/.....*....G<..A.A..Eo.....U...I.>P...X...x..0U.~;m.x.k.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.572027737729142
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuLU//QYStpXOB6Jn1:2R1//IffJ
MD5:	E2E764BE6F225C3113AC9B0271F67D01
SHA1:	9933CD2750572E28C949D393BA6D7917D69EF56C
SHA-256:	D402E87048C6392845EFB0BD541B438EABA09BC28297518F6CB2166CBFE9F537
SHA-512:	5FE3C62235E38BBCBFE8076FE15D98B8BB214A4768D946383371CFC3FF38CA2030E96868F19779423C8AA2299C8574D9993C0D9FB605C0B8AA5C9C585A8D9EEF
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...|L.D/.....*...F<..A.A..Eo.....%.....k....F..D..O.n;[.1m.....=..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.603634766077206
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQZzyl//sRltlc3Me/1:3RrROk/sqzytU3y
MD5:	EA2B030FC6E0B5AC39C7FB6EC6DD4790
SHA1:	B28248B4B78650464B98B895679E68913E450C67
SHA-256:	FA5EF028B53C9F879A95B07A4C0E440CBB91A8289D639DAE728806157B31D8B8
SHA-512:	CE3C9ED022ED85DCEA7E03AB8D85E96D0FE54C39E03A7443295AC76FA9C04B68D1B6839CF91B6621A3AEF4A5CA3CB7984B25C5DD69879251DC9CCDF2C9074ED
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .M.@L.D/.....*..&.F<..A.A..Eo.....d.....9Q].8O.z....=..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1008
Entropy (8bit):	5.166450275841842
Encrypted:	false
SSDEEP:	12:0b3Rya/CZ5tA2Lc1XwL/SvpMzeczAqjTukUbBXyK2v/MnGIw5LAnKlEuY2dgHU:0bByhrW1I/0pM7AqjTuVxyNspwBposIU
MD5:	914F51E7C48AAF43AFF1DED9814D3075
SHA1:	554E2B48B13F877771F0E138CCAB84007A9A7B5D
SHA-256:	D4639E83AF6D4A22D3DDA52EB7F895010C6B369AE08946E92391035C659C2D62
SHA-512:	369969ED57AE268C2665587DEE8C739FE692B22E9DE833868338694952FAD3FB73994D94BD85C3EB120880F84760D886FE28A215318B4B85A138E6FC4EFC31D8
Malicious:	false

Preview:	.....oy retne....(.....P.....*...:qL.D/.....;.y~A..14L.D/.....9.cmvd@.$L.D/.....oB*...K.D/.....#...(....."/.....D.4....L.D/.....[.i..%....L.D/.....k7 A.@.aL.D/.....]...I....K.D/.....,+..._.#.:qL.D/.....<...W..J...K.D/.....2q.....qL.D/.....P....V.14L.D/.....!...0.o...L.D/.....P[. q.:qL.D/.....~.,.4>....L.D/..... ..&..r...K.D/.....3....:qL.D/.....v...q.....K.D/.....a.....K.D/.....C..M....."/.....6<\|.....K.D/.....K.D/.....$..+I..@.$L.D/.....F..=z;.@.aL.D/..... ..o.@.aL.D/.....:..N.A...:qL.D/.....Gy.'.h..:qL.D/.....:qL.D/.....=..(Q.x.:qL.D/.....?..7X.L...L.D/.....q....L.D/.....u\]..q...L.D/.....o..k.....L.D/.....*.. .....L.D/.....^.~..z....L.D/.....+.{..'...L.D/.....A?.2:.....L.D/.....=....m.....L.D/.....+.U.!..V...L.D/.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1008
Entropy (8bit):	5.166450275841842
Encrypted:	false
SSDEEP:	12:0b3Rya/CZ5tA2Lc1XwL/SvpMzeczAqjTukUbBXyK2v/MnGIw5LAnKlEuY2dgHU:0bByhrW1I/0pM7AqjTuVxyNspwBposIU
MD5:	914F51E7C48AAF43AFF1DED9814D3075
SHA1:	554E2B48B13F877771F0E138CCAB84007A9A7B5D
SHA-256:	D4639E83AF6D4A22D3DDA52EB7F895010C6B369AE08946E92391035C659C2D62
SHA-512:	369969ED57AE268C2665587DEE8C739FE692B22E9DE833868338694952FAD3FB73994D94BD85C3EB120880F84760D886FE28A215318B4B85A138E6FC4EFC31D8
Malicious:	false
Preview:	.....oy retne....(.....P.....*...:qL.D/.....;.y~A..14L.D/.....9.cmvd@.$L.D/.....oB*...K.D/.....#...(....."/.....D.4....L.D/.....[.i..%....L.D/.....k7 A.@.aL.D/.....]...I....K.D/.....,+..._.#.:qL.D/.....<...W..J...K.D/.....2q.....qL.D/.....P....V.14L.D/.....!...0.o...L.D/.....P[. q.:qL.D/.....~.,.4>....L.D/..... ..&..r...K.D/.....3....:qL.D/.....v...q.....K.D/.....a.....K.D/.....C..M....."/.....6<\|.....K.D/.....K.D/.....$..+I..@.$L.D/.....F..=z;.@.aL.D/..... ..o.@.aL.D/.....:..N.A...:qL.D/.....Gy.'.h..:qL.D/.....:qL.D/.....=..(Q.x.:qL.D/.....?..7X.L...L.D/.....q....L.D/.....u\]..q...L.D/.....o..k.....L.D/.....*.. .....L.D/.....^.~..z....L.D/.....+.{..'...L.D/.....A?.2:.....L.D/.....=....m.....L.D/.....+.U.!..V...L.D/.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.177607025503601
Encrypted:	false
SSDEEP:	48:7ME6ioloiol2ol1Nol1Aiol1RROiol1jol1Cioeol162iolVMzqkmFTIF3XmHjB6:7asfMRXp+89IVXEBodRBkO
MD5:	7EE87B1C99C2EE4E77875AB4B055BA2F
SHA1:	06013EED1A5ACB0DD9AB1002B5CD0A7131089750
SHA-256:	CBEE633C06DFABD7D8DC689A9049252A1B0E8BE68A91F1A17209C349D0F25381
SHA-512:	9B1E8D814B14D757B00801C9C9450836475AD0C88CBAE31ECF26EC10FA7F9F62DFBAEC1115882597A92F2AF11CBAFDA726132A9FB30C7502E7FB55C79964DA F
Malicious:	false
Preview:	.... .c.....U..... .....h..... <.....y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1552

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	100680
Entropy (8bit):	5.198735236005732
Encrypted:	false
SSDEEP:	1536:feNgjRoaRlQShhp2VpMKRhWa11quVJzlzofqG9Z3ADWp1ttawvayjLp:G6jyaRlQShhp2VpMKRhWa11quVJa
MD5:	7077109515BD1FBF8EDB99EF26177642
SHA1:	5B69D757ED47A4CB08FD25CA697F01F19D05DBEC
SHA-256:	4965B1A9DBE3A95B647CDBF287F1CAFBA299BA98FCAFC459DC67BD2C255E411E
SHA-512:	79817D47F9CAC470E574CD7040754A70773D94BACD853D39F5AF0AB0DDFEE8BA273BF7485B9340BC10BB7EC198AB5701B2C0671F8ACA2B91DF392BDE0D563 63
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1, Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Ar ial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength :1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName: Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Ro man.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	100680
Entropy (8bit):	5.198735236005732
Encrypted:	false
SSDEEP:	1536:feNgjRoaRlQShhp2VpMKRhWa11quVJzlzofqG9Z3ADWp1ttawvayjLp:G6jyaRlQShhp2VpMKRhWa11quVJa
MD5:	7077109515BD1FBF8EDB99EF26177642
SHA1:	5B69D757ED47A4CB08FD25CA697F01F19D05DBEC
SHA-256:	4965B1A9DBE3A95B647CDBF287F1CAFBA299BA98FCAFC459DC67BD2C255E411E
SHA-512:	79817D47F9CAC470E574CD7040754A70773D94BACD853D39F5AF0AB0DDFEE8BA273BF7485B9340BC10BB7EC198AB5701B2C0671F8ACA2B91DF392BDE0D563 63
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1, Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Ar ial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength :1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName: Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Ro man.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_READER_LAUNCH_CARD

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.353593556718844
Encrypted:	false
SSDEEP:	6:YEQXJ2HXfMxyuChJ2iS5R0Y9VuoAvJfPmwrPeUkwRe9:YvXKX2yuChExhFGH56Ukee9
MD5:	C6CECBE9B2472FE10F81513600A2BC3F
SHA1:	40CCA938288C71C9845BED7B576B48EB87554460
SHA-256:	8C7527259402E31657C7C941755B5D664BB498A8AFBA655D14F0444C095C85E2
SHA-512:	D4168FE007DEF4C692147CC9BFEFD65A58B424FC42D417146346ACCE8D054F2D4C74AFD65EDFB0B4D56E8BFBE1AA4057B63B5ECF0D1338077C43EE63675F3 C4
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"a28db9a3-e858-49f7-ab71-3cbc7041711d","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"ex pirationDTS":1660363011691,"statusCode":200,"surfaceID":"DC_READER_LAUNCH_CARD","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Banner

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1393
Entropy (8bit):	5.766567882008705
Encrypted:	false
SSDEEP:	24:Yv6XUVurLgETZycPjFmaR70Oa+NCdaBcu141CjrWpHfRzVCV9FJNsn:Yv+HgALwafEaB5OUupHrQ9FJ+
MD5:	6655DB5D36CFD5C7B46B2CDFF9B41BB4
SHA1:	B297982CC8DC4B5486F6ADDAAB878FABB531AC9B
SHA-256:	119FFD5FC4574A7F2566A10954E2735DDDA5F1960FDDC7CE20D6D666108CEC53
SHA-512:	5D61400DA2C304595B66C52D612324C9C8009A763DBDE680CA74BD38AA8CEFACC0B1F8FDB3E13DBDA87DD46B2519BE7EFB7E32CE1463C4A26F86196EA9C2 F4D
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"a28db9a3-e858-49f7-ab71-3cbc7041711d","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"ex pirationDTS":1660363011691,"statusCode":200,"surfaceID":"DC_Reader_RHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_RHP_Banner"}," containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"35216_95523ActionBlock_0","campaignId":35216,"containerId":"1","controlGroupId":"","treatmentId": "0acb9735-71e6-49b8-9dbc-deee7ad1bbc6","variationId":"95523"},"containerId":1,"containerLabel":"JSON for Reader DC RHP Banner","content":{"data":"eyJdGEiOnsidH lwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctRGF5IFRyaWFsIiwiZ29fdXJsIjoiaHR0cHM6Ly9hY3JvYmF0LmFkb2JlLmNvbS91cy9lbi9zaWduL2ZyZWUtdHJpYWwu aHRtbD90cmFja2luZ2lkPVBDMVBRTFFUJm12PWluLXByb2R1Y3QmbXYyPXJlYWRlciZ0dGlkPXJocGlwbV9zIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaX plIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjEyIiwiZm9udF9zdHlsZSI6IjMifSwidGl0bG

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Retention

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	287
Entropy (8bit):	5.301420718679317
Encrypted:	false
SSDEEP:	6:YEQXJ2HXfMxyuChJ2iS5R0Y9VuoAvJf21rPeUkwRe9:YvXKX2yuChExhFG+16Ukee9
MD5:	B6235642AE081CB817C043EC6D2FDABF
SHA1:	05319B41F7E9D9C9F87A6114583ADF42398F1262
SHA-256:	D858BCAE57E181CB46D58568E3985EE678BBE0A149062BE4CF0F79E810E33071
SHA-512:	0C56B09E64D3485ACED738B13FEE011E2CED513EAFDA92D260AACE9C4245A4C6661517CB2DBFEA03DE15467939C5F44C730A0D346A835A4BE6F2B0518689A8 5A
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"a28db9a3-e858-49f7-ab71-3cbc7041711d","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"ex pirationDTS":1660363011691,"statusCode":200,"surfaceID":"DC_Reader_RHP_Retention","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\Edit_InApp_Aug2020

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	782
Entropy (8bit):	5.369816927339013
Encrypted:	false
SSDEEP:	12:YvXKX2yuChExhFGTq16Ukee1+3CEJ1KXd15kcyKMQo7P70c0WM6ZB/uhWQn:Yv6XUVr168CgEXX5kcIfANh5n
MD5:	33F004535DB04C103CA5D561896B995E
SHA1:	523E035C7415B46436E279CBA5BA856C2481B8AC
SHA-256:	CFBFE172F7C20A0129ED1111516B5390919A64D4913C61252598DEE6366688FE
SHA-512:	9EAAC5A1132567E3275A44EBD822E449F15E05C499DFDA0D66A905D3A2277586F0E3DDAC8F315A99A098920AAE2E02DAB3FE67C85850744542C1DF351A77810 A
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"a28db9a3-e858-49f7-ab71-3cbc7041711d","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"ex pirationDTS":1660363011691,"statusCode":200,"surfaceID":"Edit_InApp_Aug2020","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"Edit_InApp_Aug2020"},"containerMap": {"1":{"containerAnalyticsData":{"actionBlockId":"20360_57769ActionBlock_0","campaignId":20360,"containerId":"1","controlGroupId":"","treatmentId":"3c07988a-9c54- 409d-9d06-53885c9f21ec","variationId":"57769"},"containerId":1,"containerLabel":"JSON for switching in-app test","content":{"data":"eyJ1cHNlbGxleHBlcmltZW50Ijp 7InRlc3RpZCI6IjEiLCJjb2hvcnQiOiJicm93c2VyIn19","dataType":"application\/json","encodingScheme":true},"endDTS":1735804679000,"startDTS":1660187271729}}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:e:e
MD5:	DC84B0D741E5BEAE8070013ADDCC8C28
SHA1:	802F4A6A20CBF157AAF6C4E07E4301578D5936A2
SHA-256:	81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06
SHA-512:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB 1
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	767
Entropy (8bit):	5.091757984257626
Encrypted:	false
SSDEEP:	12:YACTTqVUMJt8otjMgtAk3QjNodA+HsoFjA5jUWGvB4WijhdsqxBoUjCnONs:YACTTqV2irgpP+Mak5j1s9iUubWOG
MD5:	E13684FD76A7B87580DFB3AB684891EF

SHA1:	235527C627188290E46410BFD667EC8C671B36CA
SHA-256:	ABC921F59A715DC126CCA054B644D08A6665AAB513AEB8FF051757A60EA32644
SHA-512:	647239A32181ED47C31807689404375917B41CCF4317F7F424CE6750CA14CB0FD91EB37406DD425F18914158C12D6A247C3F4B801EBBF05A01C66C8C10DA7519
Malicious:	false
Preview:	{"all":[{"id":"Edit_InApp_Aug2020","info":{"dg":"0163756bccfa2ce33c017cc1522bed81","sid":"Edit_InApp_Aug2020"},"mimeType":"file","size":782,"ts":1660219687000},{"id":"DC_Reader_RHP_Banner","info":{"dg":"ade49c9634d810f5e0842285f419e684","sid":"DC_Reader_RHP_Banner"},"mimeType":"file","size":1393,"ts":1660219686000},{"id":"DC_Reader_RHP_Retention","info":{"dg":"64e8b5bc2e3df2c4db521fb34ba50365","sid":"DC_Reader_RHP_Retention"},"mimeType":"file","size":287,"ts":1660219686000},{"id":"DC_READER_LAUNCH_CARD","info":{"dg":"57bfa6a21681c68819a502eb5593c7ef","sid":"DC_READER_LAUNCH_CARD"},"mimeType":"file","size":285,"ts":1660219677000},{"id":"TESTING","info":{"dg":"DG","sid":"TESTING"},"mimeType":"file","size":4,"ts":1660219647000}],"g_info":{"Version":"0.0.0.1"}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\90ee39b9-898c-4bbc-84a5-b3abe0dbcf95.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):	115777
Entropy (8bit):	6.032929733000421
Encrypted:	false
SSDEEP:	1536:NGWYBRYGI1pneBQOwQgdWtxwXcBxA1wqW23vfhPwDlLeSfhCsjUtjOjXMWe1:NCj2QyQgd2xNBIwqn3vfh2lvRgyjXC
MD5:	549D76754A5BFFB6B274ED5E03095283
SHA1:	758028EDBF578FBFE4AA52E5CFAAD15F64FDC91D
SHA-256:	C4E56759663F91C8A639EAB1EA4707AF9DA377BC4CFAF7DBB9F70405CAB35D91
SHA-512:	04D64B6F57B0147FFE750C04C4FC42A6120D3FE2D638ABC9AB2F5FF541078786C0ED5498F411EFBA7AB2E44AFA414C8CCDFB9B1B0BD99E4D29D3F713700453A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.6602196934909 09e+12,"network":1.660187295e+12,"ticks":246420290.0,"uncertainty":3722295.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13304693289712948"},"profile":{"info_cache":{"Default":{"active_time":1660219692.015397,"avatar_icon":"chrom

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):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXSoWA0:+g
MD5:	FA7200D6F80CD1757911C45559E59C0E
SHA1:	89C6E99BAEC4EBB3E9A97B928FB473D1498EBA88
SHA-256:	D9779EA4D6DD544A23C2A1C53146B6A4E596927F47DFA0680B0A7EE751D43BB2
SHA-512:	71D9B2DA8EAF404063D918812BA61C3EFB6A23A283B0332180A38C8137FBB21D7977C008D5A57A74469776945CD4ED42C0BCC09F923EDEC52D8F7FE90FA2D14
Malicious:	false
Preview:	sdPC.....A.>'..M..,,-.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64a655de-b89f-431e-8e35-acaadc02e727.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):	16478
Entropy (8bit):	5.570931318876065
Encrypted:	false
SSDEEP:	384:/obt+LlUXU1kXqKf/pUZNCgVLH2HfEVrUVCW74y:jLlGU1kXqKf/pUZNCgVLH2Hf6rUt7h
MD5:	475D05C6AFA5FCB97A38D605CBB7AEF7
SHA1:	E96ECF2EA61B529CB20C0876154856D4F22F9FFB
SHA-256:	DC1A0364CD0EBA82D95BA71D57322BD19531AA9CAEBFB5855B5A881FB309A27A
SHA-512:	1A06414B46CC60B37C2C99469375AC4F7D7588302C32AB25B034B0A39A5FF8A34D5E43F63E48EF45B3F6911FCC5FC875557FB4C604AA0AC47717A15B5E3D196
Malicious:	false

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304693290415902","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
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):	7103
Entropy (8bit):	5.017534883414716
Encrypted:	false
SSDEEP:	96:nrdyr1KKIzTRWMoi/R5mdeE3kKX1505hNObbHVk7MV1ZXJJExMAiZw4:nry1KHWM/G3kKXj0HebH2QLEw
MD5:	58FB7B9F0BD816F6DB20341ABC0A960F
SHA1:	005E25409B6F648D505AB2AEB5A68DB41B54D275
SHA-256:	4EEEF82D60C4C2393284BCC05A12432A9C83931D5AA91B51383B366F069103F3
SHA-512:	3FB1AC6440FD72E5FAB141B294B0081E9A11163FD42EDFF32ECB06722C8BD00B407C7AC4BAB643DA37268013C83C299416ADD78299795AC33F2E17969A8F962B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304693292177252","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13267638885244271","autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"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","1490045"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	16478
Entropy (8bit):	5.570931318876065
Encrypted:	false
SSDEEP:	384:/obt+LlUXU1kXqKf/pUZNCgVLH2HfEVrUVCW74y:jLlGU1kXqKf/pUZNCgVLH2Hf6rUt7h
MD5:	475D05C6AFA5FCB97A38D605CBB7AEF7
SHA1:	E96ECF2EA61B529CB20C0876154856D4F22F9FFB
SHA-256:	DC1A0364CD0EBA82D95BA71D57322BD19531AA9CAEBFB5855B5A881FB309A27A
SHA-512:	1A06414B46CC60B37C2C99469375AC4F7D7588302C32AB25B034B0A39A5FF8A34D5E43F63E48EF45B3F6911FCC5FC875557FB4C604AA0AC47717A15B5E3D196
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304693290415902","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb6b73b3-04a7-4d1f-a6df-f433309a40d0.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):	6567
Entropy (8bit):	4.988381953752544
Encrypted:	false
SSDEEP:	96:n27h7yr1KVtTRWMoiVmdeldNObbHVk7MV1ZXJJExMziZwB:n27hE1KNWM1debH2QLE+
MD5:	3DBA7371D811AA0994A98166BA542770
SHA1:	266B10F5BC79B5CA2049B8AF13AE4B036C807D86
SHA-256:	171ACEC816BE03EC97C12D9CBBCBDDFD72F4B1F1E794BF6F4B548F04E5B8AB07
SHA-512:	C456483463F65AA5E8BD9206472C9BC3D8AED6E0AF291A716686641189276FAD39A6A61B1D3E0ECB3C8FAD3068E91BBB9C9074F0E56FDCBF6C7E197CD8739810
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304693292177252","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13267638885244271","autocomplete":{"retention_policy_last_version":91},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13267638900457663","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","1490045"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cc86497f-ed56-4924-a5f1-83364ab7deb6.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):	7103
Entropy (8bit):	5.017534883414716
Encrypted:	false
SSDEEP:	96:nrdyr1KKIzTRWMoi/R5mdeE3kKX1505hNObbHVk7MV1ZXJJExMAiZw4:nry1KHWM/G3kKXj0HebH2QLEw
MD5:	58FB7B9F0BD816F6DB20341ABC0A960F
SHA1:	005E25409B6F648D505AB2AEB5A68DB41B54D275
SHA-256:	4EEEF82D60C4C2393284BCC05A12432A9C83931D5AA91B51383B366F069103F3
SHA-512:	3FB1AC6440FD72E5FAB141B294B0081E9A11163FD42EDFF32ECB06722C8BD00B407C7AC4BAB643DA37268013C83C299416ADD78299795AC33F2E17969A8F962B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304693292177252","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13267638885244271","autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"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","1490045"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e3aeef77-a893-4fdb-9658-3de8384825a8.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):	6567
Entropy (8bit):	4.9882075305049876
Encrypted:	false
SSDEEP:	96:n27h7yr1KVtTRWMoiVmdeldNObbHVk7MV1ZXJJExMAiZwB:n27hE1KNWM1debH2QLEJ
MD5:	AA7315AA5F9213239EE42C46949F4D30
SHA1:	A214693BEB5310D56EEE418F31ECC22010E716C9
SHA-256:	861241EF2D90248649E737F3451F324F6568A521FB42C1F9904E6FCFA923EC45
SHA-512:	A2A7A2AC1BF33050675B44E8DDD57121BA72E48C1AAE84C1E6CA5D274904B11E9CFDC99066EF7943B93EA62E578D0C20C450A6DBD92C095AA01B2A4DDE590399
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304693292177252","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13267638885244271","autocomplete":{"retention_policy_last_version":91},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13267638900457663","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","1490045"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ee392d12-1008-445d-b43d-9cb8553a0994.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):	15765
Entropy (8bit):	5.573587315296655
Encrypted:	false
SSDEEP:	384:/mFtnLlUXN1kXqKf/pUZNCgVLH2HfEFrUL+74LQa:0LlGN1kXqKf/pUZNCgVLH2HfUrUq7ja
MD5:	3393ABFBD1F294EDCBF3BE1124040DE7
SHA1:	4E0B25C570099720F574F17A270EB1DFC00DA8A1
SHA-256:	9251729649B806E618E6CA19E1B1D29DB2156452A6B88E5E3272CD8B87881995
SHA-512:	CB9551B255EBF683F509E2ACD6C35BBA7BF79539D1832A86BDADF9F3F2CB951B145B0EC46B7BCCF7D81B44A21AF5EBF321FE625867AA77CE27DB82BF3B13EE92
Malicious:	false

