ID: 533080
Sample Name: It.servicedesk-VoiceFax-723-2121-723.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 01:02:43
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

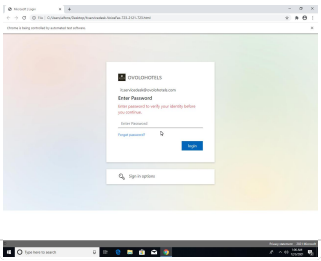
Windows Analysis Report It.servicedesk-VoiceFax-723-2…

Overview

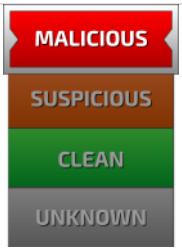
General Information

Sample Name:	It.servicedesk-VoiceFax-723-2121-723.html
Analysis ID:	533080
MD5:	53621f89e509831.
SHA1:	218d9d6fc72c73d..
SHA256:	a76c9007fd100fe..
Infos:	

Most interesting Screenshot:



Detection



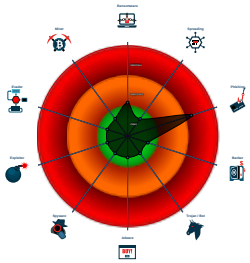
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Yara signature match
- IP address seen in connection with o…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5808 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\It.servicedesk-VoiceFax-723-2121-723.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4904 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,2614049055858890495,17816619576725297410,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1552 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
It.servicedesk-VoiceFax-723-2121-723.html	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x4683b:$c8: while(!![]) • 0x46859:$d1: parseInt(_0x9feab1(0xf0))/0x1*(-parseInt(_0x9feab1(0xc8))/0x2)+parseInt(_0x9feab1(0x10c))/0x3*(parseInt(_0x9feab1(0xee))/0x4)+parseInt(_0x9feab1(0xf2))/0x5*(-parseInt(_0x9feab1(0x103))/0x6)+ • 0x46879:$d1: parseInt(_0x9feab1(0xc8))/0x2)+parseInt(_0x9feab1(0x10c))/0x3*(parseInt(_0x9feab1(0xee))/0x4)+parseInt(_0x9feab1(0xf2))/0x5*(-parseInt(_0x9feab1(0x103))/0x6)+parseInt(_0x9feab1(0x11f))/0x7+- • 0x46898:$d1: parseInt(_0x9feab1(0x10c))/0x3*(parseInt(_0x9feab1(0xee))/0x4)+parseInt(_0x9feab1(0xf2))/0x5*(-parseInt(_0x9feab1(0x103))/0x6)+parseInt(_0x9feab1(0x11f))/0x7+-parseInt(_0x9feab1(0x118))/0x8+- • 0x468b8:$d1: parseInt(_0x9feab1(0xee))/0x4)+parseInt(_0x9feab1(0xf2))/0x5*(-parseInt(_0x9feab1(0x103))/0x6)+parseInt(_0x9feab1(0x11f))/0x7+-parseInt(_0x9feab1(0x118))/0x8+-parseInt(_0x9feab1(0x10b))/0x9*(• 0x468d7:$d1: parseInt(_0x9feab1(0xf2))/0x5*(-parseInt(_0x9feab1(0x103))/0x6)+parseInt(_0x9feab1(0x11f))/0x7+-parseInt(_0x9feab1(0x118))/0x8+-parseInt(_0x9feab1(0x10b))/0x9*(parseInt(_0x9feab1(0xd1))/0xa)+- • 0x468f7:$d1: parseInt(_0x9feab1(0x103))/0x6)+parseInt(_0x9feab1(0x11f))/0x7+-parseInt(_0x9feab1(0x118))/0x8+-parseInt(_0x9feab1(0x10b))/0x9*(parseInt(_0x9feab1(0xd1))/0xa)+-parseInt(_0x9feab1(0x119))/0xb*(-
It.servicedesk-VoiceFax-723-2121-723.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

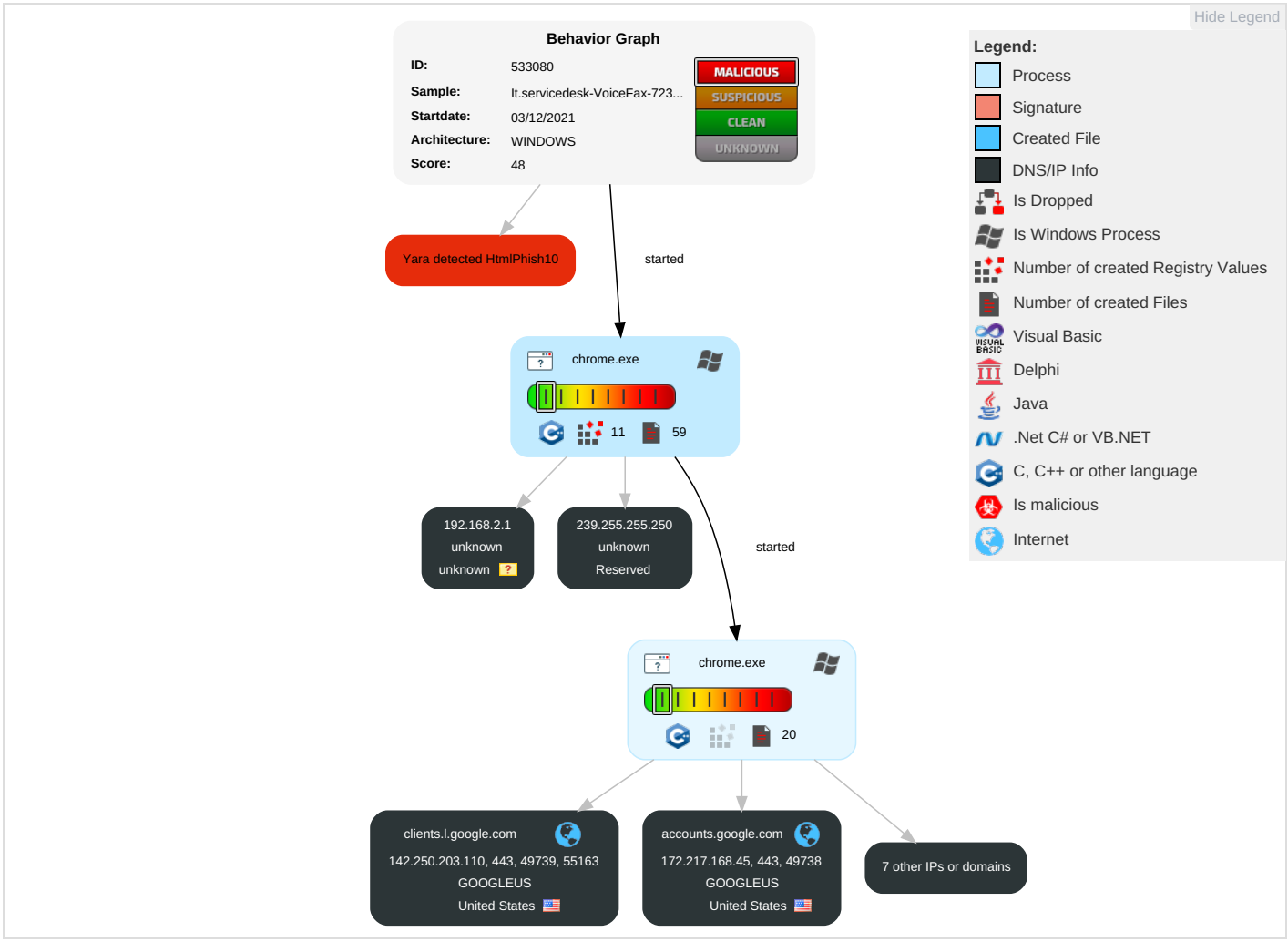
Phishing:

Yara detected HtmlPhish10

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic 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	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