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304693290415902","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f1a4c216-12d5-426a-b453-44fefa39f947.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\Last Version

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.873140679513133
Encrypted:	false
SSDEEP:	3:mB4:mu
MD5:	3A0E5D4F452CF99191634D0FFAB744A0
SHA1:	F115BBB898EEFF640D8D19AD44A86C3FCDFFC0AD
SHA-256:	B9D528D3AE283039F4700C7E4E790744C58A26353A91B536DD91CBA4F648A35F
SHA-512:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528A
Malicious:	false
Preview:	92.0.4515.107

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)

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):	115777
Entropy (8bit):	6.032929733000421
Encrypted:	false
SSDEEP:	1536:NGWYBRYGI1pneBQOwQgdWtxwXcBxA1wqW23vfhPwDlLeSfhCsjUtjOjXMWe1:NCj2QyQgd2xNBIwqn3vfh2lvRgyjXC
MD5:	549D76754A5BFFB6B274ED5E03095283
SHA1:	758028EDBF578FBFE4AA52E5CFAAD15F64FDC91D
SHA-256:	C4E56759663F91C8A639EAB1EA4707AF9DA377BC4CFAF7DBB9F70405CAB35D91
SHA-512:	04D64B6F57B0147FFE750C04C4FC42A6120D3FE2D638ABC9AB2F5FF541078786C0ED5498F411EFBA7AB2E44AFA414C8CCDFB9B1B0BD99E4D29D3F713700453A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.660219693490909e+12,"network":1.660187295e+12,"ticks":246420290.0,"uncertainty":3722295.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13304693289712948"},"profile":{"info_cache":{"Default":{"active_time":1660219692.015397,"avatar_icon":"chrom

C:\Users\user\AppData\Local\Temp\46d86dfd-bb38-4c1d-99f2-b24edd8a3ac3.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.acl

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.dic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.exc

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB

SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

Static File Info

General

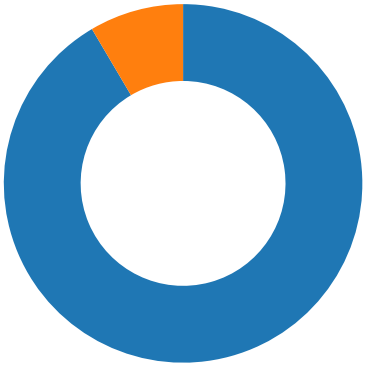
File type:	data
Entropy (8bit):	7.993575690517544
TrID:	
File name:	35
File size:	48294
MD5:	aeada84492f8313f44aae7c56d5d3f8f
SHA1:	a24677f6a7549cba7301d32a0132e153be989544
SHA256:	e94b94022adbee8686effd8c966a5380989bf8a8241c3fddd29a11de332afb6a
SHA512:	4274e4e714b49ba13edafd9120ea8b62e09ee676aa895b46d09cdb34ade350ab38a4513ae43098253740d21c9af536a9fe9820246e921803c3164aec2263ab69
SSDEEP:	768:B2Yhm9VpGro/vpgyKIXxwcqmC1F1Guoc4yj42yoH1/VYMm9Pvi5RD3IXggsmQCN+:kymRGYvKIXxK3ycZsVCJVYMmRaZgsPCU
TLSH:	B423F169CBC5C0D894B9BA151A80BF2E8E19F427C0A5BD24229AECF4CD4C8D7F5DD5B0
File Content Preview:	----------05238bf65b90dd73..Content-Disposition: attachment; name="file"; filename="35"..Content-Type: application/pdf....%PDF-1.5.%.....1 0 obj. <</Type/XObject/Subtype/Image/Width 676/Height 924/Filter/DCTDecode/ColorSpace/DeviceRGB/BitsP

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

Network Port Distribution



Total Packets: 106

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:14.523781061 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:14.523833036 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:14.523926020 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:14.524224043 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.524274111 CEST	443	51086	142.250.185.142	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:14.524363995 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.524885893 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:14.524915934 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:14.525011063 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.525043011 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:14.583643913 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:14.584434986 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:14.595161915 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:14.595211983 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:14.595376015 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:14.596395016 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.596429110 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:14.596688032 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:14.596741915 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:14.597021103 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:14.597161055 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.598040104 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:14.598136902 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:14.598352909 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:14.598483086 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:14.629671097 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:14.629718065 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:14.686876059 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:14.695053101 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:14.695101023 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:14.696348906 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:14.696482897 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:15.018774033 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:15.019201040 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:15.019203901 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:15.019963026 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:15.020261049 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:15.020339012 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.020621061 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:15.020715952 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:15.020751953 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.021109104 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:15.021142960 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:15.052177906 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:15.052321911 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:15.052360058 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:15.052392960 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:15.052624941 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:15.063389063 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:15.063512087 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:15.071484089 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.071634054 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:15.071671009 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.072022915 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.072099924 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:15.132433891 CEST	51086	443	192.168.2.3	142.250.185.142
Aug 11, 2022 05:08:15.132457018 CEST	443	51086	142.250.185.142	192.168.2.3
Aug 11, 2022 05:08:15.138896942 CEST	49901	443	192.168.2.3	172.217.16.205
Aug 11, 2022 05:08:15.138932943 CEST	443	49901	172.217.16.205	192.168.2.3
Aug 11, 2022 05:08:15.329714060 CEST	60753	443	192.168.2.3	142.250.185.132
Aug 11, 2022 05:08:15.329758883 CEST	443	60753	142.250.185.132	192.168.2.3
Aug 11, 2022 05:08:15.812881947 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:15.812942982 CEST	443	63811	5.161.54.249	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:15.813060045 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:15.816442013 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:15.816468954 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.065457106 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.113277912 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.129771948 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.129802942 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.132683039 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.132795095 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.189734936 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.190048933 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.190855980 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.190886974 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.314291000 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.324450016 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.324563026 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.324667931 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.328947067 CEST	63811	443	192.168.2.3	5.161.54.249
Aug 11, 2022 05:08:16.328974962 CEST	443	63811	5.161.54.249	192.168.2.3
Aug 11, 2022 05:08:16.573808908 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.573858976 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.573987007 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.574536085 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.574558973 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.627881050 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.640682936 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.640754938 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.643599033 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.643701077 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.681545973 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.681853056 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.681935072 CEST	60942	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:16.725914955 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.769254923 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.769342899 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.769407988 CEST	443	60942	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:16.769443989 CEST	60942	443	192.168.2.3	188.114.97.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:14.437222004 CEST	63463	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:14.454571962 CEST	53	63463	1.1.1.1	192.168.2.3
Aug 11, 2022 05:08:14.460470915 CEST	60072	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:14.462836027 CEST	57930	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:14.477977991 CEST	53	60072	1.1.1.1	192.168.2.3
Aug 11, 2022 05:08:14.480330944 CEST	53	57930	1.1.1.1	192.168.2.3
Aug 11, 2022 05:08:15.626008034 CEST	50468	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:15.735641003 CEST	53	50468	1.1.1.1	192.168.2.3
Aug 11, 2022 05:08:16.334803104 CEST	50909	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:16.518194914 CEST	53	50909	1.1.1.1	192.168.2.3
Aug 11, 2022 05:08:17.201244116 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.219064951 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.223109007 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.223165035 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.223182917 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.224201918 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.262310982 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.269685984 CEST	54146	443	192.168.2.3	188.114.97.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:17.270602942 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.279973984 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.280018091 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.280049086 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.280075073 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.286839962 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.288180113 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.294435024 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.301750898 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.301985979 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.318576097 CEST	65277	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:17.319171906 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.411371946 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.415445089 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.415813923 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.416102886 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.416398048 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.416686058 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.422013998 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.434298992 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.434331894 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.439141035 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.440227032 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.440260887 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.441163063 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.443908930 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.493128061 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.510288000 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.510682106 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.510792971 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.511012077 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.511373043 CEST	52016	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:17.956718922 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.974482059 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979585886 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979767084 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979806900 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979899883 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979942083 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.979980946 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.980048895 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.980083942 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.980120897 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.980154991 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:17.984101057 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.984175920 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.984262943 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.984373093 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:17.984447002 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.001275063 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001312971 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001349926 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001388073 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001421928 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001457930 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001496077 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001529932 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001568079 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001604080 CEST	443	54146	188.114.97.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:18.001640081 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001641035 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.001677990 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.001754045 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.001847029 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.001900911 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.002017975 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.002060890 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.002078056 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002144098 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002181053 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002216101 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002252102 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002281904 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.002289057 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002329111 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.002367020 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.003443956 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.003541946 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.003624916 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.018723011 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018790960 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018829107 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018866062 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018901110 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018938065 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.018974066 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019011021 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019047976 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019083023 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019114971 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.019118071 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019155979 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019191027 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019211054 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.019227028 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019263983 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019299984 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019308090 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.019337893 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019371986 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019407988 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019432068 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.019443989 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.019471884 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.020524979 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.020560026 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.020565033 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.020570040 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.020575047 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.020580053 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.037599087 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.045521021 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.145065069 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.162985086 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.196701050 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:18.228493929 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:18.232446909 CEST	63967	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:18.249584913 CEST	53	63967	1.1.1.1	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:08:19.028876066 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:19.046567917 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:19.052058935 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:19.052081108 CEST	443	54146	188.114.97.3	192.168.2.3
Aug 11, 2022 05:08:19.052761078 CEST	54146	443	192.168.2.3	188.114.97.3
Aug 11, 2022 05:08:20.692375898 CEST	61825	53	192.168.2.3	1.1.1.1
Aug 11, 2022 05:08:20.865446091 CEST	53	61825	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 05:08:14.437222004 CEST	192.168.2.3	1.1.1.1	0xcd20	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:14.460470915 CEST	192.168.2.3	1.1.1.1	0x6c92	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:14.462836027 CEST	192.168.2.3	1.1.1.1	0x1f29	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:15.626008034 CEST	192.168.2.3	1.1.1.1	0x7f20	Standard query (0)	to-click.fun	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:16.334803104 CEST	192.168.2.3	1.1.1.1	0x1314	Standard query (0)	sweetiestouch2u.com	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:17.318576097 CEST	192.168.2.3	1.1.1.1	0x28fa	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:17.511373043 CEST	192.168.2.3	1.1.1.1	0xac7e	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:18.232446909 CEST	192.168.2.3	1.1.1.1	0x91c1	Standard query (0)	example.org	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:20.692375898 CEST	192.168.2.3	1.1.1.1	0x7d59	Standard query (0)	sweetiestouch2u.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 05:08:14.454571962 CEST	1.1.1.1	192.168.2.3	0xcd20	No error (0)	accounts.google.com		172.217.16.205	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:14.477977991 CEST	1.1.1.1	192.168.2.3	0x6c92	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:14.480330944 CEST	1.1.1.1	192.168.2.3	0x1f29	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 11, 2022 05:08:14.480330944 CEST	1.1.1.1	192.168.2.3	0x1f29	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:15.735641003 CEST	1.1.1.1	192.168.2.3	0x7f20	No error (0)	to-click.fun		5.161.54.249	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:16.518194914 CEST	1.1.1.1	192.168.2.3	0x1314	No error (0)	sweetiestouch2u.com		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:16.518194914 CEST	1.1.1.1	192.168.2.3	0x1314	No error (0)	sweetiestouch2u.com		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:17.335828066 CEST	1.1.1.1	192.168.2.3	0x28fa	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 11, 2022 05:08:17.528471947 CEST	1.1.1.1	192.168.2.3	0xac7e	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 11, 2022 05:08:17.545917988 CEST	1.1.1.1	192.168.2.3	0x8e13	No error (0)	gstaticadssl.l.google.com		142.250.186.67	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:18.249584913 CEST	1.1.1.1	192.168.2.3	0x91c1	No error (0)	example.org		93.184.216.34	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:20.865446091 CEST	1.1.1.1	192.168.2.3	0x7d59	No error (0)	sweetiestouch2u.com		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 05:08:20.865446091 CEST	1.1.1.1	192.168.2.3	0x7d59	No error (0)	sweetiestouch2u.com		188.114.96.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- www.google.com
- https:
  - to-click.fun
  - sweetiestouch2u.com
  - fonts.gstatic.com
  - example.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	51086	142.250.185.142	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:15 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=92.0.4515.107&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-92.0.4515.107 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515. 107 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-11 03:08:15 UTC	2	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-UdWKATbrUdy0fFJ8awxpUw' 'unsafe-inline' 'strict-dynamic' http s: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 11 Aug 2022 03:08:15 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5700 X-Daystart: 72495 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-11 03:08:15 UTC	3	IN	Data Raw: 33 31 62 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 30 30 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 37 32 34 39 35 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31b<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5700" elapsed_seconds="72495"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-08-11 03:08:15 UTC	3	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5 450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:15 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49901	172.217.16.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:15 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+620
2022-08-11 03:08:15 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-08-11 03:08:15 UTC	5	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 11 Aug 2022 03:08:15 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-MIzBAZV3b4KWjeXNML11zQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-MIzBAZV3b4KWjeXNML11zQ' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-11 03:08:15 UTC	6	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-08-11 03:08:15 UTC	6	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	56424	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	48	OUT	GET /lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/m1.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: sweetiestouch2u.com

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	50	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:21 GMT Content-Type: image/jpeg Content-Length: 58153 Connection: close Last-Modified: Tue, 10 May 2022 09:38:15 GMT ETag: "627a3287-e329" Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Cache-Control: max-age=1800 CF-Cache-Status: REVALIDATED Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=t6F2xjb7p0c7R5VIAtMHRVAkS31O%2BUHTgaa3G5QV7ZIeQ64LUUwp%2Fgx2nFeUuRuD0WEh5EpfaI2vN0dTmamPQdcLQWbw7JmKgcpNCkrjUxBv0cRSj5tjrUZQg36tzR5r7YZ%2F5mZn"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc428a87e9bfb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-08-11 03:08:21 UTC	51	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e1 14 70 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 0c 01 00 00 03 00 00 00 01 02 6c 00 00 01 01 00 03 00 00 00 01 03 56 00 00 01 02 00 03 00 00 00 03 00 00 00 9e 01 06 00 03 00 00 00 01 00 02 00 00 01 12 00 03 00 00 00 01 00 01 00 00 01 15 00 03 00 00 00 01 00 03 00 00 01 1a 00 05 00 00 00 01 00 00 00 a4 01 1b 00 05 00 00 00 01 00 00 00 ac 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 22 00 00 00 b4 01 32 00 02 00 00 00 14 00 00 00 d6 87 69 00 04 00 00 00 01 00 00 00 ec 00 00 01 24 00 08 00 08 00 08 00 0a fc 80 00 00 27 10 00 0a fc 80 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 32 3a 30 35 3a 30 36 20 Data Ascii: JFIFpExifMM*IV(1"2i$"Adobe Photoshop CC 2019 (Windows)2022:05:06
2022-08-11 03:08:21 UTC	51	IN	Data Raw: 04 00 00 00 01 00 00 03 3e 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 72 01 1b 00 05 00 00 00 01 00 00 01 7a 01 28 00 03 00 00 00 01 00 02 00 00 02 01 00 04 00 00 00 01 00 00 01 82 02 02 00 04 00 00 00 01 00 00 12 e6 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 ff d8 ff ed 00 0c 41 64 6f 62 65 5f 43 4d 00 01 ff ee 00 0e 41 64 6f 62 65 00 64 80 00 00 00 01 ff db 00 84 00 0c 08 08 08 09 08 0c 09 09 0c 11 0b 0a 0b 11 15 0f 0c 0c 0f 15 18 13 13 15 13 13 18 11 0c 0c 0c 0c 0c 0c 11 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 0d 0b 0b 0d 0e 0d 10 0e 0e 10 14 0e 0e 0e 14 14 0e 0e 0e 0e 14 11 0c 0c 0c 0c 11 11 0c 0c 0c 0c 0c 0c 11 0c 0c 0c 0c 0c 0c 0c 0c Data Ascii: >rz(HHAdobe_CMAdobed
2022-08-11 03:08:21 UTC	52	IN	Data Raw: 2d 6b 49 3b a6 aa ef fd 13 5e ef a3 63 df ea 7d 0a fd 35 0c 87 ac de c7 56 fe 23 13 10 2f 6e ee 5d 77 80 61 c5 8e 03 e9 16 19 03 5f 61 d7 f3 55 2f ac 0e b1 bd 3e b2 09 0d ba cd 84 0f ce 6b 3d 4f 6b bf b4 d5 79 f8 b9 0f c9 6d 99 6f 75 85 ae dc c6 bf d3 f6 92 03 1d b7 ec f5 53 fa 3d a3 f9 af a1 bf f4 8b 3f ad dc 2f e8 18 36 b7 51 f6 bb d8 08 ef b7 7f bb fe 92 93 00 1e e6 9a e8 c3 ce 9a c3 a8 03 5e 87 8b f1 79 df 4a a1 bd c5 a3 d9 5b 9c 34 1c 8f f7 a8 cb 49 0f ad 82 a3 d9 a0 99 04 7e eb a7 7f fd 24 42 dd 74 f0 83 f7 42 60 c6 81 e0 06 a0 9f 15 74 c4 92 e5 0c b1 8c 49 2f 5e 0e f7 ef 88 90 0c 73 12 37 44 fc d1 5a 3b 20 61 cb e9 ad c7 52 e6 30 93 fd 90 ae 56 dd 42 aa 45 12 dd 89 b1 13 dc 07 47 a7 b1 95 8f 51 dc f6 49 0e a7 93 03 ee 49 32 b5 be ac b6 2a ba 3f ff Data Ascii: -kI;^c}5V#/n]wa_aU/>k=OkymouS=?/6Q^yJ[4I~$BtB`tI/^s7DZ; aR0VBEGQII2*?
2022-08-11 03:08:21 UTC	54	IN	Data Raw: b0 d7 8e d2 19 02 7c 34 51 9d 59 e2 38 45 6f 5b 34 3a 86 1d 17 13 2d 87 76 7b 49 6b 87 f6 d9 b5 c8 1d 1a 9b f3 6d b7 02 eb 3e d1 55 20 49 b5 a1 fb 67 b3 b7 83 bd df d6 52 c8 cc 6b 1a eb 1e 7d ad 12 55 cf a8 ed 1f 65 cd c8 b3 f9 db 72 3d de 43 6b 5c d1 ff 00 4d c9 26 46 83 75 fd 33 1e 9a c3 1b 58 86 88 f8 f8 83 10 a8 64 34 b5 a4 b4 46 dd 5b f2 5a fd 4b 32 ba ea 70 1c 9d 25 60 59 99 38 ae 7b f4 73 b8 07 94 d2 17 c2 c8 b6 b6 73 bd ee 0d fa 2e 3b 9b f0 3e e4 fd 3b 18 64 5c c3 61 96 37 dc 5b fb c6 40 d7 f9 29 b3 36 bf 13 1e c1 c8 60 69 fe cf b3 fe fa 8b d1 ed fd 3d 6d ec 4c 7c dd ed 52 78 31 33 dc 4b 89 3c 92 49 fb d1 58 55 47 3a d0 fb 36 d6 e3 b5 ee 68 86 ee e1 c5 bf e0 dc ed ff 00 f9 f3 f9 09 ea cd a0 bc 30 3d 81 e7 86 3d c6 a7 69 fc 8b 5b bf fe 82 b3 c1 26 Data Ascii: |4QY8Eo[4:-v{Ikm>U IgRk}Uer=Ck\M&Fu3Xd4F[ZK2p%`Y8{ss.;>;d\a7[@)6`i=mL|Rx13K<IXUG:6h0==i[&
2022-08-11 03:08:21 UTC	55	IN	Data Raw: 69 60 fa 2d 03 e8 b2 7f f2 5f 4d 04 e4 b9 ce db ac 4f 0a 19 55 fa 80 ce ab 26 c7 e4 63 19 a1 f0 07 15 bf 56 7f e4 99 fd 85 05 f7 66 8c 68 3d 06 e0 d6 2c 2e a5 4d 99 b6 8c 66 3b 6f a8 76 97 fe e8 3f 49 ff 00 d9 51 6f 5f a2 c6 16 58 7d 1b 1b a3 9a ee c7 e2 a1 56 6d 6e 73 ac 63 81 ed 28 ea 90 13 f5 6b 58 c6 fa 55 e8 c6 0d ad 1c e8 04 2e 7d c3 73 89 56 f3 72 bd 47 72 ab b7 68 1b 9c 60 1e 3c 4f c1 10 90 17 a5 ad 69 f7 0d 0c c8 f2 2b 1e e6 ba 97 ba 87 7d 26 18 9f 1f 03 fd a6 ad 80 1c e2 21 a4 81 d8 09 3f f9 15 99 d6 85 ad cc 69 2c 83 65 6d 88 3f bb 2c 3b 8f ef 7d 14 fc 67 56 3c 83 ab 5a 75 8e 4f 82 6b ac 0e 68 6b 60 b4 7e 25 35 6d ee e1 bc 9f 88 1a fc 15 dc 7a 6a 0c da 6a ac b0 e9 b4 34 34 41 fd dd be e6 ff 00 5d 4d 12 06 a5 af 92 32 90 a1 a3 b1 d0 f1 aa 3d 1d Data Ascii: i`-_MOU&cVfh=,.Mf;ov?IQo_X}Vmnsc(kXU.}sVrGrh`<Oi+}&!?i,em?,;}gV<ZuOkhk`~%5mzjj44A]M2=
2022-08-11 03:08:21 UTC	56	IN	Data Raw: 6f 6f 6c 00 00 00 00 00 42 63 6b 67 4f 62 6a 63 00 00 00 01 00 00 00 00 00 00 52 47 42 43 00 00 00 03 00 00 00 00 52 64 20 20 64 6f 75 62 40 6f e0 00 00 00 00 00 00 00 00 00 47 72 6e 20 64 6f 75 62 40 6f e0 00 00 00 00 00 00 00 00 00 42 6c 20 20 64 6f 75 62 40 6f e0 00 00 00 00 00 00 00 00 00 42 72 64 54 55 6e 74 46 23 52 6c 74 00 00 00 00 00 00 00 00 00 00 00 42 6c 64 20 55 6e 74 46 23 52 6c 74 00 00 00 00 00 00 00 00 00 00 00 00 52 73 6c 74 55 6e 74 46 23 50 78 6c 40 52 00 00 00 00 00 00 00 00 00 00 0a 76 65 63 74 6f 72 44 61 74 61 62 6f 6f 6c 01 00 00 00 00 50 67 50 73 65 6e 75 6d 00 00 00 00 50 67 50 73 00 00 00 00 50 67 50 43 00 00 00 00 4c 65 66 74 55 6e 74 46 23 52 6c 74 00 00 00 00 00 00 00 00 00 00 00 54 6f 70 20 55 6e 74 46 23 52 6c 74 00 00 Data Ascii: oolBckgObjcRGBCRd doub@oGrn doub@oBl doub@oBrdTUntF#RltBld UntF#RltRsltUntF#Pxl@Rvecto rDataboolPgPsenumPgPsPgPCLeftUntF#RltTop UntF#Rlt
2022-08-11 03:08:21 UTC	58	IN	Data Raw: 58 54 00 00 00 01 00 00 00 00 00 00 6e 75 6c 6c 54 45 58 54 00 00 00 01 00 00 00 00 00 00 4d 73 67 65 54 45 58 54 00 00 00 01 00 00 00 00 00 00 06 61 6c 74 54 61 67 54 45 58 54 00 00 00 01 00 00 00 00 00 0e 63 65 6c 6c 54 65 78 74 49 73 48 54 4d 4c 62 6f 6f 6c 01 00 00 00 08 63 65 6c 6c 54 65 78 74 54 45 58 54 00 00 00 01 00 00 00 00 00 09 68 6f 72 7a 41 6c 69 67 6e 65 6e 75 6d 00 00 00 0f 45 53 6c 69 63 65 48 6f 72 7a 41 6c 69 67 6e 00 00 00 07 64 65 66 61 75 6c 74 00 00 00 09 76 65 72 74 41 6c 69 67 6e 65 6e 75 6d 00 00 00 0f 45 53 6c 69 63 65 56 65 72 74 41 6c 69 67 6e 00 00 00 07 64 65 66 61 75 6c 74 00 00 00 0b 62 67 43 6f 6c 6f 72 54 79 70 65 65 6e 75 6d 00 00 00 11 45 53 6c 69 63 65 42 47 43 6f 6c 6f 72 54 79 70 65 00 00 00 00 4e 6f 6e 65 00 00 00 09 Data Ascii: XTnullTEXTMsgeTEXTaltTagTEXTcellTextIsHTMLboolcellTextTEXThorzAlignenumESliceHorzAlignde faultvertAlignenumESliceVertAligndefaultbgColorTypeenumESliceBGColorTypeNone

<table>
<thead>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
</thead>
<tbody>
<tr><td>2022-08-11 03:08:21 UTC</td><td>59</td><td>IN</td><td>Data Raw: f3 48 2e 0d 7b 3f 95 bf fc f4 e5 90 74 d0 aa 39 59 b7 fa 85 ee ad ef a1 c7 69 73 4b 3d b2 27 fa 3e df 51 f5 ff 00 c2 6f 56 71 ee 6b 18 6b bd ed 66 d2 05 6e 71 80 41 12 d6 ee 29 d1 26 ac fe 08 c9 00 0e 9b 25 f5 6c 67 3a a7 fb 45 4e d1 da 14 ee 64 8f 1f 82 ad 65 44 f6 94 ee 2e fa b1 f0 af f6 4a 1d 63 9e 6d 80 75 80 dd 7e f9 56 2b a3 05 bc ee 7f c5 d1 ff 00 51 b5 66 1d e1 f0 d7 10 3c 11 40 71 02 49 3f 34 6c 76 51 89 ee eb d6 ec 1a fe 8d 55 83 e2 e1 3f 8b a5 c9 2c fa 28 de f0 d0 24 92 92 56 ae 17 ff d1 bc d5 30 a0 14 82 81 99 92 70 a2 0a 70 81 53 20 ac e2 38 54 5f 92 44 b7 1d a6 cf 98 07 68 55 82 b1 7f e8 ba 2d ef fc eb 05 84 7c 18 d3 ff 00 7e 6b 92 8e ea ec 3b a1 fa bb 95 55 b8 2e c6 26 5f 44 3a c7 3b 87 7a 8e b6 df 53 fe dd f5 91 05 8e d9 97 f6 6a eb d8 cd
Data Ascii: H.{?t9YisK='>QoVqkkfnqA)&%lg:ENdeD.Jcmu~V+Qf<@qI?4lvQU?,($V0ppS 8T_DhU-|~k;U.&_D:;zSj</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>60</td><td>IN</td><td>Data Raw: cb 81 10 77 1f 1f ec ec 46 67 2a 48 ed e7 ab 04 ef 8a bf 77 d3 a7 f5 5b f8 bc 8f 24 93 63 9e 12 42 93 7a 3f ff d4 67 e5 5d ea d6 c1 61 a1 8e 74 3e c6 31 b6 39 a2 1d b7 d9 67 b7 de fd ac 46 c7 bf d4 6e d1 b9 cf 66 8e dc 00 3c 98 dd b7 db bb 6f d2 59 f9 7d 46 9c 4a fd 6b 1d fd 46 08 97 91 f9 ac 95 ce 64 75 7c dc 86 ba 86 fe 8a ab 1d 26 b6 12 4b 81 d1 8c b1 ff 00 4a df ea fe 7f ee 28 44 4d dd 96 c4 a5 60 46 87 7b fd 27 b6 aa d6 5c f3 5d 2f 6d af 11 2d 63 83 88 dc 76 b3 76 d2 76 ef 72 e8 6b c3 63 30 9d 8e 48 87 31 cd 73 88 90 5c f1 0e 7b 87 ee 2e 2b ea 0f 48 7f db ef ea 19 2c f4 db 8a c0 ca 19 a0 26 cb 77 6f b1 ed 69 dd fa 3a 1b fe 13 fd 32 ea fa 8f 51 15 b4 86 76 e5 45 96 5a d0 e9 f9 b3 60 c6 68 9a df 4f a2 83 ad b5 cd c0 ad cf 38 c2 91 65 d6 3a 37 d4 d0 4d
Data Ascii: wFg*Hw[$cBz?g]at>19gFnf<oY}FJkFdu|&KJ(DM`F{'\]/m-cvvvrkc0H1s\{.+H,&woi:2QvEZ`hO8e:7M</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>62</td><td>IN</td><td>Data Raw: 4a aa fb 09 52 40 75 63 96 8a b2 c2 08 73 49 69 1c 10 60 83 e4 95 97 3e da ec 2e 89 0c 26 40 89 22 35 28 0e 74 ea 54 8b b6 d1 61 ee e8 6f de 43 bf ea 5a a5 88 d4 79 b1 4c fa 25 e4 50 72 5a c1 fd af ca ba 8e 87 40 c7 e9 6c d9 63 ab ca ce db 7b ae 6c 48 61 7f a1 43 3e 93 5f e8 b7 f3 9d fe 92 ef f4 4c 58 3d 3b 0a cc dc 96 52 d1 ec 00 d9 69 98 f6 8f cc dd f9 ae b7 f9 bf fd 56 bb 3a db f6 bc 76 d8 c6 36 87 b8 0f 4e 04 00 2b 3f a2 af fe 29 bb 7d aa 62 5a 0d 4e a9 97 95 78 c3 c4 2e 02 8c c7 57 61 34 cf bd 8c fd 25 cd 71 b3 6b bf b1 b3 fc 22 4a bd f7 9c 9c f7 e4 de c0 c6 50 df b3 31 81 da 02 4e fc 87 b1 cd 1f 9c fd 8c 67 fc 52 49 21 ff d7 a7 75 9f 68 e9 fb 1d fc e6 3e 92 7b b0 9f 64 7f c5 fd 05 47 a6 74 f7 f5 4e a1 5e 13 09 63 5e 4b ae b0 72 ca 9b fc eb c7 f2 ff
Data Ascii: JR@ucsIi`>.&@"5(tTaoCZyL%PrZ@lc{lHaC>_LX=;RiV:v6N+?)}bZNx.Wa4%qk"JP1NgRI!uh>{dGtN^c^Kr</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>63</td><td>IN</td><td>Data Raw: 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a
Data Ascii: xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>64</td><td>IN</td><td>Data Raw: 74 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 57 69 6e 64 6f 77 73 29 22 20 73 74 45 76 74 3a 63 68 61 6e 67 65 64 3d 22 2f 22 2f 3e 20 3c 2f 72 64 66 3a 53 65 71 3e 20 3c 2f 78 6d 70 4d 4d 3a 48 69 73 74 6f 72 79 3e 20 3c 70 68 6f 74 6f 73 68 6f 70 3a 44 6f 63 75 6d 65 6e 74 41 6e 63 65 73 74 6f 72 73 3e 20 3c 72 64 66 3a 42 61 67 3e 20 3c 72 64 66 3a 6c 69 3e 30 37 32 33 30 34 38 30 32 34 30 42 36 32 41 31 45 44 42 44 45 46 31 33 45 43 34 33 44 35 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 34 32 37 37 43 43 34 44 42 30 46 36 33 44 33 35 44 37 44 30 37 42 38 32 37 38 34 46 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 36 41 31 33 37 43 32 39 39 42 34 31 42 43 34 39 33 43 32 37
Data Ascii: t="Adobe Photoshop CC 2019 (Windows)" stEvt:changed="/"/> </rdf:Seq> </xmpMM:History> <photoshop:DocumentAncestors> <rdf:Bag> <rdf:li>07230480240B62A1EDBDEF13EC43D505</rdf:li> <rdf:li>104277CC4DB0F63D35D7D07B82784F24</rdf:li> <rdf:li>16A137C299B41BC493C27</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>66</td><td>IN</td><td>Data Raw: 20
Data Ascii:</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>67</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 63 70 72 74 00 00 00 fc 00 00 00 32 64 65 73 63 00 00 01 30 00 00 00 6b 77 74 70 74 00 00 01 9c 00 00 00 14 62 6b 70 74 00 00 01 b0 00 00 00 14 72 54 52 43 00 00 01 c4 00 00 00 0e 67 54 52 43 00 00 01 d4 00 00 00 0e 62 54 52 43 00 00 01 e4 00 00 00 0e 72 58 59 5a 00 00 01 f4 00 00 00 14 67 58 59 5a 00 00 02 08 00 00 00 14 62 58 59 5a 00 00 02 1c 00 00 00 14 74 65 78 74 00 00 00 00 43 6f 70 79 72 69 67 68 74 20 31 39 39 39 20 41 64 6f 62 65 20 53 79 73 74 65 6d 73 20 49 6e 63 6f 72 70 6f 72 61 74 65 64 00 00 00 64 65 73 63 00 00 00 00 00 00 00 11 41 64 6f 62 65 20 52 47 42 20 28 31 39 39 38 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: cprt2desc0kwtptbkptrTRCgTRCbTRCrXYZgXYZbXYZtextCopyright 1999 Adobe Systems Incorporated descAdobe RGB (1998)</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>68</td><td>IN</td><td>Data Raw: 27 4e 92 49 d2 4e e9 24 e9 dc 96 b5 c4 52 56 aa 18 86 a6 70 e5 52 e6 8b 33 34 5a 10 8c 07 08 41 94 e4 ee cc d3 79 ce 44 23 c6 49 49 d3 a7 67 49 24 e9 d3 a4 9d 3c ed ee 41 66 64 50 d6 b8 0a 58 91 b3 5d a3 b2 75 16 51 84 60 38 42 10 15 79 16 45 92 79 ca 72 21 c2 ee a4 9d dd 24 93 a4 93 a7 74 92 75 23 6b dc 0d 12 f3 e0 d4 d1 c8 cd a7 cd c3 66 e5 7b ba ec cc 9a 03 8c 21 08 42 15 a6 49 ce 4a 52 9c a6 7b 15 12 4f 27 74 99 d2 4e 92 74 9d 3a 74 f2 d4 33 b9 3c ff 00 9e ad d5 f7 b9 1c ed 1d 3e 72 97 4e d1 d4 b7 16 68 c6 30 84 61 01 c2 b1 67 29 c9 de 73 73 5a d0 c3 77 77 74 ee 92 49 24 e9 27 74 9d dd cf b1 c8 f4 e5 07 0f db 71 40 f4 7c 7e 72 04 00 65 a9 46 5c fd bb b2 64 d1 8a 9d e8 08 24 23 ca 69 e7 32 59 d3 d3 e3 e5 27 49 dd d2 49 24 9d 27 4e 9d 3a 9d bd 6f 24 f4
Data Ascii: 'NIN$RVpR34ZAyD#IIgI$<AfdPX]uQ`8ByEyr!$tu#kf{!BIJR{O'tNt:t3<>rNh0ag)ssZwwtI$'tq@|~reF\d$#i2Y'II$'N:o$</td></tr>
<tr><td>2022-08-11 03:08:21 UTC</td><td>70</td><td>IN</td><td>Data Raw: f2 94 cc 63 58 b3 cd 3b a4 e9 d2 76 77 49 24 ef af ac d0 8b 42 0a 4f 19 49 a3 42 8a ce d5 59 d5 6e db 3f 3f e7 ab 4b af 7c 7e 22 5e 95 5a f7 9d 36 af 5f 76 55 53 a9 ca 65 31 ac d8 e6 9d 25 24 93 b3 a7 74 99 de 5d 39 20 18 b3 34 a5 05 24 ea b5 5c 0a 17 ad 04 1a 87 2e 5f 9c d2 37 a0 06 f7 95 2f 4e 85 8f 35 9e e7 4a 52 c1 d3 ca 53 29 8d 68 fc d3 a7 74 9d 9d 27 74 c9 d3 df dc 60 e7 98 cc ef 00 a1 c1 4b 27 96 af 7b 57 42 90 6e 3d c5 c7 f1 e6 ef 16 c7 93 0f d3 85 a9 e4 a4 ed f4 6d 57 4e 9d e4 42 18 f6 4d cd c9 3a 4e e9 33 ba 74 ce 9f 76 ec 73 f2 77 49 18 0e ac 24 ea 30 a6 3d ac 51 cc 05 99 2c d2 0f 09 5b ae 25 ee 1b 3f ae 36 87 9c cf d0 09 a9 41 dd 3b c8 a4 29 ec 1f 9a 9a 49 d3 a4 93 bb a4 e9 fa 84 3c 6a bd 4c 84 11 d7 12 77 85 2c e0 45 49 ca 42 d8 2e 3d 0a 98
Data Ascii: cX;vwI$BOIBYn??K|~"^Z6_vUSe1%$t]9 4$\._7/N5JRS)ht't`K'{WBn=mWNBM:N3tvswI$0=Q,[%?6A;)I<jLw,EIB.=</td></tr>
</tbody>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	71	IN	Data Raw: 39 5e 9e 56 f1 f1 c1 b3 64 55 eb 55 ab 52 bc 16 85 2f 41 cc cc a8 26 91 6d 5c b5 e7 13 92 b1 e9 79 7b 75 6c 5b d2 c4 d0 f9 dd e5 6f b1 a3 5c 49 da 5e a8 29 67 d2 a9 4e b5 77 d6 ef d3 46 00 80 e2 81 9f 47 a4 7c 7a 4e 69 8e bd 4a 40 1c 4d a7 99 df 52 cf a2 26 99 26 69 71 d2 22 5d 0f 65 6b 4b 97 b5 a7 9f 3f 09 52 ef e9 d3 0c 5d d8 9b 7d b5 4c 6a 55 ab 41 df 77 b9 93 33 a8 86 b0 2b e7 83 a6 6c ba 21 51 15 2a 40 82 95 bb 14 fb 50 e6 d1 0b 4a c3 ac fc 79 91 12 17 bb fd 5e 7c d6 ec 72 be 59 2e 9f 73 18 41 84 a7 39 4b b8 8e 15 3a e9 e4 fd 3f 63 39 a2 38 2a d3 ab 52 89 fa 38 67 d5 ae 28 06 8d 20 c1 4b 42 aa e9 de 85 20 c5 cc 55 ce b3 a9 bb 11 7b 14 ab 5a b1 c5 79 62 f4 3c 9a 01 80 8b 22 ca 46 d4 a1 5d 24 a5 d8 75 53 b0 59 35 3a 54 aa d2 a7 ad b5 0a 35 01 5c 61 a5 Data Ascii: 9^VdUUR/A&m\y{ul[o\l^)gNwFG|zNiJ@MR&&iq"]ekK?R]}LjUAw3+l!Q*@PJy^|rY.sA9K:?c98*R8g(KB U{ Zyb<"F]$uSY5:T5\a
2022-08-11 03:08:21 UTC	72	IN	Data Raw: 6b 7f 5e f5 0a b2 e2 22 a7 2c a0 f6 be 86 68 02 b5 5a d5 aa 56 b7 ab 72 45 85 50 82 b4 ee 44 14 e9 d5 08 e3 29 cd 26 1c ed 17 8b 1c 19 29 da 35 88 13 4b 33 9f 95 9f 44 ee 31 f0 b1 39 0e ea fe db 38 b1 f8 e4 a3 1a d4 bd 93 70 81 08 41 5e b0 01 56 8e 9e b5 b8 00 40 09 4d 1a f4 ea 80 71 69 92 48 63 46 3b 72 22 84 61 6a c2 65 68 a4 b3 85 46 c4 bb 3d 1c fe 78 bb 1a 7b 6f 0e 72 a6 1a 78 46 17 7d 56 ea 80 86 2a f5 ab 80 20 c8 2e c5 a9 08 03 3c 9a b5 4a e2 82 72 9e 00 81 1e 40 b1 cd e6 c0 b6 5d 49 cf 60 ae 6a dc ed 92 35 cd dc fd 19 e8 74 e2 85 2e 0d d9 46 2b a5 ef 6c 38 e3 01 06 bd 6a f5 c1 5f 1d ad 15 46 c5 d7 08 00 10 b3 d8 34 6b 91 0e 73 ba f8 1c e1 48 a6 9e c2 b2 49 1c 1c f2 99 84 bb 0d 7c d2 76 15 68 72 fc d6 a3 b4 20 bb be a0 ee d0 1c 02 0a d5 eb d7 05 5c Data Ascii: k^",hZVrEPD)&)5K3D198pA^V@MqiHcF;r"ajehF=x{orxF}V* .<Jr@]I`j5t.F+l8j_F4ksHI|vhr \
2022-08-11 03:08:21 UTC	74	IN	Data Raw: 04 05 49 53 74 70 48 54 8c 53 ae 68 14 de d4 a2 fa 00 41 48 76 cc 78 68 62 60 a7 a3 06 4a 5a 68 c8 be d0 49 84 16 c9 e3 c8 6c 4c 02 f2 1a 6b 4a 90 af 46 92 63 58 b2 72 5c 92 5d 3c e8 06 40 c7 54 e0 0e ed 9c c8 c8 23 34 71 0e b6 c7 2b 62 1b 06 ea 94 b0 be e3 37 34 9c e2 c5 c9 17 ae bc d8 8d 0c bb 29 9a 44 50 ef b4 21 39 31 19 33 86 f4 72 64 31 31 d5 d3 7a ce 36 ce ad 80 81 f1 db 25 30 0e 04 d8 21 dd 55 3d 97 35 ba ed 63 85 47 15 b3 31 8c cb 90 a6 08 77 54 6b 42 c9 f5 6c 13 23 ae 3a 64 c9 4f 1e 54 3a 1c bb a6 de a5 31 6d a0 43 15 71 d0 c9 97 9f 30 82 80 ab 1a d6 db 61 ae 81 20 3e 2a 01 ac f9 d0 81 b4 ed b4 f6 a6 30 da c5 03 17 2d 31 3c f9 d3 48 2a b3 7a 01 5b 8c 61 d0 d1 03 33 c8 6c 8e 64 e5 36 a9 e7 56 03 e8 18 c7 d0 4e 76 38 31 06 b9 65 08 b4 54 cd 5a 61 Data Ascii: IStpHTShAHvxhb`JZhlILkJFcXr\]<@T#4q+b74)DP!913rd11z6%0!U=5cG1wTkBl#:dOT:1mCq0a >*0-1<H*z [a3ld6VNv81eTZa
2022-08-11 03:08:21 UTC	75	IN	Data Raw: 32 54 e2 a9 8b cd cd 17 30 af db 23 5b 43 06 d3 8a 10 c9 95 92 a0 e6 e2 71 2e e5 5f ff c4 00 25 10 00 02 02 02 02 03 01 01 01 01 01 01 01 00 00 00 01 02 00 03 04 05 10 11 06 12 20 13 30 14 40 15 16 50 ff da 00 08 01 01 00 01 02 00 87 ef af a2 0d 45 7b e3 bf 8e ba 4b 05 c3 f8 89 91 af ca f1 cb 6a 4c 8c 79 91 5d 26 8f 20 c4 ce 04 1e fd bd be ba 9d f0 5b b6 9d f6 20 9d f6 58 13 00 e3 ae 47 f4 28 6a 2a 27 5c 0f 8e e0 b9 6f f8 eb e1 d7 23 45 95 a9 4b eb bf fc cf 83 4e df 1b 74 1c 18 a4 37 60 f6 1b db b8 0f 53 d5 60 1d 71 dc 20 0f 63 6f 1d 7d 75 fc ca 1a 88 f6 eb 9e a0 1e a2 0b 83 75 f3 d7 19 5a dc 9d 1b 22 e5 54 f6 62 21 c4 f2 2a 32 83 88 20 33 a8 0f 22 1e 3b 07 db be fd 8d 86 c3 69 b4 7f d0 50 d7 dc f5 82 75 cf 41 c5 c0 fd f5 6d 76 69 72 75 c9 75 37 3d 2d 85 Data Ascii: 2T0#[Cq._% 0@PE{KjLy]& [XG(j*'\o#EKNt7`S`q co}uuZ"Tb!*2 3";iPuAmviruu7=-
2022-08-11 03:08:21 UTC	76	IN	Data Raw: f6 07 b1 c7 7c 77 c0 fe 23 f9 56 9e d9 89 b3 73 33 6a d4 e8 3a ce 99 a3 5e 99 9b 8c 3d 56 3f 88 0f 1d cb d6 5d a6 cc b5 55 c6 8e 5d 5f 92 8e 3a 20 ca 1c 80 c9 c7 58 53 01 d6 2c 1c 8e 00 50 81 4f b7 60 f7 fc 07 d9 e4 7f 00 31 c3 55 9c fb 58 f2 cc 6a 76 38 59 39 34 e4 63 57 ab d3 e2 64 e4 57 b7 c9 d9 ec 30 b1 b2 16 a0 b9 6d a9 6c 81 e4 6d c0 86 30 42 58 54 b5 b2 8a fd f5 84 45 83 9e 84 01 62 c1 3b 04 1e 44 1f c4 7f 64 3a ca 32 0e 59 de 4a ea cb cc cc f2 8f 16 cc 70 83 12 8d b6 b2 ad 06 46 8f fd b6 5f 69 a6 95 19 a7 12 e5 1e 44 5a 75 1a 74 20 4f cf d1 11 54 0c 16 00 7c 08 20 8b 01 ec 41 04 03 9e bf e6 33 48 89 10 ee 62 2e 72 b0 45 c0 cf 28 d5 75 76 bf 23 5a da ef fc f4 a2 28 ce 27 21 17 c9 61 8a 0c 23 80 0f 15 45 0b 30 60 00 0e 7a 80 01 d8 82 08 22 8e 07 04 Data Ascii: |w#Vs3j:^=V?]U]_: XS,PO`1UXjv8Y94cWdW0mlm0BXTEb;Dd:2YJpF_iDZut OT| A3Hb.rE(uv#Z('!a#E0`z"
2022-08-11 03:08:21 UTC	78	IN	Data Raw: 26 3c c2 c4 b9 be 44 10 45 82 2c 1c 18 0f f4 ef 92 71 69 ed de fb 30 30 44 68 d1 ac 6b 08 68 09 3c 34 64 7b 68 dc 4b 11 cd fa 9f f7 6b f6 b9 85 2d aa c4 7b c6 46 3d 95 a5 78 f1 92 c4 ad 54 05 49 9f 48 5a 2a ad 44 1f 22 08 20 8b 16 29 10 0f e9 df c6 05 30 cb ac c0 c5 ef db f4 b9 9a e6 bb de 1e 1a 3d e6 db b6 5b 0b 31 06 30 67 a7 71 55 b6 9b 75 d5 d3 52 21 f6 66 71 91 52 1c 70 f2 f6 42 a5 5c 9c c2 cf 8e f7 59 04 1f 22 08 22 c1 16 08 21 fe 63 eb 1a 93 2d 6c 7a 20 2f 3d f2 f6 1f af ee 94 e6 5f df 66 5f 1a 8c ab 6d d8 d7 46 3d 4a f7 e0 be 8e bc ac e7 d2 ea f2 70 95 c3 b3 52 f9 88 e9 8e d7 d9 6d b4 b2 b5 96 55 7e 66 44 a6 cf 71 f4 20 8b 16 2c 11 60 fe bd fc 6b 68 e8 cd 86 6a d7 c5 ad 95 6e 45 82 f7 d2 d5 8d 98 e3 6a 32 1d c1 42 d5 5d aa bf 41 46 d2 ad dd 1b 4f Data Ascii: &<DE,qi00Dhkh<4d{hKk-{F=xTIHZ*D")0=[10gqUuR!fqRpB\Y""!c-lz /=_f_mF=JpRmU~fDq ,`khjnEj2B]AFO
2022-08-11 03:08:21 UTC	79	IN	Data Raw: 9e b2 10 f6 b6 6a ce 55 94 e2 18 01 b6 d5 a7 c6 b2 6c c7 d7 f2 66 b7 5a ed 63 13 cf 55 ab 96 2d 19 9d ed 62 6c 79 aa 54 e1 a3 25 b8 cf 84 70 46 18 c7 5a 4a 5e 2c 4c 2a ad 17 2d 4d 4e 69 76 76 76 7b 2c 77 7b 19 bb 0d 89 5d f6 33 5b 2d 0d 0f 02 29 47 4b 2f 60 56 29 ef 13 23 36 0b 6a ad dc 62 e1 80 33 21 cd e7 07 09 cd 8e cc c5 49 1c 26 6f b1 97 58 d6 3d ae cf 60 e3 48 ab 3a 61 d1 53 57 e0 d8 ff 00 9f ab cb a0 5c 7a ed ae f4 e8 14 bb f6 6b 1e c7 b1 ec 2c 5c 14 0d 3a a1 ad 96 c6 e4 4e 81 57 ce c8 10 c5 e0 ae 97 c8 bf 74 c2 b3 1b 31 f5 36 3e c8 c5 c9 9d aa e2 e1 5e d6 92 58 a1 24 40 34 d9 e1 6f be fb ec c8 36 b5 a0 c1 3c 79 00 00 af 5e 9e 85 1c 38 62 e6 d3 52 d4 af 2d 57 a8 af 44 38 b0 b3 13 d0 50 29 5c bb 26 0b 5b 2e 8f 09 ed 48 33 db 6b 77 53 a0 48 61 ae d9 Data Ascii: jUlfZcU-blyT%pFZJ^,L*-MNivvv{,w{]3[-)GK/`V)#6jb3!I&oX=`H:aSW\zk,\:NWt16>^X$@4o6<y^8bR-WD8P)\& [.H3kwSHa
2022-08-11 03:08:21 UTC	80	IN	Data Raw: 96 24 40 23 46 8e 6d 37 35 ad 6e 46 b1 ec 36 b5 e6 d8 f1 81 1c 88 a1 62 29 1c 76 d0 9e fe 14 28 bc b4 50 0b 3e bf 15 1e 5b 52 5f 6e 6e 0e 43 9d fe 5e ba 9c 54 c7 6c 4a 54 9b 31 72 72 16 d5 78 61 e5 9b c5 74 44 b4 b2 2c ec 39 7f d3 be c4 1c 12 e5 cd c6 d3 7b 5f 55 38 f6 9b 8d a6 d2 e5 8c 03 8e 95 56 24 cf 48 09 86 12 20 e0 11 16 56 b6 5a 78 eb c4 f4 fb 1c 34 ad c9 5a d6 dc 9d 2e 35 af ed 66 46 25 38 b5 66 ba 62 86 d7 5d 7c be 5a 1b e3 c4 75 25 8c 77 62 21 76 6f 72 c0 88 20 e1 8b 9b 25 cd 71 b0 6b 35 ad 2d 7b 9a c2 e5 c9 e0 72 04 40 26 ce a8 1b b2 79 30 4e c4 b9 a3 b2 9c 0c 3d 06 56 d0 0c fc 9b f0 ea 71 4e 37 ae e3 3f 43 87 51 a0 66 61 03 76 31 85 e8 c8 c9 4b 23 73 4d 1a fc 30 5a 5b 7d 76 bc b1 99 cb 06 48 b0 70 63 16 67 36 c7 83 1b 17 1a c6 b2 cb 5a c2 e5 Data Ascii: $@#Fm75nF6b)v(P>[R_nnC^TlJT1rrxatD,9{_U8V$H VZx4Z.5fF%8fb]|Zu%wb!vor %qk5-{r@&y0N=VqN7?C Qfav1K#sM0Z[}vHpcg6Z
2022-08-11 03:08:21 UTC	82	IN	Data Raw: 34 10 45 e4 c1 c1 35 87 97 0b a5 83 be b0 3c 89 18 a5 da 0c ad 2b 0f 63 00 23 55 8d df 46 34 68 66 01 48 a4 7c 18 61 8c 08 31 a3 02 0c 31 a3 07 19 09 43 d6 54 ac 58 b0 0e 8c 30 c6 8d 0c 3c f4 45 b2 f6 52 b1 78 07 90 a4 4a 41 56 5f 56 5f 65 71 4e 2e 46 bf 76 0a d7 b5 d3 3d 46 02 b3 51 49 10 c2 4c b0 69 6c 48 b0 1e 0c 31 f8 68 41 86 18 c1 a3 43 0c 61 97 56 25 b4 b2 95 89 12 00 43 43 0c 24 c3 0f 06 18 65 b3 2a 20 50 0f 22 2f 0c c0 59 9a 51 88 04 32 05 ed 95 c6 06 e7 07 3c 8d 9e 9f 33 01 96 89 80 87 83 0f 0d 3c 75 d2 09 d7 c3 46 86 34 60 d0 c6 86 30 20 c3 1c 50 28 2b 12 24 40 07 4c 18 18 63 12 78 26 34 b2 64 85 61 00 51 c0 89 18 f7 8c 82 57 4b 4e ba f6 3c 7a 5e 85 d8 eb 7c 83 1b 33 22 8c fc 2c 25 ac 34 ec 92 0c 63 e3 8d 5c 1c 19 d1 11 a3 46 86 34 68 63 43 0c Data Ascii: 4E5<+c#UF4hfH|a11CTX0<ERxJAV_V_eqN.Fv=FQILilH1hACaV%CC$e* P"/YQ2<3<uF4`0 P(+$@ Lcx&4daQWKN<z^|3",%4c\F4hcC