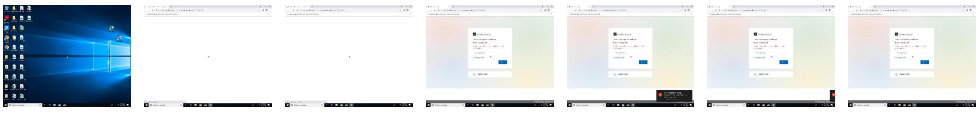
Behavior Graph

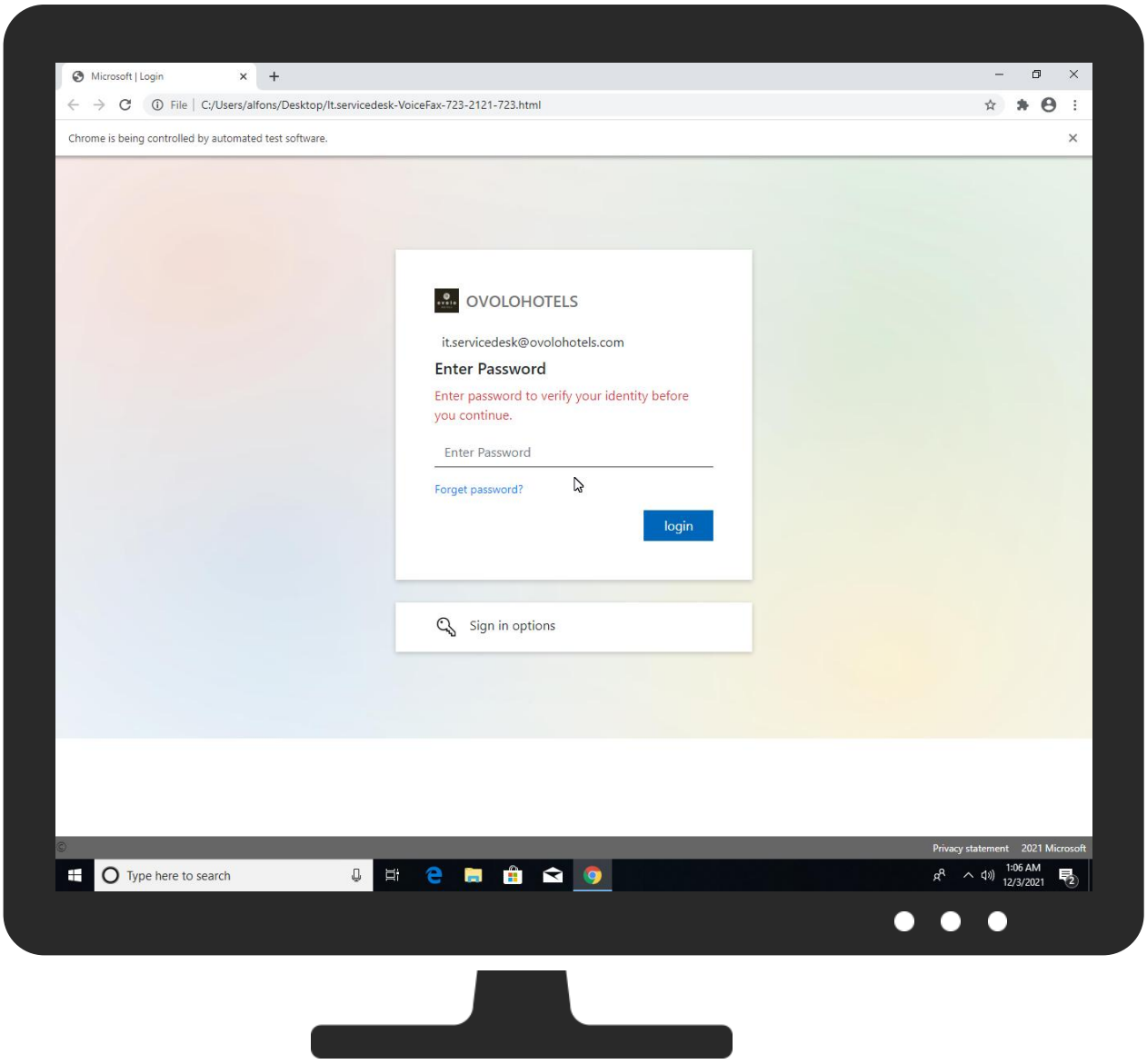


Screenshots

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
aadcdn.msauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/hosted-libraries-pushers	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.icoz-u	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/hosted-libraries-pushersCross-Origin-Resource-Policy:	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/hosted-libraries-pushers	0%	URL Reputation	safe	
http://https://dietcare.us/next.php	0%	Virustotal		Browse
http://https://dietcare.us/next.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.224.189.9	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	false		high
http://https://logo.clearbit.com/ovolohotels.com	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.224.189.9	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533080
Start date:	03.12.2021
Start time:	01:02:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	It.servicedesk-VoiceFax-723-2121-723.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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:	MAL
Classification:	mal48.phis.winHTML@11/83@7/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.18.10.207	PaymentReceipt.html	Get hash	malicious	Browse	
	_0.html	Get hash	malicious	Browse	
	wXvjhk5m3v.html	Get hash	malicious	Browse	
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	
	VM845.html	Get hash	malicious	Browse	
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	
	ATT14851.html	Get hash	malicious	Browse	
	DHL Receipt.html	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT29220.html	Get hash	malicious	Browse	
	Updated Proposal and Statements.docx	Get hash	malicious	Browse	
	ATT17593.html	Get hash	malicious	Browse	
	ATT91376.html	Get hash	malicious	Browse	
	Statement.html	Get hash	malicious	Browse	
	50837%%fax838393839379he8883838298272738383.htm	Get hash	malicious	Browse	
	WMHighfield.html	Get hash	malicious	Browse	
	Employee payment plan.HTM	Get hash	malicious	Browse	
	V-M RTAmpcapital5EG1-TGQO2F-IOC8.htm	Get hash	malicious	Browse	
239.255.255.250	PaymentReceipt.html	Get hash	malicious	Browse	
	ATT01313.html	Get hash	malicious	Browse	
	IM-87678A-1A1.msi	Get hash	malicious	Browse	
	IM-87678A-1A1.msi	Get hash	malicious	Browse	
	PaymentReceiptPDF.html	Get hash	malicious	Browse	
	fel.com.html	Get hash	malicious	Browse	
	_0.html	Get hash	malicious	Browse	
	wXvjhk5m3v.html	Get hash	malicious	Browse	
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	
	leco.com-FAX-59087-pdf.htm	Get hash	malicious	Browse	
	EmployeeAssessment.html	Get hash	malicious	Browse	
	(MT-103-USD)___717.htm	Get hash	malicious	Browse	
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	LockBit_Ransomware.hta	Get hash	malicious	Browse	
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	