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	83	IN	Data Raw: 61 a5 65 23 bf 80 03 c9 e3 d3 ff 00 a3 4d 28 2b 16 59 7a 82 3c 43 e4 69 2c 55 d4 83 cc 1d 85 63 70 ba 43 88 25 07 e4 7f 1a d4 4d 61 88 8c c4 7e 21 e2 5a 8a 41 78 e4 57 1d 54 de 94 6a 58 01 d4 9b 56 0d 2f 9b 12 97 e8 0e 63 fc ab 0f af 77 14 d2 7c b2 8a c7 b7 e0 82 28 87 57 6c c6 b1 b2 7e 3c 7b 01 cc 46 2d 50 13 7c ac e7 ab 9a b6 ca a3 e5 4c dc 98 d2 ae ec 8b ea 69 34 b1 66 f9 55 b5 cb f5 35 c8 38 f4 51 73 58 a9 75 48 25 7f 5b 81 58 d2 3f bb 88 79 17 f7 7a 7e d3 7d c5 0a 61 b7 0f 3a df 88 a1 c4 8e 74 3d cd d4 a9 00 a9 dc 1d 45 61 24 07 b9 2d 87 63 c9 7c 48 7d 54 d6 26 00 49 84 48 07 e7 80 fe aa 75 a9 b5 56 b4 aa 39 30 f1 0a 8c fe 16 c8 7a 35 30 be 95 90 96 42 50 f3 22 99 cf 8d 99 bf 88 d2 83 a0 14 48 b0 06 b2 fe 2c a3 d4 d4 63 f3 33 1f dd 15 6f f6 7f e6 6a Data Ascii: ae#M(+Yz<Ci,UcpC%Ma~!ZAxWTjXV/cw|(Wl~<{F-P|Li4fU58QsXuH%[X?yz~}a:t=Ea$-c|H}T&IHuV90z50BP "H,c3oj
2022-08-11 03:08:21 UTC	84	IN	Data Raw: e9 e7 e9 5a b2 10 7c 20 06 d7 40 08 bd a9 99 6e 77 26 9f 1b 29 c3 a0 02 24 37 77 3c cd 60 60 8a f2 a8 6b 0b e6 73 5d 9f 09 6c f1 21 d8 1d 03 11 7d 2e 6b 0c 1c 42 c8 81 ad 7d 85 ad 51 12 4a 04 d3 42 17 91 a2 e2 8a bd a8 9d 06 94 b1 46 d2 39 b2 8d cd 62 99 ac 88 06 fa 5f a1 d6 b1 51 e5 ef 51 c0 2a 97 3b 80 00 34 b3 32 00 6e bb 13 fc 80 ab 85 71 6d 34 af 0e 60 34 b0 7a 29 2e fe 13 fd 7d e6 9e c6 a7 de 9e 3b 7e d6 18 d8 ed bb 1e 82 8b 23 b6 5c a4 b8 45 1f 08 23 5f 9d 45 0b e1 62 66 b0 79 35 3e 51 29 91 be ba 0a cb 82 7c 43 8f 1b 12 57 c8 9f cd 44 61 e2 3c ca de 96 08 0d ce 82 ec c6 df e9 53 4d 22 fd 99 83 8f c4 0a 90 ca a0 7e 7c c3 97 26 56 ac 5e 28 94 84 49 20 02 c7 70 02 fc 3d 6c 39 13 52 e1 25 78 cc ee ae 97 8c dc 5c 03 d2 a4 05 63 72 ba 8c ea 57 50 e0 6e Data Ascii: Z| @nw&)$7w<``ks]l!}.kB}QJBF9b_QQ*;42nqm4`4z).};~#\E#_Ebfy5>Q)|CWDa<SM"~|&V^(I p=l9R%x\crWPn
2022-08-11 03:08:21 UTC	86	IN	Data Raw: 99 ab a8 b0 b0 e0 a2 29 10 8d 5b 63 40 d0 e5 5a 4d ff 00 08 fe b5 6c 02 ff 00 c4 b5 7d e1 f7 96 fd bb 5a 51 2a 39 d3 2c 25 fc 86 6d 3f 4a 1d c6 77 d0 cf 34 92 58 e9 65 0b 61 4c f2 e2 f3 ee 20 8a 3f f9 9d ae 68 cb 89 79 1b f0 a4 6e df 37 36 fd 05 7f 62 ec eb f3 57 7f f3 d3 36 07 b4 67 67 d6 3c 4a a8 5e 8a 45 cd 5a 80 15 bd 65 db 56 3a 01 47 0f 84 12 4b a5 fe a4 9e 42 a1 09 9a 69 92 35 f5 bb 56 14 13 dd 29 61 d5 c5 8d 21 24 e4 24 73 a8 59 54 18 47 f1 29 b5 11 d4 1a 49 46 57 b0 63 b1 1b 1a 78 64 43 c9 8e 53 56 00 d6 7e d2 7f de d2 af 87 3d 72 31 ff 00 28 af fb af f1 7f f1 e3 ad aa f4 32 b5 66 c3 e0 ff 00 fc 41 46 db 70 d7 d0 57 2a b5 5d f1 2b 7d 04 27 5f 98 a3 f6 55 16 f0 f7 95 77 3e a7 dd 68 2a c3 f6 ad a8 0e 26 8b b4 69 7b 66 bd cf 40 35 35 93 03 89 9a da Data Ascii:)[c@ZMl}ZQ*9,%m?Jw4XeaL ?hyn76bW6gg<J^EZeV:GKBi5V)a!$$sYTG)IFWcxdCSV~=r1(2fAFpW*]+}'_Uw> h*&i{f@55
2022-08-11 03:08:21 UTC	87	IN	Data Raw: 6c dd a1 23 0f 48 d0 2d 34 87 14 6d ae 5b fc d8 5c d6 6e cd ec 57 5d 40 93 6f 30 fa d1 59 f1 e2 d7 1d f2 9f e9 59 9a 31 f1 0b 0a c9 d9 d1 a3 6f 89 c5 bc e3 f8 21 43 12 9f 9b 13 4b d9 b8 8e e2 76 b6 12 76 d5 b9 46 fb 07 fe 86 b5 b1 a1 c4 1e 55 6e 22 c7 af 05 88 17 3c b4 03 a9 34 65 ed 07 95 f5 24 aa d1 96 19 c6 f9 63 49 07 ff 00 ac de ad da 78 90 3f c5 8b f9 c7 5a d1 d8 55 f2 91 5b 50 e6 2a fc 41 d4 b7 cb ad 2e 6b 70 3e 74 c7 0a 18 f2 95 81 f9 8f 75 af ed fa 56 55 2f f2 fa d3 26 17 0d 0f 44 00 7e b4 4c 33 96 20 f7 93 03 7f 20 41 ae ef b1 d3 97 7b 3c a5 8f f1 b9 fe 8b 57 96 56 1a 66 91 97 f9 5a 8f fd 4e 8c 37 8a 76 73 ce d7 a9 7b ec 4a 48 10 4c 52 cc 9b 12 79 30 27 46 06 a5 84 06 98 a4 79 5b 30 02 cc ff 00 20 28 b3 96 07 5b 02 9e 40 0d aa 39 e2 ce ab a1 1e Data Ascii: l#H-4m[\nW]@o0YY1o!CKvvFUn"<4e$clx?ZU[P*A.kp>tuVU/&D~L3 A{<WVfZN7vs{JHLRy0'Fy[0 ([@9
2022-08-11 03:08:21 UTC	88	IN	Data Raw: a5 9d 4a c4 35 00 8d 5a 92 74 2a 0e 62 86 d5 dc f6 b4 8c bb 4c 8b 27 cf 63 c0 0a 96 5c 24 f9 7c 44 48 a4 8a e5 d3 4f 66 de e7 4f 70 7f 60 77 60 88 35 3f ca 92 25 da ed cc d6 9a 6f 5a 7a d3 36 d4 56 78 4d ad 96 4d 8f 43 59 40 d7 f1 4e c6 ff 00 2a 25 71 36 df 30 23 e7 47 ed 71 db 9d 80 3e 9b d0 ef f1 4c 0e 84 c6 3f 93 11 5f da 66 03 96 2a 40 7f fd 6b 7f d5 a9 61 3e 2d 99 c2 fd 6a 72 cd 18 3c 8a f9 a8 bd 46 8d 10 4b f8 58 5c fa d6 43 71 5e 1a 08 ac dd 01 a2 d7 63 b9 a2 45 0b 5e ad 7e 1a 56 5c 16 6e 6e d2 b1 f4 8d 6d 57 9a 7f f8 68 c3 e5 6a 02 69 ad cc 91 7f 4a 27 b5 70 dd 44 29 4a 3b 55 93 93 c0 e2 93 7c a3 41 4a 5d 85 b4 34 c9 8a 78 82 dc a3 95 20 f4 15 0f 7c e1 56 dd 6d 4b f1 1a 8e 3c 66 15 99 46 51 22 de f4 aa 4b 30 b9 37 16 eb 49 04 8c 90 80 5c b0 67 1f Data Ascii: J5Zt*bL'c\$|DHOfOp`w`5?%oZz6VxMMCY@N*%q60#Gq>L?_f*@ka>-jr<FKX\Cq^cE^~V\nnmWhjiJ'pD)J;U|A J]4x |VmK<fFQ"K07I\g
2022-08-11 03:08:21 UTC	90	IN	Data Raw: 07 11 42 ae 6e 4d 5c fb 02 f5 ca ac 37 b7 ad 27 c6 28 1f c2 09 f9 53 30 a2 49 bb 1a c2 e1 8f 79 a8 70 6e 08 3a dc 53 4d 23 1c da 9d d8 9b 9f 99 34 a4 9b 13 6b e9 e7 44 ec 69 98 5c d5 89 34 1a 41 d1 7f 5a fc 0b f0 a9 fa 9a b4 78 74 f3 2c 7e 54 1a 06 ea 1c d7 78 ad 4b 0e 34 a2 a6 5f ba 17 fd e3 7d eb 5a 6c 3e 2f 0b 38 de 39 55 a8 e6 39 79 ea 28 dc 13 bd 0c 57 65 62 22 23 52 86 ae a2 f5 68 fd 6b fb 16 14 ff 00 e1 2f e9 59 90 01 56 c1 e2 bf e1 3f e9 44 a2 7a 0e 04 c8 64 3b 13 7f a5 5c 9a 39 aa f2 5b e1 50 3f dc 39 e7 2f c9 07 f3 35 a7 1b 73 e7 44 8d 68 ed ec 46 bb c8 28 1b e5 1f 5a 27 76 a5 e1 3a ed 20 3e a2 a7 41 76 50 7d 0d 34 20 93 04 b9 7a a8 cd fa 52 e2 18 84 63 e9 ce a7 c4 92 a1 58 a0 36 6c 80 9b 9e 84 8a 73 a5 b6 a2 37 ab 28 b5 1d 00 fc 4d b5 18 ed d6 Data Ascii: BnM\7'(S0Iypn:SM#4kDi\4AZxt,~TxK4_}Zl>/89U9y(Web"#Rhk/YV?Dzd;\9[P?9/5sDhF(Z'v: >AvP}4 zRcX6ls7(M
2022-08-11 03:08:21 UTC	91	IN	Data Raw: 05 61 9a 2e f5 64 25 ad a9 b0 b7 96 56 1b 83 d3 81 35 71 b1 a4 95 32 b7 d7 a5 32 13 5e 2a de 81 89 57 a5 6a 45 58 11 56 61 47 2d 5c d5 94 50 24 1a f1 65 35 18 60 72 8a cb e3 3b 2a 96 f9 0a 24 5c ee 75 3e f4 5a af 56 36 f7 9a fb 3d ec f9 db f0 47 fc da b5 e0 14 1a c8 0c d2 0f bc 6d bf 74 70 b5 02 6a c9 7b d2 87 21 8e b4 cc 6f 71 6e 94 48 df 85 b5 e1 6a b6 94 0f 3d 69 30 d8 32 a1 14 4e d8 88 82 d8 5e 56 1f b8 48 b2 93 b3 13 a5 aa 0c 0c 50 9c 16 37 bd 9c 47 dd 64 40 40 19 5a d2 91 9b 5d f4 f1 54 bd a3 65 c5 40 92 2a d9 95 64 03 56 da c4 9a c1 4c 8a 61 12 e0 dc 82 40 89 98 2d b9 1c 8f 5d af 0e c2 2c 52 f2 2a 72 39 f9 1d 09 ac 0c b2 77 6c 5e 29 97 78 e4 19 48 f9 1a 8c 8d 08 a3 62 53 a6 dc 8f 95 76 63 1e f5 23 10 4a 4f 89 14 e5 17 a8 c0 fb bb 15 1d 36 a3 71 7f Data Ascii: a.d%V5q22^*WjEXVaG-\P$e5`r;*$\u>ZV6=Gmtpj{!oqnHj=i02N^VHP7Gd@@Z]Te@*dVLa@-],R*r9wl^)xHbS vc#JO6q
2022-08-11 03:08:21 UTC	92	IN	Data Raw: 55 c9 24 d0 ab 55 c7 b0 28 1a 56 b9 51 4d 19 b1 ab 30 60 48 3d 46 95 39 b0 32 13 eb ad 49 6b dd 6a 64 75 75 52 1c 02 34 d7 46 d0 82 39 83 58 d9 58 95 88 46 96 20 3b f9 f4 5a 48 22 48 d3 f0 8e bb 93 d4 f1 b1 db d9 34 5e 06 53 f9 49 1c 2c 6a d5 b7 11 7a 24 e5 14 f2 b8 51 f3 3d 29 41 8e 35 1a 5c 0a cf 3c ef f1 4a df ad bd e6 95 7e 1a 51 e3 1f 69 f6 d4 10 4f 88 31 44 ee ec ec 3f 11 c9 b2 af 99 ae d7 81 a6 ec 6c 5e 29 a0 ec 6f b4 f7 c7 19 dc 82 65 2e d7 41 7f 8d 8d 62 25 ec b9 13 15 32 41 81 ec d3 3c 18 3c 90 e5 97 13 2b 1c ba 87 eb ce 88 84 03 6b 80 07 b9 38 89 96 2d 86 ee 7a 2d 00 00 02 c0 0b 01 46 e0 01 72 68 20 3a dc f3 34 55 81 1c a9 3b 13 b5 70 97 88 b6 1c 2c a9 13 01 98 f7 4e 73 b5 bf f1 13 9f c4 b5 08 fb 2c 91 cd de 61 e6 2c 7b d4 20 8d ab ba 0f 8a c0 Data Ascii: U$U(VQM0`H=F92IkjduuR4F9XXF ;ZH"H4^SI,jz$Q=)A5\<J~QiO1D?I^)oe.Ab%2A<<+k8-z-Frh :4U;p,Ns,a,{
2022-08-11 03:08:21 UTC	94	IN	Data Raw: 08 34 a2 49 d6 b9 f0 63 4d 1a 33 74 1f 53 43 b2 fb 1f 07 83 23 ef 02 f7 b3 9e b3 49 a9 1f 2f 60 0d 7d 82 58 d7 dc 62 57 ff 00 33 fa ad 7d 00 a1 a5 a8 9e 7b f0 cb 56 1e de 86 bb d9 db a2 e9 57 78 c7 57 5a 0b 87 41 e5 5a 71 b0 a2 0d 65 52 6b 52 37 26 95 2c b7 b1 ad 45 5e ac a6 b7 ab 9a bf da 57 aa a9 ab 13 56 34 01 ad 78 9a 23 5a 06 77 61 b3 d9 bf cc 2a 23 8e 9d 25 8c b2 3f 77 25 c9 b0 0c 50 6c 69 54 b3 c3 88 7b b2 82 d9 80 3e 55 0b 2a ab c8 aa 21 25 58 db 71 b0 35 84 85 15 89 95 a3 40 2e c8 a4 81 c8 66 ac 34 2c b2 43 2b 18 da e2 f6 da fc c8 34 93 2e 1d e1 c4 59 5e e2 ca 72 87 23 40 54 53 03 2c 69 8a 72 54 5c 17 17 b3 13 cf ca b1 d0 80 b3 c0 af 1a 9d 5f 3e 62 f5 87 40 1a 31 a1 5b db f3 0f 95 2a 22 a2 9b bb 58 81 f8 58 fd 79 d4 51 ce 7b d6 78 41 5f 16 7b 21 Data Ascii: 4IcM3tSC#I/`}XbW3}{VWxWZAZqeRkR7&,E^WV4x#Zwa*#%?w%PliT{>U*!%Xq5@.f4,C+4.Y^r#@T S,irT_>b@1[*"XXyQ{xA_{!