	'Vm Note'jessica.mancel On Wed, 01 Dec 2021 210259 +0100.html	Get hash	malicious	Browse	
	'Vm Note'usename On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	PaymentReceipt.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT01313.html	Get hash	malicious	Browse	• 104.16.18.94
	PaymentReceiptPDF.html	Get hash	malicious	Browse	• 104.16.19.94
	_0.html	Get hash	malicious	Browse	• 104.16.19.94
	wXvjhk5m3v.html	Get hash	malicious	Browse	• 104.16.18.94
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	• 104.16.19.94
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	• 104.16.18.94
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 104.16.18.94
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 104.16.18.94
	'Vm Note'usename On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	• 104.16.19.94
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	• 104.16.19.94
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ATT01159.html	Get hash	malicious	Browse	• 104.16.18.94
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT14851.html	Get hash	malicious	Browse	• 104.16.19.94
	WMHighfield.html	Get hash	malicious	Browse	• 104.16.18.94
	Gracehealthmi.org7X9YCEB6AI.htm	Get hash	malicious	Browse	• 104.16.18.94
	DHL Receipt.html	Get hash	malicious	Browse	• 104.16.19.94
	phish.htm	Get hash	malicious	Browse	• 104.16.19.94
	html.html	Get hash	malicious	Browse	• 104.16.18.94
d26p066pn2w0s0.cloudfront.net	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	• 52.84.148.85
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	• 13.32.22.81
	'Vm Note'usename On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	• 13.224.96.22
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	• 13.224.96.11
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	• 13.224.96.22
	AtlanticareINV25-67431254.htm	Get hash	malicious	Browse	• 13.224.96.22
	ATT17593.html	Get hash	malicious	Browse	• 13.224.96.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT91376.html	Get hash	malicious	Browse	• 13.224.96.127
	FORMAP781419 - AP RemittanceAdvice.htm	Get hash	malicious	Browse	• 13.32.99.33
	REF ID 398046279094.html	Get hash	malicious	Browse	• 13.32.19.54
	ATT00001.html	Get hash	malicious	Browse	• 13.224.96.39
	suspicious.htm	Get hash	malicious	Browse	• 13.224.96.22
	RemittanceAdvice-9793573.htm	Get hash	malicious	Browse	• 13.224.96.22
	9337297373923u33678391.htm	Get hash	malicious	Browse	• 143.204.98.37
	eFax-72766.htm	Get hash	malicious	Browse	• 143.204.98.37
	RemittanceAdvice-14532878.htm	Get hash	malicious	Browse	• 13.224.96.11
	Devoncs-Attachment 2021-11-09 File - 5849057.html	Get hash	malicious	Browse	• 13.32.219.88
	sda-361693.htm	Get hash	malicious	Browse	• 52.222.149.82
	.html	Get hash	malicious	Browse	• 143.204.98.24
	2-0121-40Z Invoice.html	Get hash	malicious	Browse	• 13.224.193.89