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	95	IN	Data Raw: 50 a8 0d dd 28 2e 5f e2 28 f6 a8 b3 84 80 45 60 ba a3 3b 43 20 6e 60 ab 5c 53 99 99 20 8a 55 96 33 9f b9 2c 03 8b f3 55 7b 06 1e 86 b1 f0 26 41 85 91 09 24 90 d0 b0 37 3f 5a 24 0b 0b 0a d7 7f 63 ce b1 18 b9 4c 78 74 04 8f c6 cd a2 a0 ea c7 fa 56 1f 03 e3 43 de 4d b1 99 87 f2 41 f9 69 89 37 3c 05 c1 ad 4d 64 ec 98 74 fc 4e ed c0 56 bc 0f b1 9a cb 45 88 51 bb 10 a3 e7 4a 90 ac 76 d1 40 14 d1 6e 6e bc 8f 01 ec 79 f0 54 17 26 9e 43 6d 85 00 05 5a 8b 35 00 2b ec 98 cc 8c 6c 92 e9 f3 e4 6a f6 35 6f 62 e7 7a dc 71 d0 d7 21 c3 22 96 1b ec 28 61 b0 92 62 0d 81 40 02 df e2 26 c2 bc 47 86 b5 e5 ec ed 52 43 22 ba 9d 41 a4 ec ae d7 92 38 12 d8 4c 42 77 f8 61 c9 11 8d 9d 07 f0 35 15 60 ca 6c c3 62 29 85 9d 34 ea 2a 37 36 16 07 cf 5a 58 d8 97 74 4b f3 23 4a 8e 25 37 b3 Data Ascii: P(._(E`;C n`\S U3,U{&A$7?Z$cLxtVCMAi7<MdtNVEQJv@nnyT&CmZ5+lj5obzq!"(ab@&GRC"A8LBwa5`lb)4 *76ZXtK#J%7
2022-08-11 03:08:21 UTC	96	IN	Data Raw: 00 04 4b 10 4d dc ec b7 e4 3a d7 76 e1 9e 73 9f bc 0c c1 37 73 b0 5a c6 4b 35 c8 50 d6 b9 0d b2 03 b2 e9 b9 ab 8b 4b 89 72 36 21 06 40 6a 38 a7 74 2c 40 16 b5 f5 d2 87 2a 15 72 fd a2 e3 62 62 83 d7 67 7f e8 38 5d aa fe d8 37 bd 7d a7 07 95 db ef a2 16 7f 31 c9 a8 1c d4 58 d0 5a 2d e9 ec de 4c 61 e8 10 56 bc 05 bd 8d f8 8e 1a d1 69 6a cb a5 1b 56 be f2 c4 13 b6 f4 59 98 fc 46 ac a0 1e 95 9f b3 c2 73 8a 46 5f 91 d4 55 c9 ad 3d b5 55 67 73 e1 51 73 f2 a6 9a 67 91 c5 99 b7 f2 e8 28 01 56 14 2e 05 68 2b 52 2a e6 c4 50 16 5e 75 88 c7 63 f0 98 5c 33 15 9e 57 b0 71 a1 8d 06 ac df 21 4a 8b 1e 1b 0c 0e 55 50 2e 77 f5 35 64 60 0d af a1 23 a5 61 e3 c5 36 24 8c ee a3 2c 64 fe 40 77 a7 76 b0 16 5a b1 1e b4 b3 e2 5a fb a5 d3 f9 93 5d 0e b5 88 c4 62 21 c3 25 83 4a f9 73 Data Ascii: KM:vs7sZK5PKr6!@j8t,@*rbbg8]7}1XZ-LaVijVYFsF_U=UgsQsg(V.h+R*P^uc\3Wq!JUP.w5d`#a6$,d@wvZZ]b!%Js
2022-08-11 03:08:21 UTC	98	IN	Data Raw: 5d cd 94 6b 61 4c 5a 36 88 00 8a f6 60 76 61 4e d3 b8 39 b3 30 f1 b3 73 f2 a5 fb 5b a2 dc 64 5c cb ce e7 90 a8 b0 b8 78 22 98 1e f0 46 b9 80 17 b7 91 a1 14 41 2d a8 14 49 a3 98 f0 f1 7b 17 a3 c7 4a b0 b7 b0 00 b9 36 16 a6 9f 2e 2b 18 84 45 bc 71 1d df cd bc b8 8b 7b 57 a1 c4 70 24 8e 1a f0 1c 77 ab fb 56 f7 97 35 9b 07 8f ff 00 f1 9f f9 70 b6 f4 00 24 d6 60 5c fd 28 12 45 64 53 98 6a 6c 2a ee 17 a1 b9 a5 c3 f6 73 e3 59 7e f3 14 6e 3f 81 74 55 a6 c7 9c 68 40 0c 41 7b b8 9f e2 ea 69 64 84 40 ee 21 99 13 21 be 9b 73 15 d9 78 72 d3 49 8d 99 dc b6 ca 43 3b 13 d2 a6 9f b4 22 30 67 c2 a3 8d 10 31 24 22 6e e4 1d af 48 56 47 38 b9 f2 2a 96 23 76 21 7a 52 18 c3 8f 0a ba df 72 d6 f5 bd 23 4e 8a a0 73 20 f3 35 12 e3 0e 26 45 19 8f 78 56 fc 82 28 ac 22 48 c0 cc ec 77 Data Ascii:]kaLZ6`vaN90s[d\x"FA-I{J6.+Eq{Wp$wV5p$`\(EdSjl*sY~n?tUh@A{id@!!sxrIC;"0g1$"nHVG8*#v!zRr#Ns 5&ExV("Hw
2022-08-11 03:08:21 UTC	99	IN	Data Raw: 01 14 49 de c6 c8 33 3b 39 1d 3a 0a 95 f1 31 b9 8c f7 45 2c 83 62 2d fe b4 a2 46 0f 6e f6 d6 4b 6d 6a cd c1 24 56 47 17 56 16 35 32 c6 f7 ca 75 b0 f8 88 1b 1b d4 82 35 8b 52 f9 89 22 93 0e a1 01 05 61 82 f2 9d f3 3c 9c 85 05 89 e4 0b 6b b0 20 f2 50 34 15 1f d9 8b 15 6e f0 31 16 00 9b eb a1 5a 9e 44 46 c9 85 63 6d 4b 9b 35 e8 09 31 10 fc 4a 1c 7c b4 35 72 6a e4 81 b5 6b ed 8b d6 27 b5 f1 9f 67 80 94 45 01 a7 9b 71 12 1f d5 8f e5 15 06 13 0d 16 1b 0d 1e 48 63 16 55 fe a4 f3 63 cc d5 8d 69 56 2b c6 c4 03 ec 1e 1a 69 42 87 b2 c7 1a 86 54 60 b9 4b 0a 3a 81 d3 4a b0 f7 5a d5 aa f8 49 7a a8 cd f4 f7 7a 56 82 ae 68 c6 b3 cd fe 1c 46 df c4 fe 15 a0 a0 2d b6 15 7e 2d 8a 9e 2c 3a 69 9c f8 8f 45 1b 9a 0f f6 4c 2c 50 88 b0 98 70 15 15 76 24 e9 59 49 55 72 19 05 97 2e Data Ascii: I3;9:1E,b-FnKmj$VGV52u5R"a<k P4n1ZDFcmK51J|5rjk'gEqHcUciV+iBT`K:JZIzzVhF-~-,:iEL,Ppv$YIUr.
2022-08-11 03:08:21 UTC	100	IN	Data Raw: 5e a9 bd 61 b1 18 88 fb 42 15 52 a2 22 11 c6 e7 36 84 1a 46 c3 e1 95 c0 cc 65 b8 3e 82 a7 92 40 25 52 d2 96 7c c4 9d 6e db 9a 75 c5 19 5d 2e f9 b2 9f 96 99 aa 29 5d c3 ea 72 ed 7d 05 28 0a 46 c3 4a 29 85 62 4d c9 2a a0 7a 9d ab 14 d8 c8 d6 ee 30 d1 2a 90 43 65 16 3b b3 75 34 d8 cc 66 17 0c 1c 95 69 03 6b f0 8d 8d 64 c2 c4 a7 4b 20 ac 42 e2 13 17 86 8c ba 4a a3 30 1d 6a 64 53 24 aa ea cd 3d d5 5b 43 94 d0 c4 4a 15 9a c2 d7 34 22 c5 47 3a 03 92 36 56 0a 28 4b 1a 16 8a 36 22 e0 93 be 84 d0 6a f9 d1 82 50 f7 f0 91 66 f4 a1 ab 03 70 76 a0 2f 56 02 fb 9e 36 0f da 32 0d 5e f1 c1 e4 bf 99 bd 92 1f 3a 39 47 f8 87 f5 eb 5a e5 c4 00 a7 93 8f c0 7f d2 ae 6f c2 cd c2 e6 b5 f6 35 e0 38 6a 6a cc 0d 5c 50 f6 c7 b9 b3 45 30 e7 e0 6f e9 ed 6f 6a d3 80 37 25 ac a0 5c b1 e4 Data Ascii: ^aBR"6Fe>@%R|nu].)]r}(FJ)bM*z0*Ce;u4fikdK BJ0jdS$=[CJ4"G:6V(K6"jPfpv/V62^:9GZo58jj\PE0ooj7%\
2022-08-11 03:08:21 UTC	102	IN	Data Raw: fd 05 08 70 79 8c 81 5d dd e3 2a 7f 5a c4 63 e2 43 11 90 18 dc 5e 31 aa e6 5a 2b 8c 8a 60 8c ba 2e a7 62 39 da ac 6a de 94 8c ac ae 2e ac a5 48 ea 2a 05 8e 34 b6 61 18 b2 5f 52 2a 41 8a 95 70 d1 87 45 39 73 1e a3 db d6 79 88 d4 b0 45 f4 1a 9a d3 86 9e f1 83 19 a1 d1 f9 8e 4d 59 96 fa f4 23 a1 e8 68 8b 0a f3 ab d0 bd 02 46 b5 b7 0b f3 e3 bf b1 60 28 01 4a 05 3b de d4 06 bc fa 9a 8d 74 67 17 a2 c7 c1 13 bf a2 d6 35 c7 e1 58 c7 99 b9 a5 b8 32 b9 7f 23 a0 a5 51 60 2c 38 17 81 25 51 ac 6f fc 9a ba d0 16 e9 44 7b 21 40 a2 4f b0 32 dc d0 7e cb c4 03 cb 11 0b 0a d6 fc 00 3c 7a ec 45 34 f1 43 8d 97 52 17 ba 04 7c 63 46 6a 8a 1c 14 d2 30 2c c2 42 05 f9 69 58 ac 39 8a 58 c7 f7 a8 0e fa 11 7f d4 54 f2 24 51 02 4e 46 62 23 b1 bd 5e de 94 22 8d a4 2a 48 51 b0 a8 82 b1 Data Ascii: py]*ZcC^1Z+`.b9j.H*4a_R*ApE9syEMY#hF`(J;tg5X2#Q`,8%QoD{!@O2~<zE4CR|cFj0,BiX9XT$QNFb#^'"*HQ
2022-08-11 03:08:21 UTC	103	IN	Data Raw: 23 37 e7 5a 8a b0 fd 8f bc 8d 93 6b 8d 0f 43 46 d6 22 cc a6 c7 d6 af b7 ec b7 96 43 d5 bd c6 bc 6e c0 53 12 c6 fb 91 90 f2 00 0f d6 95 c6 78 99 6f 7d b9 9a 36 ba 9f 09 b6 a3 91 14 e0 dc 2d f4 b9 34 aa ac c0 ee 97 0a db 05 a9 30 f2 87 80 34 0f d0 6a a6 82 95 4c 6a e4 6f 88 6c 69 24 b3 a1 05 4e b7 15 70 c0 80 54 ee 08 b8 ae cd 9f 68 bb a6 3c e2 39 6b 17 87 24 c0 7e d0 a3 70 05 9c 0a 05 6e 3a db d2 b5 d3 50 2a e6 8d ef 7a d2 b3 61 01 f3 f6 6d 56 2a dd 08 35 9a c6 b4 fd 93 ba c4 09 07 e1 93 46 fe 21 ec ed fb 05 81 ae 7e 7c 05 b8 0f 64 f0 22 32 f6 d4 ed 5e 03 73 60 35 00 1b 6f ca 94 14 36 24 ab 5a dd 46 f5 98 39 44 f0 15 25 7a 83 7b d4 91 1d 4e 78 d6 c4 1b e9 51 e7 77 24 78 c6 63 71 b5 b9 0a 62 cc 2f 72 df cb e7 41 89 41 7b 6c 55 b6 bf 5a c5 e0 a4 3f 65 94 b0 Data Ascii: #7ZkCF"CnSxo}6-404jLjoli$NpTh<9k$~pn:P*zamV*5F!~|d"2^s`5o6$ZF9D%z{NxQw$xcqb/rAA{lUZ?e
2022-08-11 03:08:21 UTC	104	IN	Data Raw: 79 8e 43 66 92 f6 9a 7d 95 86 84 8a c6 bf fd 1e c9 08 a1 fa b4 43 e4 63 e8 52 1a 52 4d 32 70 f1 93 42 1e 12 6c d3 8a 8a 46 93 e7 0d a4 79 8a 49 e7 57 fe 8f 65 15 87 eb 44 78 78 d7 5c a6 58 b9 12 22 92 78 d2 f7 0c 79 4c 46 ad fd c7 b9 92 f5 ac 6c 4c 65 9a de d5 84 21 11 e8 d3 f7 0d 71 65 de 54 ad b5 1e 5a 13 66 af fd 1e e6 3f 51 ba 25 a8 df 44 65 fb 13 16 2c d4 76 b0 90 88 8b 84 8d 3e df f8 4f 55 c1 b4 69 ca ec 46 a4 9a e0 d2 e3 5b fd c6 a4 55 dd f3 bd fa 9a d2 f8 2c b2 32 68 f3 47 dc 1c d0 f9 c2 11 1c 43 b3 ea 17 52 34 5f e7 5f bc 6b 3a 49 d1 a5 a9 7a b0 11 f5 3e f2 0e e2 b7 4b d2 63 74 9b 24 ed b7 9b 13 c3 ad 89 91 ef 1a 7e f6 ef e0 d6 57 a6 cb f1 92 68 84 bc a2 99 f5 1d 44 8b a9 a7 fd 96 7d 4f b8 d1 7d ad 8f 0d 7a 7a d2 a5 5f bc 5e ea 64 63 05 ee 56 c6 Data Ascii: yCf}CcRRM2pBlFyIWeDxx\X"xyLFlLe!qeTZf?Q%De,v>OUiF[U,2hGCR4__k:Iz>Kct$~WhD}O}zz_^dcV

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	56425	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	107	OUT	GET /lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: sweetiestouch2u.com

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:22 UTC	108	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:22 GMT Content-Type: image/svg+xml Content-Length: 364 Connection: close Last-Modified: Tue, 10 May 2022 09:38:15 GMT ETag: "627a3287-16c" Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Cache-Control: max-age=1800 CF-Cache-Status: EXPIRED Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=z3tGogxMMQLZrGL94rrue4Ys2d31RVEk uHBYNlmfeRDqVP%2FOnO%2B8FF9qV%2BC%2FpozQOW3fkNomUCNCpobNlwkrwUdTVPH2RPvhUYcncOOY Uk81AvC7pIalaYHEtMXey1Sudq5D5CzD"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc42c9e47bb43-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-08-11 03:08:22 UTC	109	IN	Data Raw: 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 37 39 32 22 20 77 69 64 74 68 3d 22 31 37 39 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 23 66 66 66 22 20 64 3d 22 4d 31 34 39 30 20 31 33 32 32 71 30 20 34 30 2d 32 38 20 36 38 6c 2d 31 33 36 20 31 33 36 71 2d 32 38 20 32 38 2d 36 38 20 32 38 74 2d 36 38 2d 32 38 6c 2d 32 39 34 2d 32 39 34 2d 32 39 34 20 32 39 34 71 2d 32 38 20 32 38 2d 36 38 20 32 38 74 2d 36 38 2d 32 38 6c 2d 31 33 36 2d 31 33 36 71 2d 32 38 2d 32 38 2d 32 38 2d 32 38 2d 36 38 74 32 38 2d 36 38 6c 32 39 34 2d 32 39 34 2d 32 39 34 2d 32 39 34 71 2d 32 38 2d 32 38 2d 32 38 2d 32 38 2d 36 38 74 32 38 2d 36 38 6c 31 33 36 2d 31 33 36 71 32 38 2d 32 38 20 36 38 Data Ascii: <svg height="1792" width="1792" xmlns="http://www.w3.org/2000/svg"><path fill="#fff" d="M1490 1322q0 40-28 68l-136 136q-28 28-68 28t-68-28l-294-294-294 294q-28 28-68 28t-68-28l-136-136q-28-28-28-68t28-68l294-294-294-294q-28-28-68t28-68l136-136q28-28 68
2022-08-11 03:08:22 UTC	109	IN	Data Raw: 20 32 38 20 32 38 20 36 38 74 2d 32 38 20 36 38 6c 2d 32 39 34 20 32 39 34 20 32 39 34 20 32 39 34 71 32 38 20 32 38 20 32 38 20 36 38 7a 22 2f 3e 3c 2f 73 76 67 3e Data Ascii: 28 28 68t-28 68l-294 294 294 294q28 28 28 68z"/></svg>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	60753	142.250.185.132	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:15 UTC	1	OUT	GET /url?q=%68%74%74%70%73%3A%2F%2F%74%6F%2D%63%6C%69%63%6B%2E%66%75%6E%2F%65%72%69%58%46%76%4B%56%48%63%36%23%79%65%78%6F%72%79%76%6A%78%6A&sa=D&sntz=1&usg=AOvVaw2t3jeNlZEFZI-xvhukbEyl HTTP/1.1 Host: www.google.com Connection: keep-alive sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" sec-ch-ua-mobile: ?0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 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 X-Client-Data: CKqPywE= Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+620
2022-08-11 03:08:15 UTC	3	IN	HTTP/1.1 200 OK Location: https://to-click.fun/eriXFvKVHc6#yexoryvjxj Cache-Control: private Content-Type: text/html; charset=UTF-8 Strict-Transport-Security: max-age=31536000 BFCache-Opt-In: unload P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Date: Thu, 11 Aug 2022 03:08:15 GMT Server: gws Content-Length: 385 X-XSS-Protection: 0 Expires: Thu, 11 Aug 2022 03:08:15 GMT Set-Cookie: __Secure-ENID=6.SE=D5t-FZQmyWJrPyIzdaZOwvH2osJo-1hZZX8jDPCgZipXhAmKawj9FI-pRi_SisI8c6k3ETdr8rzoESEVPEzTQUiZVzZ2aK9mkLyhaLCqIEzV4GSxz7wd680xOBkLHhKQNLG79qJ-wL_KUqmmj1e2n5Bv9YHQSAMM01LtoYZmpmU; expires=Sun, 10-Sep-2023 19:26:33 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:15 UTC	4	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 52 65 64 69 72 65 63 74 69 6e 67 3c 2f 54 49 54 4c 45 3e 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 31 3b 20 75 72 6c 3d 68 74 74 70 73 3a 2f 2f 74 6f 2d 63 6c 69 63 6b 2e 66 75 6e 2f 65 72 69 58 46 76 4b 56 48 63 36 23 79 65 78 6f 72 79 76 6a 78 6a 22 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 6f 6e 4c 6f 61 64 3d 22 6c 6f 63 61 74 69 6f 6e 2e 72 65 70 6c 61 63 65 28 27 68 74 74 70 73 3a 2f 2f 74 6f 2d 63 6c 69 63 6b 2e 66 75 Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>Redirecting</TITLE><META HTTP-EQUIV="refresh" content="1; url=https://to-click.fun/eriXFvKVHc6#yexoryvjxj"></HEAD><BODY onLoad="location.replace('https://to-click.fu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	63811	5.161.54.249	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:16 UTC	6	OUT	GET /eriXFvKVHc6 HTTP/1.1 Host: to-click.fun Connection: keep-alive sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" sec-ch-ua-mobile: ?0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 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 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Referer: https://www.google.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-11 03:08:16 UTC	7	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 11 Aug 2022 03:08:16 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0 Expires: 0 Last-Modified: Thu, 11 Aug 2022 03:08:16 GMT Location: https://sweetiestouch2u.com/?utm_source=g3Ase2bbTdNbHV Pragma: no-cache Set-Cookie: _subid=ke01dc5ghv6;Expires=Sunday, 11-Sep-2022 03:08:16 GMT;Max-Age=2678400;Path=/ Set-Cookie: fc907=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWFtc1wiOntcIjI5OFwiOjE2NjAxODcyOTZ9LFwiY2FtcGFpZ25zXCI6e1wiMTQxXCI6MTY2MDE4NzI5Nn0sXCJ0aW1lXCI6MTY2MDE4NzI5Nn0ifQ.wqlTsClQ0ZdBgHGhlwLhdRKDsoiL74X1U3n8XIkmpBw;Expires=Friday, 22-Mar-2075 06:16:32 GMT;Max-Age=1660273696;Path=/ Vary: Accept-Encoding Access-Control-Allow-Origin: *

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	60942	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:16 UTC	8	OUT	GET /?utm_source=g3Ase2bbTdNbHV HTTP/1.1 Host: sweetiestouch2u.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/92.0.4515.107 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 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" sec-ch-ua-mobile: ?0 Referer: https://www.google.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:16 UTC	8	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Cache-Control: max-age=0, private, must-revalidate Cross-Origin-Window-Policy: deny Set-Cookie: k=SFMyNTY.g3QAAAAHbQAAAARhdW5xdAAAAAFtAAAABTk0ODE4bQAAAApwbFplcWJBa0 x3bQAAAANoaWRtAAAAJk1qVWRzbHZheUhBeHliZnJvQWhnTFdWenBFV3hOeGF0UVJ3c0VPbQAAAAJobG QAA25pbG0AAAAFc3ViXzFkAANuaWxtAAAABXN1Yl8yZAADbmlsbQAAAAd0cmFja2VybQAAAAdub3RyYW NrbQAAAAN1bnFtAAAADGpPaEFybGFkalFDVg.3k3I9_-D4wnzo68cXigHAQ_ZFbfr-qRRYcqme9n0EfM; path=/; expires=Fri, 11 Aug 2023 03:08:16 GMT; max-age=31536000 X-Content-Type-Options: nosniff X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Xss-Protection: 1; mode=block CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1CZmL2X9mJai5skH4QCqJVghKqQnm%2F xgwYAO94ZmxzpMi7%2BbfA83npJGOcWp6VwS1S20qc7XD%2BbeANfH8LaObP%2BZNSwY2XOZ2PJj5czp t9UwNyWQDuJad5rmfrec9F2FCPyIYzg2"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc40c4a679bd0-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-08-11 03:08:16 UTC	10	IN	Data Raw: 31 0d 0a 0a 0d 0a Data Ascii: 1
2022-08-11 03:08:16 UTC	10	IN	Data Raw: 32 30 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 Data Ascii: 200<!DOCTYPE html><html lang="en"><head><meta charset="UTF-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0,maximum-scale=1.0, user-scalable=no"><meta name="r
2022-08-11 03:08:16 UTC	10	IN	Data Raw: 66 66 61 0d 0a 75 62 73 65 74 3d 6c 61 74 69 6e 2d 65 78 74 22 29 3b 2e 66 61 64 65 49 6e 55 70 7b 61 6e 69 6d 61 74 69 6f 6e 3a 61 20 2e 34 73 20 66 6f 72 77 61 72 64 73 7d 40 6b 65 79 66 72 61 6d 65 73 20 61 7b 30 25 7b 6f 70 61 63 69 74 79 3a 30 3b 74 72 61 6e 73 66 6f 72 6d 3a 74 72 61 6e 73 6c 61 74 65 33 64 28 30 2c 32 72 65 6d 2c 30 29 7d 74 6f 7b 6f 70 61 63 69 74 79 3a 31 3b 74 72 61 6e 73 66 6f 72 6d 3a 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 7d 7d 62 6f 64 79 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 4d 6f 6e 74 73 65 72 72 61 74 2c 41 72 69 61 6c 2c 48 65 6c 76 65 74 69 63 61 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 36 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 34 7d 68 31 2c 68 32 2c 68 33 2c 68 34 2c 68 35 2c Data Ascii: ffaubset=latin-ext");.fadeInUp{animation:a .4s forwards}@keyframes a{0%{opacity:0;transform:translate3d(0,2rem,0)}to{opacity:1;transform:translateZ(0)}}body{font-family:Montserrat,Arial,Helvetica,sans-serif;font-size:16px;line-height:1.4}h1,h2,h3,h4,h5,
2022-08-11 03:08:16 UTC	11	IN	Data Raw: 7a 2d 69 6e 64 65 78 3a 33 3b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 75 70 70 65 72 63 61 73 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 37 35 72 65 6d 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 61 64 75 6c 74 20 73 70 61 6e 7b 74 65 78 74 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 6d 61 69 6e 7b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 Data Ascii: z-index:3;text-transform:uppercase;font-size:.875rem;display:-ms-flexbox;display:flex;-ms-flex-align:center;align-items:center;-ms-flex-direction:column;flex-direction:column}.adult span{text-shadow:none}.main{display:-ms-flexbox;display:flex;-ms-flex-dir
2022-08-11 03:08:16 UTC	13	IN	Data Raw: 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 2e 32 35 72 65 6d 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 7d 2e 67 75 72 6c 5f 5f 6e 61 68 20 2e 69 6d 67 20 69 6d 67 2c 2e 67 75 72 6c 5f 5f 79 65 61 68 20 2e 69 6d 67 20 69 6d 67 7b 77 69 64 74 68 3a 31 2e 35 72 65 6d 3b 68 65 69 67 68 74 3a 31 2e 35 72 65 6d 7d 2e 67 75 72 6c 5f 5f 6e 61 68 20 73 70 61 6e 2e 63 6f 75 6e 74 2c 2e 67 75 72 6c 5f 5f 79 65 61 68 20 73 70 61 6e 2e 63 6f 75 6e 74 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 35 72 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 7d 2e 62 74 6e 62 6f 78 7b 77 69 64 74 68 3a 31 Data Ascii: -items:center;-ms-flex-pack:center;justify-content:center;margin-bottom:.25rem;background:#fff}.gurl__nah .img img,.gurl__yeah .img img{width:1.5rem;height:1.5rem}.gurl__nah span.count,.gurl__yeah span.count{font-size:1.25rem;line-height:1}.btnbox{width:1
2022-08-11 03:08:16 UTC	14	IN	Data Raw: 66 62 37 0d 0a 72 65 6d 3b 6d 69 6e 2d 77 69 64 74 68 3a 36 2e 35 72 65 6d 3b 68 65 69 67 68 74 3a 36 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 20 31 72 65 6d 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 62 74 6e 2d 2d 72 6f 75 6e 64 20 69 6d 67 2e 74 69 6d 65 73 2c 2e 6e 6f 74 2d 62 74 6e 2d 2d 72 6f 75 6e 64 20 69 6d 67 2e 74 69 6d 65 73 7b 77 69 64 74 68 3a 33 72 65 6d 3b 68 65 69 67 68 74 3a 33 72 65 6d 7d 2e 62 74 6e 2d 2d 72 6f 75 6e 64 20 69 6d 67 2e 68 65 61 72 74 2c 2e 6e 6f 74 2d 62 74 6e 2d 2d 72 6f 75 6e 64 20 69 6d 67 2e 68 65 61 72 74 7b 77 69 64 74 68 3a 33 72 65 6d 3b 68 65 69 67 68 74 3a 33 72 65 6d 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a Data Ascii: fb7rem;min-width:6.5rem;height:6.5rem;margin:0 1rem;-ms-flex-direction:column;flex-direction:column}.btn--round img.times,.not-btn--round img.times{width:3rem;height:3rem}.btn--round img.heart,.not-btn--round img.heart{width:3rem;height:3rem;margin-top:

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:16 UTC	15	IN	Data Raw: 62 74 6e 62 6f 78 20 61 2c 2e 73 74 65 70 2e 61 63 74 69 76 65 20 2e 73 74 65 70 5f 5f 68 65 61 64 65 72 7b 6f 70 61 63 69 74 79 3a 31 7d 2e 73 74 65 70 2e 68 69 64 64 65 6e 20 2e 73 74 65 70 5f 5f 62 6f 64 79 2c 2e 73 74 65 70 2e 68 69 64 64 65 6e 20 2e 73 74 65 70 5f 5f 66 6f 6f 74 65 72 2c 2e 73 74 65 70 2e 68 69 64 64 65 6e 20 2e 73 74 65 70 5f 5f 68 65 61 64 65 72 7b 6f 70 61 63 69 74 79 3a 30 7d 2e 62 67 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 21 69 6d 70 6f 72 74 61 6e 74 3b 7a 2d 69 6e 64 65 78 3a 30 7d 2e 62 67 2c 2e 62 67 3a 61 66 74 65 72 7b 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 31 30 30 25 3b 6c 65 66 74 3a 30 3b 74 6f 70 3a 30 3b 72 69 67 68 74 3a 30 3b 62 6f 74 74 6f 6d 3a 30 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d Data Ascii: btnbox a,.step.active .step__header{opacity:1}.step.hidden .step__body,.step.hidden .step__footer,.step.hidden .step__header{opacity:0}.bg{position:fixed!important;z-index:0}.bg,.bg:after{width:100%;height:100%;left:0;top:0;right:0;bottom:0;display:block}
2022-08-11 03:08:16 UTC	17	IN	Data Raw: 62 65 3c 2f 61 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 64 75 6c 74 22 3e 3c 73 70 61 6e 3e 61 64 75 6c 74 20 6f 6e 6c 79 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 6d 61 69 6e 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 74 65 70 62 6f 78 22 3e 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 74 65 70 22 3e 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 74 65 70 5f 5f 69 6e 65 72 22 3e 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 74 65 70 5f 5f 68 65 61 64 65 72 22 3e 3c 68 31 20 63 6c 61 73 73 3d 22 74 2d 63 65 6e 74 65 72 22 3e 57 68 6f 20 69 73 20 74 68 65 20 68 6f 74 74 65 73 74 20 6f 6e 65 3f 3c 2f 68 31 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d Data Ascii: be adult only <main class="main"> <h1 class="t-center">Who is the hottest one?</h1> <div class=
2022-08-11 03:08:16 UTC	18	IN	Data Raw: 31 30 33 33 0d 0a 3c 69 6d 67 20 63 6c 61 73 73 3d 22 74 69 6d 65 73 22 20 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 64 36 63 34 63 31 30 38 61 37 65 65 39 39 32 33 66 38 32 65 32 33 30 36 62 63 62 39 63 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 68 65 61 72 74 2d 72 65 64 2e 73 76 67 22 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 6f 75 6e 74 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 6f 76 65 72 2d 73 6c 69 64 65 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 61 76 61 74 61 72 20 6c 61 7a 79 6c 6f 61 64 22 20 64 61 74 61 2d 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 Data Ascii: 1033<img class="times" src="/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart-red.svg"> <div class="gurl__avatar lazyload" data-src="/lstatic/ae
2022-08-11 03:08:16 UTC	19	IN	Data Raw: 36 62 63 62 39 63 2f 69 6d 61 67 65 73 2f 6d 35 2e 6a 70 67 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 73 74 61 74 69 73 74 69 63 22 3e 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 6e 61 6d 65 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6d 67 22 3e 3c 69 6d 67 20 63 6c 61 73 73 3d 22 74 69 6d 65 73 22 20 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 64 36 63 34 63 31 30 38 61 37 65 65 39 39 32 33 66 38 32 65 32 33 30 36 62 63 62 39 63 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 74 69 6d 65 73 2d 62 6c 75 65 2e 73 76 67 22 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 6f 75 6e 74 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 79 65 61 68 22 3e Data Ascii: 6bcb9c/images/m5.jpg"> <img class="times" src="/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times-blue.svg">
2022-08-11 03:08:16 UTC	21	IN	Data Raw: 61 73 73 3d 22 74 69 6d 65 73 22 20 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 64 36 63 34 63 31 30 38 61 37 65 65 39 39 32 33 66 38 32 65 32 33 30 36 62 63 62 39 63 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 68 65 61 72 74 2d 72 65 64 2e 73 76 67 22 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 6f 75 6e 74 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 6f 76 65 72 2d 73 6c 69 64 65 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 61 76 61 74 61 72 20 6c 61 7a 79 6c 6f 61 64 22 20 64 61 74 61 2d 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 64 36 63 34 63 31 30 38 61 37 65 65 Data Ascii: ass="times" src="/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart-red.svg"> <div class="gurl__avatar lazyload" data-src="/lstatic/ae9d6c4c108a7ee
2022-08-11 03:08:16 UTC	22	IN	Data Raw: 2f 6d 31 30 2e 6a 70 67 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 73 74 61 74 69 73 74 69 63 22 3e 20 0d 0a Data Ascii: /m10.jpg">
2022-08-11 03:08:16 UTC	22	IN	Data Raw: 35 34 66 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 6e 61 68 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6d 67 22 3e 3c 69 6d 67 20 63 6c 61 73 73 3d 22 74 69 6d 65 73 22 20 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 64 36 63 34 63 31 30 38 61 37 65 65 39 39 32 33 66 38 32 65 32 33 30 36 62 63 62 39 63 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 74 69 6d 65 73 2d 62 6c 75 65 2e 73 76 67 22 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 6f 75 6e 74 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 75 72 6c 5f 5f 79 65 61 68 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6d 67 22 3e 3c 69 6d 67 20 63 6c 61 73 73 3d 22 74 69 6d 65 73 22 20 73 72 63 3d 22 2f 6c 73 74 61 74 69 63 2f 61 65 39 Data Ascii: 54f <img class="times" src="/lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times-blue.svg"> <img class="times" src="/lstatic/ae9
2022-08-11 03:08:16 UTC	23	IN	Data Raw: 62 32 36 0d 0a 3c 61 20 63 6c 61 73 73 3d 22 62 74 6e 20 62 74 6e 2d 62 6c 6f 63 6b 20 62 74 6e 2d 2d 70 72 69 6d 61 72 79 22 20 68 72 65 66 3d 22 2f 67 6f 2f 3f 61 3d 31 38 36 38 30 31 32 26 63 72 3d 35 37 37 34 38 26 6c 69 64 3d 31 39 39 35 33 26 6d 68 3d 54 57 70 56 5a 48 4e 73 64 6d 46 35 53 45 46 34 65 57 4a 6d 63 6d 39 42 61 47 64 4d 56 31 5a 36 63 45 56 58 65 45 35 34 59 58 52 52 55 6e 64 7a 52 55 38 74 4d 7a 55 34 4e 7a 55 25 33 44 26 6d 6d 69 64 3d 32 37 36 30 26 70 3d 30 26 72 66 3d 75 75 26 72 6e 3d 7a 63 34 5a 6f 64 47 55 79 73 34 57 6d 64 65 56 45 68 47 26 74 3d 6e 6f 74 72 61 63 6b 22 3e 69 20 61 67 72 65 65 3c 2f 61 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 73 74 65 Data Ascii: b26i agree ... /.ste
2022-08-11 03:08:16 UTC	25	IN	Data Raw: 63 2f 69 6d 61 67 65 73 2f 6d 31 30 2e 6a 70 67 22 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 62 67 2d 2d 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 33 2e 31 2e 6d 69 6e 2e 6a 73 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 32 35 36 2d 46 67 70 43 62 2f 4b 4a 51 6c 4c 4e 66 4f 75 39 31 74 61 33 32 6f 2f 4e 4d 5a 78 6c 74 77 52 6f 38 51 74 6d 6b 4d 52 64 41 75 38 3d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 2e 6a 73 64 65 6c 69 76 72 2e 6e 65 74 2f 6e 70 6d 2f 6c 61 7a 79 6c 6f 61 64 40 32 2e 30 2e 30 2d 72 Data Ascii: c/images/m10.jpg"> ... /.bg--><script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script><script src="https://cdn.jsdelivr.net/npm/lazyload@2.0.0-r