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 104.26.6.139
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 104.26.7.139
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 104.26.6.139
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 104.26.7.139
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 104.26.7.139
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 172.67.70.134
	S2pmCqOFEf.exe	Get hash	malicious	Browse	• 162.159.130.233
	trynagetmybinsufucker98575.arm7	Get hash	malicious	Browse	• 172.67.247.213
	arm7	Get hash	malicious	Browse	• 162.159.132.56
	GenoSec.x86	Get hash	malicious	Browse	• 104.31.160.230
	NitroRansomware.exe	Get hash	malicious	Browse	• 162.159.135.232
	HackLoader.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.15350.rtf	Get hash	malicious	Browse	• 162.159.135.233
	PaymentReceipt.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT01313.html	Get hash	malicious	Browse	• 104.16.18.94
	1D4l9eR0W4.exe	Get hash	malicious	Browse	• 23.227.38.74
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 104.26.6.139
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 104.26.6.139
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 172.67.70.134
	QEuPmJ4lVYW4nj1.exe	Get hash	malicious	Browse	• 104.21.19.200
AMAZON-02US	beamer.x86-20211202-2350	Get hash	malicious	Browse	• 34.249.145.219
	beamer.arm-20211202-2350	Get hash	malicious	Browse	• 34.249.145.219
	a-r.m-4.Sakura	Get hash	malicious	Browse	• 54.171.230.55
	GenoSec.arm7	Get hash	malicious	Browse	• 176.34.166.240
	S2pmCqOFEf.exe	Get hash	malicious	Browse	• 52.216.166.67
	12.dll	Get hash	malicious	Browse	• 13.225.75.74
	NVTNgwAjOK	Get hash	malicious	Browse	• 54.102.91.74
	lAe63MagsK	Get hash	malicious	Browse	• 13.233.103.244
	GenoSec.x86	Get hash	malicious	Browse	• 198.251.137.253
	HackLoader.exe	Get hash	malicious	Browse	• 52.217.109.12
	mirai.x86	Get hash	malicious	Browse	• 44.224.113.150
	Yoshi.x86-20211202-2050	Get hash	malicious	Browse	• 13.52.72.80
	7009.xlsx	Get hash	malicious	Browse	• 13.250.31.113
	invoice dhl.delivery document and original invoice sign.exe	Get hash	malicious	Browse	• 44.227.76.166
	oeOZvHnuaU	Get hash	malicious	Browse	• 54.171.230.55
	Milleniumbpc.xlsx	Get hash	malicious	Browse	• 44.231.165.140
	PQPv91RexG	Get hash	malicious	Browse	• 34.249.145.219
	WAYBILL 44 7611 9546 - Joao Carlos.exe	Get hash	malicious	Browse	• 75.2.115.196
	HBL No_PZU100035300.xlsx	Get hash	malicious	Browse	• 3.64.163.50
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 3.108.154.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0ee07748-c0f6-46d6-bff5-6d23e1019095.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	390414
Entropy (8bit):	6.021396811511392
Encrypted:	false
SSDEEP:	6144:95xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:/kxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	082AE0CE62E93A47426749924CB95D81
SHA1:	A5EAC43BA202F1197114BB263095D1BF9560F031
SHA-256:	F56223625A2140037A45CDE8F1A177CFE08BA8D170FF8B32882863EA16C94BDC
SHA-512:	478D66DAF9791A217F542715D115C2635B271A50F2A5BD44212C48CE6D65B30C0E5A41B7B04EE2D4F0DF547615CEC177B5B6586E4504A8AE5C3799EB3B5A61B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075673178"},"plugins":{"resource_cache_update":"1638522285.338

C:\Users\user\AppData\Local\Google\Chrome\User Data\3249fd06-1910-4c4e-a2a8-caac25dcf80f.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):	388256
Entropy (8bit):	6.014556486745422
Encrypted:	false
SSDEEP:	6144:p5xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:jkxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	D44CF65B90315911CDEB0536FA72EA07
SHA1:	1233E0BD5997DB1D9510924D5C77DF129B0C4E05
SHA-256:	232C2A7F86E54E7379322AFC70419992E137D0AF3FA012355D759557F421A582

C:\Users\user\AppData\Local\Google\Chrome\User Data\3249fd06-1910-4c4e-a2a8-caac25dcf80f.tmp	
SHA-512:	249020C69D91B34B304C5E203831C448E11CF955F4729ABE94534CC08F61BC01B4FDF591718D50BFC9CF048297958273FB674A21F3AECCC5E9650F16D10747C7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13282995824436

C:\Users\user\AppData\Local\Google\Chrome\User Data\9bab0ff2-ae34-4746-b196-6e123d8016eb.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):	388256
Entropy (8bit):	6.014556387062204
Encrypted:	false
SSDEEP:	6144:l5xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:3kxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	900E887068A5EE636B7A76DB8EADC03D
SHA1:	79AB3F5C61E130EBAD3A781694C6F9B4DFF18A71
SHA-256:	33E5B34D7BB16B16707405C9B93C3B5797BFCEAB83AD8140A152642B755ADBDF
SHA-512:	93314373A19076B52D1A55560CBAE0A4A41140B