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:16 UTC	26	IN	Data Raw: 63 74 69 6f 6e 28 74 29 7b 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 69 28 6e 28 74 68 69 73 29 29 7d 29 7d 29 7d 28 6a 51 75 65 72 79 29 3b 66 75 6e 63 74 69 6f 6e 20 64 69 73 61 62 6c 65 43 6f 70 79 28 65 29 7b 72 65 74 75 72 6e 21 31 7d 66 75 6e 63 74 69 6f 6e 20 72 65 45 6e 61 62 6c 65 28 29 7b 72 65 74 75 72 6e 21 30 7d 24 28 66 75 6e 63 74 0d 0a Data Ascii: ction(t){t.preventDefault(),i(n(this))}}}}){jQuery);function disableCopy(e){return!1}function reEnable(){return!0}$(funct
2022-08-11 03:08:16 UTC	26	IN	Data Raw: 35 33 35 0d 0a 69 6f 6e 28 29 7b 24 28 74 68 69 73 29 2e 62 69 6e 64 28 22 63 6f 6e 74 65 78 74 6d 65 6e 75 22 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 7d 29 7d 29 2c 24 28 64 6f 63 75 6d 65 6e 74 29 2e 6b 65 79 64 6f 77 6e 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 31 32 33 21 3d 65 2e 6b 65 79 43 6f 64 65 26 26 28 28 21 65 2e 63 74 72 6c 4b 65 79 7c 7c 21 65 2e 73 68 69 66 74 4b 65 79 7c 7c 37 33 21 3d 65 2e 6b 65 79 43 6f 64 65 29 26 26 76 6f 69 64 20 30 29 7d 29 2c 64 6f 63 75 6d 65 6e 74 2e 6f 6e 73 65 6c 65 63 74 73 74 61 72 74 3d 6e 65 77 20 46 75 6e 63 74 69 6f 6e 28 22 72 65 74 75 72 6e 20 66 61 6c 73 65 22 29 2c 77 69 6e 64 6f 77 2e 73 69 64 65 62 61 72 26 26 28 64 6f 63 75 6d Data Ascii: 535ion(){$(this).bind("contextmenu",function(e){e.preventDefault()})}),$(document).keydown(function(e){return 123!=e.keyCode&&((!e.ctrlKey||!e.shiftKey||73!=e.keyCode)&&void 0)}),document.onselectstart=new Function("return false"),window.sidebar&&(docum
2022-08-11 03:08:16 UTC	28	IN	Data Raw: 31 64 38 0d 0a 2f 3f 61 3d 31 38 36 38 30 31 32 26 63 72 3d 35 37 37 34 38 26 6c 69 64 3d 31 39 39 35 33 26 6d 68 3d 54 57 70 56 5a 48 4e 73 64 6d 46 35 53 45 46 34 65 57 4a 6d 63 6d 39 42 61 47 64 4d 56 31 5a 36 63 45 56 58 65 45 35 34 59 58 52 52 55 6e 64 7a 52 55 38 74 4d 7a 55 34 4e 7a 55 25 33 44 26 6d 6d 69 64 3d 32 37 36 30 26 70 3d 30 26 72 66 3d 75 26 72 6e 3d 7a 63 34 5a 6f 64 47 55 79 73 34 57 6d 64 65 56 45 68 47 26 74 3d 6e 6f 74 72 61 63 6b 22 3b 0a 20 20 20 20 69 66 20 28 75 20 21 3d 3d 20 22 22 29 20 7b 0a 20 20 20 20 20 20 20 20 68 69 73 74 6f 72 79 2e 72 65 70 6c 61 63 65 53 74 61 74 65 28 6e 75 6c 6c 2c 20 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 2c 20 75 29 0a 20 20 20 20 7d 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 Data Ascii: 1d8/?a=1868012&cr=57748&lid=19953&mh=TWpVZHNsdmF5SEF4eWJmcm9BaGdMV1Z6cEVXeE54YXRRUndzRU8tMzU4NzU%3D&mmid=2760&p=0&rf=uu&rn=zc4ZodGUys4WmdeVEhG&t=notrack"; if (u !== "") { history.replaceState(null, document.title, u) }</script><script
2022-08-11 03:08:16 UTC	28	IN	Data Raw: 31 0d 0a 0a 0d 0a Data Ascii: 1
2022-08-11 03:08:16 UTC	28	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	50001	142.250.186.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:17 UTC	28	OUT	GET /s/montserrat/v25/JTUHjIg1_i6t8kCHKm4532VJOt5-QNFgpCtr6Hw5aXo.woff2 HTTP/1.1 Host: fonts.gstatic.com Connection: keep-alive sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" Origin: https://sweetiestouch2u.com sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://fonts.googleapis.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-11 03:08:17 UTC	29	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/apps-themes Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy: same-origin; report-to="apps-themes" Report-To: {"group":"apps-themes","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/apps-themes"}]} Timing-Allow-Origin: * Content-Length: 12708 X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Date: Thu, 04 Aug 2022 05:41:25 GMT Expires: Fri, 04 Aug 2023 05:41:25 GMT Cache-Control: public, max-age=31536000 Age: 595612 Last-Modified: Mon, 11 Jul 2022 18:55:59 GMT Content-Type: font/woff2 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:17 UTC	30	IN	Data Raw: 77 4f 46 32 00 01 00 00 00 00 31 a4 00 10 00 00 00 00 7b e8 00 00 31 44 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 76 1b d2 48 1c 86 34 06 60 3f 53 54 41 54 48 00 85 12 11 08 0a 81 81 48 e7 2b 0b 84 40 00 01 36 02 24 03 88 7c 04 20 05 84 7c 07 20 0c 07 1b 77 6b b3 11 51 d7 47 ef 56 14 25 8b f5 2b 47 45 29 1 1 7d 41 f6 7f 38 e0 86 0c b0 e1 eb 0d a0 f8 6e 13 46 42 3d ab 97 23 02 b6 35 aa 6a 11 dd fc 3d d7 c8 03 9b ef 67 38 93 9f 21 0e 01 c8 cc b8 01 e3 17 09 c7 31 74 51 85 f6 54 cb 64 0d 91 8e d0 d8 27 b9 a4 41 b4 66 55 f7 cc 2c 8b ec 3a 62 bb 9b 45 03 be 8b 84 2c 84 c5 7c 91 c0 91 e7 88 10 82 f8 06 22 7e 46 c4 89 98 40 94 7c b2 11 23 22 c6 19 c9 85 a8 2f 4f ff 3f f6 fc f6 cc 7d df 0d d3 fa 57 47 2d 9a 48 88 78 f3 8c 87 06 59 Data Ascii: wOF21{1DvH4`?STATHH+@6$| | wkQGV%+GE)}A8nFB=#5j=g8!1tQTd'AfU,:bE,|"~F@|#"/O?}WG-HxY
2022-08-11 03:08:17 UTC	30	IN	Data Raw: 63 6c 08 3e c8 7c 90 11 24 64 04 61 7e ff d7 a9 cd db ad 53 c6 6b 75 bd b7 97 5a d3 48 c1 49 48 69 72 81 60 45 b6 82 f4 05 08 a3 8f 40 1c 05 f0 df 80 00 1d 02 07 e7 06 b4 4a 8b e4 7a 13 c5 75 d2 02 57 a6 96 e9 f6 ad b6 08 f2 5e f7 c0 e1 0d 8e b2 38 3c df d9 20 39 23 e3 7d 10 f5 ce ce ee 60 30 58 62 41 9c 59 ec 92 fe 0d 41 3e 9f ee 9c 01 96 87 d7 62 0f ef 0c 29 e3 1d 48 be 39 23 83 bb 93 33 26 b3 3e c8 5e 91 b1 41 a6 20 fc 50 59 ac f0 23 a5 b1 a2 0f 63 05 91 fc ef ef 9b be de 99 d3 72 a9 65 c5 c8 ce 6b 47 4c ff df fd 03 36 9e 86 4d f4 00 ff 44 09 67 31 a5 01 e7 8b ad 7d bc a4 05 b7 ba 45 0c fc 5a 43 2d 91 59 4e 73 9c dd de ff af 1b 3b d4 99 d9 3d e0 b9 af 72 29 a5 88 04 09 e2 8a 48 90 20 41 9c c7 ef 1e 63 4b 8f f8 65 b0 7d ab 80 9e c0 0b 2a d6 2a 76 03 82 Data Ascii: cl>|$da~SkuZHIHir`E@JzuW^8< 9#}`0XbAYA>b)H9#3&>^A PY#crekGL6MDg1}EZC-YNs;=r)H AcKe}**v
2022-08-11 03:08:17 UTC	31	IN	Data Raw: 52 2f f2 19 fb 90 80 fe 1c 51 df f0 98 62 e7 23 95 0c ed 78 e1 77 0a 32 3f 6f c8 1d ce 1c f9 4a 9d 35 f9 23 dc 19 bc 76 d1 1e 53 2e 3b 2e 20 4e 73 18 75 2b 23 b6 1c 4d e5 a4 ab fd 94 9c 94 84 57 96 1a ec 35 cc ea e7 dd 29 52 58 16 0f 6b c3 94 50 85 8e cd 45 12 1e d4 dd 13 13 92 6a 0d b1 a3 ba a0 08 6a 61 17 ca ed 72 95 95 dd b6 c3 dd 29 29 32 71 00 ef 8a 4f 86 bb a9 b4 9d c9 a6 9c 21 72 d7 00 05 69 c4 a4 87 75 d6 14 5d 46 d2 84 77 76 54 5f b7 81 61 99 ed 56 ac 86 0f fb 44 b8 69 c9 06 67 70 f0 4e 24 30 f8 ab 7b 64 77 bf f1 1b 9a f1 5e 6e 03 c3 52 c2 da 59 61 c7 94 15 1c 9f e8 57 46 38 55 f9 3a 03 cd d7 48 82 31 67 c3 3c bd 3f 8c 34 75 57 69 99 9f c9 fb 4f 54 49 a3 a3 27 f9 74 5c 1b d0 36 34 3e da 1a 8a 66 53 b7 89 38 19 6f 2c 53 a1 af 34 a4 0d 44 56 af 0c Data Ascii: R/Qb#xw2?oJ5#vS.;. Nsu+#MW5)RXkPEjjar))2qO!riu]FwvT_aVDigpN$0{dw^nRYaWF8U:H1g<?4uWiOTI't \64>fS8o,S4DV
2022-08-11 03:08:17 UTC	32	IN	Data Raw: d5 8f 2d ed 42 96 7f 5b 2f 03 5b ec 96 78 42 55 be 55 28 2a 36 a5 2b 6b 61 7e d3 af 19 d6 63 e6 f6 20 0a de 19 0e d0 f9 87 5c 8a 57 f9 2f 36 69 ed 56 71 15 42 76 bd b5 3b fd bd 5e 0b 43 43 c1 bc 47 e1 5b 75 1f 6b 32 94 10 21 3c 82 2b 1d 54 5e c2 ab 57 a8 0c 47 5a bc a4 79 53 7f 6c 1b 7a b9 4d da 02 28 25 5b 6a b7 0c a3 f0 c5 2d b7 bf 63 d8 93 f1 15 20 44 a8 70 bd 64 30 c8 55 a0 dc 18 63 b5 db cf e4 ac 0b 2e e9 f4 17 33 2a 17 27 0f c0 31 f1 70 1c e7 24 ce 59 de fe e2 81 91 4b 21 8f 48 3e 09 8e 61 52 b9 54 37 b7 ef 50 0f b0 60 c0 91 4b 80 de e3 5b 89 03 64 41 23 80 ff a7 3b 52 be 78 85 80 7e 80 32 40 15 80 35 86 c1 58 06 7b 79 db cf 80 38 38 17 11 05 34 88 a6 11 88 5c 86 33 46 8e 92 14 eb 4d 8b 4a 9a 1d 72 39 24 9d 4b 89 22 fe b1 03 85 46 2a 30 da 58 23 8c Data Ascii: -B[/[xBUU(*6+ka~c \W/6iVqBv;^CCG[uk2!<+T^WGZySlzM(%[j-c Dpd0Uc.3*'1p$YK!H>aRT7P`K[dA#;Rx ~2@5X{y884\3FMJr9$K"F*0X#
2022-08-11 03:08:17 UTC	34	IN	Data Raw: 26 5c 84 13 0e 3a e9 b9 b3 11 42 27 4e bc 44 c9 32 64 ca 62 50 a0 50 3f ff 53 a4 d8 10 e5 2a 54 aa 56 c3 68 a8 46 4d 46 38 e6 9b e3 ba dd b6 c7 7d 9d 1e f8 d3 77 ef 23 c0 07 63 5c f1 cc 29 1f 23 c2 67 4f 6d b4 29 56 78 e1 9d 7d b1 c6 06 63 5d b5 cd 56 db b5 e3 50 0c 0b 2c 1e 3e 6b 52 22 62 12 4e ec 39 70 24 a0 e2 41 cd 8d 17 77 ff f2 a4 15 24 98 46 2f 3e aa 44 8b 14 25 46 1f 7a b1 12 a4 4b 91 2a 4d be 1c b9 f2 24 f9 d9 20 fd 0d 30 d8 40 5d 4a 34 a8 55 a7 de 30 65 86 f3 56 ca ec 87 4b 2e 3b e7 82 8b ce 23 c8 98 89 00 20 67 02 00 bd 04 20 27 01 f1 b7 00 fb bb 00 f6 73 60 9e 06 00 14 9d 97 3e 2c 0a 6a 65 7f 14 68 17 83 5c 99 06 44 78 c5 a6 19 1c 0b 31 34 db 27 11 ec c3 20 22 71 25 f4 46 32 7a 2b 3f 29 7d ca 24 98 3e 24 4a 2d 2b 46 b5 d4 cf ce c7 0b 8b 9a 6a Data Ascii: &\:B'ND2dbPP?S*TVhFMF8}w#c\)#gOm)Vx}c]VP,>kR"bN9pAwF/>D%FzK*M$ 0@]J4U0eVK.;# g 's`>,je h\Dx14' "q%F2z+?)}$>$J-+Fj
2022-08-11 03:08:17 UTC	35	IN	Data Raw: 38 a8 3b c7 d8 98 70 c0 cf 00 8d 92 13 d5 83 d5 be 5a 9b 6e 86 bb 7e 8a a9 5e ad 69 40 d9 a1 05 d2 aa 22 63 c6 2d cb 63 fd 85 45 06 3f 8a f9 b0 19 2c bd 85 86 b3 77 e3 a7 8a 4d cb fe 1f e4 65 f0 62 4e f9 92 e5 7f 3a 5e cc d5 28 a1 25 0b 8c d3 97 21 7a 88 25 38 b9 42 3a 6c d1 a4 3b 60 9b 93 71 48 3d 23 5f 5e dc 00 24 49 39 28 60 38 f1 b1 bf 82 20 59 2e a1 09 d9 5c 99 80 75 dc 72 36 21 a4 76 4f c9 a4 39 2f a0 21 39 98 3a 7d 4a 9d 20 93 7f b8 77 d8 22 0e 9c 21 36 36 c9 38 4f 3c a3 83 35 e9 be 61 78 99 ed 80 3f 04 d4 3e ea 96 e4 99 e8 db a9 14 d7 a0 d2 d4 8c 15 4d 3e fc ee 31 31 36 16 61 58 4b 6a 6a 14 00 95 a0 07 54 fa e5 a2 2b 92 a9 cf 9b 05 5c dd ed 61 cd 0f 2f cc 05 8e 32 ad 1b af 9c f8 fc 21 69 02 ce ca cc 41 bb 4c d6 3c 0b 4a e9 36 b5 fc e4 35 b9 97 3c Data Ascii: 8;pZn~^i@"c-cE?,wMebN:^(%!z%8B:l;`qH=#_^$I9(`8 Y.\ur6!vO9/!9:}J w"!668O<5ax?>M>116aXKjjT+\a/2!iAL<J65<
2022-08-11 03:08:17 UTC	36	IN	Data Raw: e8 2f f9 8e a8 23 9a 48 92 68 c9 4e 58 f2 2f 28 d3 da bd ba 7f 85 ea e1 c7 3e 1a 43 e1 27 17 9a 5d 3c 1d 7a 13 e5 7a ca 7e 89 5a 0a 8a 25 a7 50 ea 90 a4 ad 4d 30 77 d7 77 c3 ee 7f ff f9 ec dc ab d8 1b 96 7d f0 35 9c 67 86 3c fd 4c dc 18 c8 62 f6 97 a6 cb f9 1f 92 2e 09 7a 62 b6 8b 2f 21 b4 4a 75 b8 53 19 33 74 97 ee 5d 77 61 b0 b3 d4 e8 2b 6b 64 7f 0c b9 9c 3f 28 f1 39 ae 0a 09 ae 51 68 c2 5d 4a f0 65 cc 07 7d 18 f6 db 18 4c e5 9a 17 2d 5a 30 3b 75 d3 50 47 6f 43 5a ea 18 da 64 df ba 63 e1 22 44 84 0e 7b cb b6 89 58 db c8 e9 93 0a 24 dd c3 e9 ef b4 78 7e bc 2d fe 83 16 f7 f7 b6 25 7d 7d 20 f3 5e bd fc f5 0c 24 8a e5 ba 19 99 be 1f 69 c1 5f 21 de a9 2d 21 45 cb c3 3f 26 2b bf b7 c3 91 9d e1 fd 2f c5 9e f6 39 24 53 f1 19 9a c1 c2 5f fb 69 fd e8 cf f5 be 8a Data Ascii: /#HhNX/(>C']<zz~Z%PM0ww}5g<Lb.zb/!JuS3t]wa+kd?(9Qh]Je}L-Z0;uPGoCZdc"D{X$x~-%}} ^$i_!-!E? &+/9$S_i
2022-08-11 03:08:17 UTC	38	IN	Data Raw: ec 41 c9 d8 97 45 86 ad 1f 5c de fa 28 f3 ba 74 c2 fb 4a df f5 ef 77 ed ea c6 90 0e 0f 33 33 3b 5e fe 4f 11 8b 5b 5d e6 1a 78 bd 2b 91 47 e6 90 6f 94 b6 ff e8 9c fa da 9f f0 09 4c dd fe bc 4c 77 40 92 1c 66 f6 19 7a 83 53 55 bc 6e b2 dd b7 29 3f 7b aa 2e 62 bd 5f 05 0b 5f 92 29 6d 5a ab 3b 34 a6 d0 73 1a fe b4 02 87 6d 84 be 9b 7f 4f 52 76 d8 64 5e ee 64 f2 08 1b 6c 7c e4 18 8d fc 9b c7 bd 62 eb 66 b5 49 87 98 f3 1e ac e0 15 3d 7f 60 cb 5f b8 b8 59 e3 ae 10 d9 25 52 91 d5 5d 21 5f d9 56 a9 a4 44 6c 38 5f 85 1b 15 4a 1c 55 89 a4 02 7d 60 d0 d1 4b f5 3f c4 a5 a1 44 c2 7a 5b 2e 3f db 9c 36 4f 88 46 e5 d5 ef c7 20 95 f3 8d 0d da f6 67 32 82 cc 7d 0c 76 b0 af eb 35 a1 09 b3 62 49 65 25 21 75 a0 70 8a 20 be a8 c0 f6 e5 af 4f ea 9f 9b e0 a5 2d 9f df 37 f0 8a 3d Data Ascii: AE\(tJw33;^O[]x+GoLLw@fzSUn)?{.b__)mZ;4smORvd^dl|bfI=`_Y%R]!_VDl8_JU}`K?Dz[.?6OF g2}v5bIe%!up O-7=
2022-08-11 03:08:17 UTC	39	IN	Data Raw: 87 bc cf 21 90 9f e3 71 0e 82 7d 0f 0e e8 ee 7b 8a 0a 96 f1 92 39 fb 5b 06 e3 db d9 cc ef 41 f8 6c e1 cd 01 e6 b7 b3 df 3e 88 cc 51 c6 e4 92 5c 37 7f 2d 28 bd 22 f8 2f 4f f8 a5 d3 3d c6 77 74 c6 37 0c e6 0b 0c fa 5d b0 b0 b4 f7 cc 57 f3 04 af 3a df 63 de e9 ad 3b cc 6f 93 74 fe 70 81 a7 57 7c ce 6c 7c bc 70 56 0f 75 00 77 63 a9 8a 49 b6 86 85 aa 80 b5 81 af 75 ab 85 67 37 3d 59 34 c7 9d 7d 8f 8e 10 a6 33 df e9 7d 0f 04 ad c8 78 ab 48 39 ff f4 9e 8e 0d b3 d5 4e de c9 0d 5d 13 5b 95 d2 80 89 ae 53 3f a4 4e 39 19 ef d2 19 18 03 f4 77 c1 d8 5b b6 c6 be 63 30 df ab ff 7d 30 e7 84 9c 25 63 d2 65 2c 1a ad d0 44 67 9a 0a 41 d5 b0 b5 ee 3c d4 6e 5a ed 39 ba 2b 00 2c 9c db 9c d9 bf ee 0d 91 ec 9f 46 dc 07 16 06 ec 3a ba 88 3b bb ef b0 9a 47 5e 3c 18 9e d2 7c fa 20 17 Data Ascii: !q}{9[Al>Q\7-("/O=wt7]W:c;otpW|lpVuwcIug7=Y4}3}xH9N][S?N9w[c0}0%ce,DgA<nZ9+,F:;G^<|

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:17 UTC	40	IN	Data Raw: 2c bf 90 3e cc 16 9a b9 3c 8b 54 0a c4 08 21 7b d8 75 7e 45 ad 4c 33 fd aa 07 ea f7 a8 ef 17 e5 46 43 75 5f 34 96 ce fb f6 a6 05 ed 08 16 b4 91 8d ab c0 8e 21 aa 0b 22 e1 79 55 03 d8 e1 72 40 fc 3c c2 7c 16 11 81 e5 21 c0 60 7d cd 75 ce ad a2 59 be a4 ce bd 92 76 c9 de 4e 70 f9 37 3f bb 80 6f 15 8b f8 36 3b 5f 24 16 d4 94 68 35 bd e0 56 29 f5 4a 8f b2 57 dd aa 32 f7 ab 68 f5 4c 6a 06 88 61 0b 32 d6 5a b1 27 31 6a 62 a5 b9 d2 e4 08 b5 c0 ef 4d f9 3b 0a 0b 77 e4 17 ac c6 dc d5 4f 88 82 9d 9a c0 b7 89 36 4c a3 df a6 d1 6e d3 a7 5a c0 b3 f8 d0 60 d5 9a 41 f0 b4 98 93 55 69 04 68 2e 5e 32 68 3f c5 cc 8b 9a b4 3b 00 3e 39 c5 5f 9f 73 99 ff f0 37 ae c5 df 3c ac b5 1e fc fa aa 22 3c bf 28 5a 5c 14 41 5d 16 50 37 98 a9 78 ee aa c8 7e 55 91 30 7f 1a cf 9e 78 6e 4d Data Ascii: ,><T!{u~EL3FCu_4!"yUr@<|!`}uYvNp7?o6;_$h5V)JW2hLja2Z'1jbM;wO6LnZ`AUih.^2h?;>9_s7<"<(Z\A]P7x~U0xnM
2022-08-11 03:08:17 UTC	41	IN	Data Raw: f3 a3 48 cd eb a1 8d 16 e6 21 42 1b 0f f4 eb 70 17 0d 15 10 da 88 88 1b 3a 4c 17 90 ad 4a f2 84 53 f7 ea 8b 3f 9f a4 07 15 43 2d 05 c8 aa c3 af 1d 64 79 85 f9 31 cc 18 33 7c 5a 82 d4 0e 24 49 36 ca 56 3d b3 9f 1a 77 fa f9 42 d2 c4 b2 bd 20 ad 52 37 98 c7 bb 6a d8 35 dc a3 dd 54 5d 24 28 17 94 1d 11 27 30 17 62 21 1e 22 21 15 72 20 03 f4 f1 94 6c a7 32 f3 28 28 c1 19 d4 e0 63 7a ed 9e 5d 1e 2a a5 f9 9b d9 34 c9 2c 87 bc bb b8 d2 75 a1 10 36 27 34 d4 d5 cd 19 8f 8c 05 0d 87 e0 88 69 be 49 89 d7 74 bf b2 eb 4d ae a1 86 77 1b 86 29 d0 ac 96 66 22 50 11 f7 8e 47 64 dc 36 28 8c a8 ee 22 91 e0 fc 02 c3 8c 10 62 06 ad 76 07 a1 86 49 a4 fc bb 34 94 f7 8c 50 41 d8 df 2b c1 59 34 87 07 ac 82 df 00 58 69 71 e5 8c 50 c7 ef a8 55 0e 45 17 b2 73 03 71 e9 94 46 23 11 c0 Data Ascii: H!Bp:LJS?C-dy13|Z$I6V=wB R7j5T]$('0b!"!r l2((cz]*4,u6'4iItMw)f"PGd6("bvI4PA+Y4XiqPUEsqF#

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	63659	93.184.216.34	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:18 UTC	42	OUT	GET /media.ext HTTP/1.1 Host: example.org Connection: keep-alive sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" Accept-Encoding: identity;q=1, *;q=0 sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: video Referer: https://sweetiestouch2u.com/ Accept-Language: en-US,en;q=0.9 Range: bytes=0-
2022-08-11 03:08:18 UTC	42	IN	HTTP/1.1 404 Not Found Accept-Ranges: bytes Age: 221725 Cache-Control: max-age=604800 Content-Type: text/html; charset=UTF-8 Date: Thu, 11 Aug 2022 03:08:18 GMT Expires: Thu, 18 Aug 2022 03:08:18 GMT Last-Modified: Mon, 08 Aug 2022 13:32:53 GMT Server: ECS (bsa/EB1A) Vary: Accept-Encoding X-Cache: 404-HIT Content-Length: 1256 Connection: close
2022-08-11 03:08:18 UTC	43	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 45 78 61 6d 70 6c 65 20 44 6f 6d 61 69 6e 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 Data Ascii: <!doctype html><html><head> <title>Example Domain</title> <meta charset="utf-8" /> <meta http-equiv="Content-type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1" /> <style t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	56422	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:20 UTC	44	OUT	GET /lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart-red.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: sweetiestouch2u.com

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	48	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:21 GMT Content-Type: image/svg+xml Content-Length: 811 Connection: close Last-Modified: Tue, 10 May 2022 09:38:15 GMT ETag: "627a3287-32b" Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Cache-Control: max-age=1800 CF-Cache-Status: REVALIDATED Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EZO6L2dvl4clsgDd%2BQpjZDwgadHfYG luUE0wq2JfnLvn8SmlDKh%2Fa7uyNvuesgkG%2FQOdE6ggYrIXfX1OEI8GTcmT6J8YEYnu6qkX2BaPeZILJ0%2F1mq RT8Qfp%2F1UAw0u1zxiyNdKZ"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc4274ef29b83-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-08-11 03:08:21 UTC	49	IN	Data Raw: 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 37 39 32 22 20 77 69 64 74 68 3d 22 31 37 39 32 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 31 22 20 69 64 3d 22 73 76 67 32 37 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 3c 64 65 66 73 20 69 64 3d 22 64 65 66 73 33 31 22 3e 3c 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 20 69 64 3d 22 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 36 32 39 22 3e 3c 73 74 6f 70 20 6f 66 66 73 65 74 3d 22 30 22 20 69 64 3d 22 73 74 6f 70 36 32 35 22 20 73 74 6f 70 2d 63 6f 6c 6f 72 3d 22 72 65 64 22 20 73 74 6f 70 2d 6f 70 61 63 69 74 79 3d 22 31 22 Data Ascii: <svg height="1792" width="1792" version="1.1" id="svg27" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns="http://www.w3.org/2000/svg"><defs id="defs31"><linearGradient id="linearGradient629"><stop offset="0" id="stop625" stop-color="red" stop-opacity="1"
2022-08-11 03:08:21 UTC	49	IN	Data Raw: 20 73 74 6f 70 2d 6f 70 61 63 69 74 79 3d 22 31 22 2f 3e 3c 2f 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 3e 3c 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 20 78 6c 69 6e 6b 3a 68 72 65 66 3d 22 23 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 36 32 39 22 20 69 64 3d 22 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 36 33 31 22 20 78 31 3d 22 32 33 30 2e 31 33 37 22 20 79 31 3d 22 34 38 37 2e 38 39 22 20 78 32 3d 22 31 32 30 38 2e 39 38 36 22 20 79 32 3d 22 39 36 31 2e 39 37 33 22 20 67 72 61 64 69 65 6e 74 55 6e 69 74 73 3d 22 75 73 65 72 53 70 61 63 65 4f 6e 55 73 65 22 2f 3e 3c 2f 64 65 66 73 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 75 72 6c 28 23 6c 69 6e 65 61 72 47 72 61 64 69 65 6e 74 36 33 31 29 22 20 64 3d 22 4d 38 39 36 20 31 36 36 34 71 2d 32 36 20 30 2d 34 Data Ascii: stop-opacity="1"/></linearGradient><linearGradient xlink:href="#linearGradient629" id="linearGradient631" x1="230.137" y1="487.89" x2="1208.986" y2="961.973" gradientUnits="userSpaceOnUse"/></defs><path fill="url(#linearGradient631)" d="M896 1664q-26 0-4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	56421	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:20 UTC	44	OUT	GET /lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-heart.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: sweetiestouch2u.com
2022-08-11 03:08:21 UTC	45	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:21 GMT Content-Type: image/svg+xml Content-Length: 329 Connection: close Last-Modified: Tue, 10 May 2022 09:38:15 GMT ETag: "627a3287-149" Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Cache-Control: max-age=1800 CF-Cache-Status: HIT Age: 1119 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=kbEx4Ri4LWfxRU2QO15x8wycPlpatbP9 EqZdTS3sLqLEbO%2FFy5%2BTT7UxH3XZsT1HAIRO%2B9wJ0XlAvtZjVyIPSo2I3eX57nceaYlWoJA%2Fk%2BnCsb1D eX4OkgUHMePfYMADqP6aJKX%2F"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc4275aa49b3a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

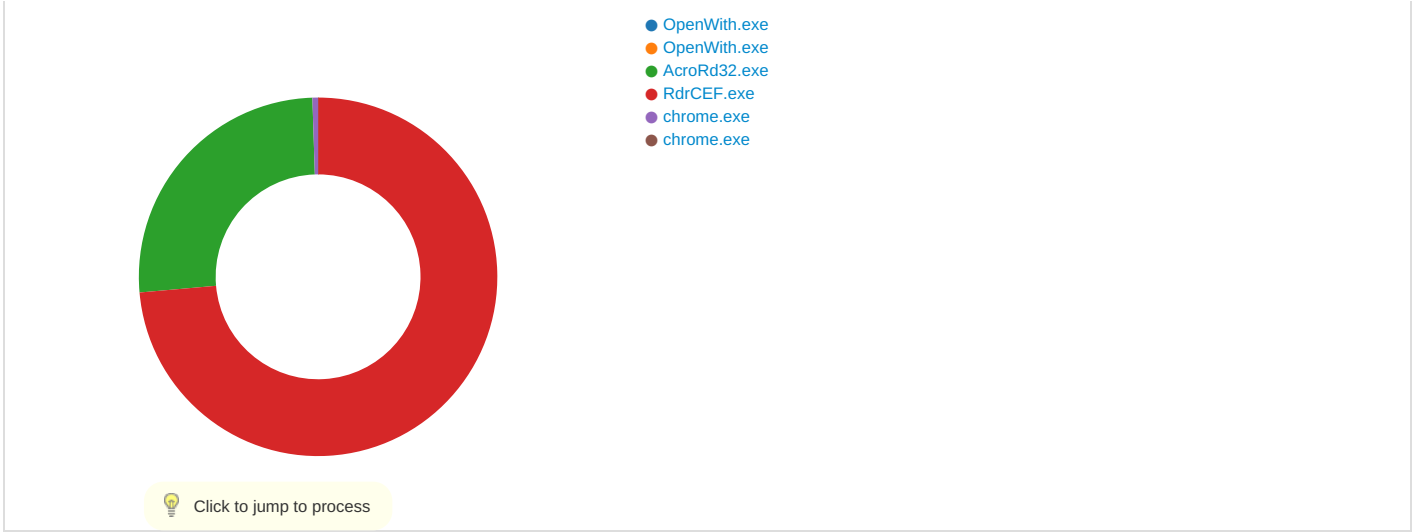
Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	46	IN	Data Raw: 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 37 39 32 22 20 77 69 64 74 68 3d 22 31 37 39 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 23 66 66 66 22 20 64 3d 22 4d 38 39 36 20 31 36 36 34 71 2d 32 36 20 30 2d 34 34 2d 31 38 6c 2d 36 32 34 2d 36 30 32 71 2d 31 30 2d 38 2d 32 37 2e 35 2d 32 36 54 31 34 35 20 39 35 32 2e 35 20 37 37 20 38 35 35 20 32 33 2e 35 20 37 33 34 20 30 20 35 39 36 71 30 2d 32 32 30 20 31 32 37 2d 33 34 34 74 33 35 31 2d 31 32 34 71 36 32 20 30 20 31 32 36 2e 35 20 32 31 2e 35 74 31 32 30 20 35 38 54 38 32 30 20 32 37 36 74 37 36 20 36 38 71 33 36 2d 33 36 20 37 36 2d 36 38 74 39 35 2e 35 2d 36 38 2e 35 20 31 32 30 2d 35 38 54 31 33 Data Ascii: <svg height="1792" width="1792" xmlns="http://www.w3.org/2000/svg"><path fill="#fff" d="M896 1664q-26 0-44-18l-624-602q-10-8-27.5-26T145 952.5 77 855 23.5 734 0 596q0-220 127-344t351-124q62 0 126.5 21.5t120 58T820 276t76 68q36-36 76-68t95.5-68.5 120-58T13
2022-08-11 03:08:21 UTC	46	IN	Data Raw: 2d 36 32 33 20 36 30 30 71 2d 31 38 20 31 38 2d 34 34 20 31 38 7a 22 2f 3e 3c 2f 73 76 67 3e Data Ascii: -623 600q-18 18-44 18z"/></svg>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	56423	188.114.97.3	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-11 03:08:21 UTC	46	OUT	GET /lstatic/ae9d6c4c108a7ee9923f82e2306bcb9c/images/icon-times-blue.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: sweetiestouch2u.com
2022-08-11 03:08:21 UTC	46	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:08:21 GMT Content-Type: image/svg+xml Content-Length: 425 Connection: close Last-Modified: Tue, 10 May 2022 09:38:15 GMT ETag: "627a3287-1a9" Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Cache-Control: max-age=1800 CF-Cache-Status: HIT Age: 1119 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=okhBrGvJ%2FXztXGXOYqzf2ypx27oOEcdWsYQh6qiRAkmQkrJG67%2BK4PrDNISy3%2BM8sPHkwk62GN2W5qLayr9Xi9PXJml2W%2FmTk4Hyo7EEpgc%2FLGNwcT5CUmF4pJMjkZFu%2BCVpX0cd"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738dc427fa645c20-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-08-11 03:08:21 UTC	47	IN	Data Raw: 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 37 39 32 22 20 77 69 64 74 68 3d 22 31 37 39 32 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 31 22 20 69 64 3d 22 73 76 67 31 35 37 35 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 23 34 63 66 66 63 33 22 20 64 3d 22 4d 31 34 39 30 20 31 33 32 32 71 30 20 34 30 2d 32 38 20 36 38 6c 2d 31 33 36 20 31 33 36 71 2d 32 38 20 32 38 2d 36 38 20 32 38 74 2d 36 38 2d 32 38 6c 2d 32 39 34 2d 32 39 34 2d 32 39 34 20 32 39 34 71 2d 32 38 20 32 38 2d 36 38 20 32 38 74 2d 36 38 2d 32 38 6c 2d 31 33 36 2d 31 33 36 71 2d 32 38 2d 32 38 2d 32 38 2d 32 38 2d 36 38 74 32 38 2d 36 38 6c 32 39 34 2d 32 39 34 2d 32 39 34 2d 32 39 34 71 2d 32 38 2d 32 Data Ascii: <svg height="1792" width="1792" version="1.1" id="svg1575" xmlns="http://www.w3.org/2000/svg"><path fill="#4cffc3" d="M1490 1322q0 40-28 68l-136 136q-28 28-68 28t-68-28l-294-294-294 294q-28 28-68 28t-68-28l-136-136q-28-28-28-68t28-68l294-294-294-294q-28-2
2022-08-11 03:08:21 UTC	47	IN	Data Raw: 20 32 39 34 20 32 39 34 2d 32 39 34 71 32 38 2d 32 38 20 36 38 2d 32 38 74 36 38 20 32 38 6c 31 33 36 20 31 33 36 71 32 38 20 32 38 20 32 38 20 36 38 74 2d 32 38 20 36 38 6c 2d 32 39 34 20 32 39 34 20 32 39 34 71 32 38 20 32 38 20 32 38 20 32 38 20 36 38 7a 22 20 69 64 3d 22 70 61 74 68 31 35 37 33 22 20 66 69 6c 6c 2d 6f 70 61 63 69 74 79 3d 22 31 22 2f 3e 3c 2f 73 76 67 3e Data Ascii: 294 294-294q28-28 68-28t68 28l136 136q28 28 28 68t-28 68l-294 294 294 294q28 28 28 68z" id="path1573" fill-opacity="1"/></svg>

Statistics

Behavior



System Behavior

Analysis Process: OpenWith.exe PID: 1264, Parent PID: 820

General

Target ID:	0
Start time:	05:06:52
Start date:	11/08/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff7f6dc0000
File size:	119840 bytes
MD5 hash:	5D37A62943F1071FFFFE1DE74B8F2778
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: OpenWith.exe PID: 2972, Parent PID: 820

General

Target ID:	4
Start time:	05:07:14
Start date:	11/08/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff7f6dc0000
File size:	119840 bytes
MD5 hash:	5D37A62943F1071FFFFE1DE74B8F2778
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: AcroRd32.exe PID: **2320**, Parent PID: **2972**

General

Target ID:	5
Start time:	05:07:20
Start date:	11/08/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\35
Imagebase:	0xa60000
File size:	3141816 bytes
MD5 hash:	0EAC436587F5A1BEF8AEB2E2381D2405
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A8D5DF	CreateDirectoryExW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1552	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	AD8435	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock2320.1.1965920984.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	B08F44	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9rscy23_i5v9my_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B56078	HttpSendRequestA
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A916fp71_i5v9mz_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9zvk0cb_i5v9n0_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91ke9q8k_i5v9n1_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9q4yww8_i5v9n2_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9gb73b1_i5v9n3_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91wwumfp_i5v9n4_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91ktscin_i5v9n5_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9du022m_i5v9n6_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9ac2g24_i5v9n7_174.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_READER_LAUNCH_CARD	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Retention	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Banner	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\Edit_InApp_Aug2020	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	ACA265	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1552	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst	success or wait	1	B14127	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\ToolsSearch	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	A6DDA3	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	A6DDA3	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	A6DDA3	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	ACB32D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	ACB32D	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/alfredo/Desktop/35	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	35	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	ADB8C9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 61 6C 66 72 65 64 6F 2F 44 65 73 6B 74 6F 70 2F 33 35 00	success or wait	1	ADB8C9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 32 30 38 31 31 30 35 30 37 33 30 2D 30 37 27 30 30 27 00	success or wait	1	ADB8C9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	48294	success or wait	1	ADB8E9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	ADB8E9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	ADB8A7	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	ADB8C9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	ADB8C9	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 32 31 30 36 30 38 30 38 31 33 35 33 2D 30 37 27 30 30 27 00	success or wait	1	ADB8C9	RegSetValueExW

Analysis Process: RdrCEF.exe PID: **5268**, Parent PID: **2320**

General

Target ID:	8
Start time:	05:07:26
Start date:	11/08/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043

Imagebase:	0xa80000
File size:	7227576 bytes
MD5 hash:	4AC861CBCAFA331A72C04BF35AE792E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	25	B99718	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	75	B99775	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	166	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	5	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	12	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1631	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\microsoftGraph\microsoft-graph-js-sdk-web.js	unknown	4096	success or wait	27	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\microsoftGraph\microsoft-graph-js-sdk-web.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	8	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	B85D50	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	6	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	18	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	18	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	41	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	45	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	43	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	B85D50	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\css\main-selector.css	unknown	4096	success or wait	32	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	4	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\css\main.css	unknown	4096	success or wait	15	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\css\main.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\js\selector.js	unknown	4096	success or wait	28	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	51	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	7	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	10	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	24	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	B85D50	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	15	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\js\plugin.js	unknown	4096	success or wait	372	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\unified-share\js\plugin.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	180	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	219	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	245	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	16	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	B85D50	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	152	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	101	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\css\main-selector.css	unknown	4096	success or wait	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\css\main-selector.css	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\css\main.css	unknown	4096	success or wait	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\css\main.css	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\js\selector.js	unknown	4096	success or wait	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\js\selector.js	unknown	4096	end of file	1	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\js\plugin.js	unknown	4096	success or wait	13	B85D50	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\task-handler\js\plugin.js	unknown	4096	end of file	1	B85D50	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	B99718	ReadFile

Analysis Process: chrome.exe PID: **3932**, Parent PID: **2320**

General

Target ID:	9
Start time:	05:08:07
Start date:	11/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://www.google.com/url?q=%68%74%74%70%73%3A%2F%2F%74%6F%2D%63%6C%69%63%6B%2E%66%75%6E%2F%65%72%69%58%46%76%4B%56%48%63%36%23%79%65%78%6F%72%79%76%6A%78%6A&sa=D&sntz=1&usg=AOvVaw2t3jeNlZEFZI-xvhukbEyl
Imagebase:	0x7ff68c970000
File size:	2438312 bytes
MD5 hash:	74859601FB4BEEA84B40D874CCB56CAB
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF68C9A885B	RegSetValueExW

Analysis Process: chrome.exe PID: **6336**, Parent PID: **3932**

General

Target ID:	12
Start time:	05:08:09
Start date:	11/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1752,12796533771390455494,5363625801302401924,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2156 /prefetch:8
Imagebase:	0x7ff68c970000
File size:	2438312 bytes
MD5 hash:	74859601FB4BEEA84B40D874CCB56CAB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly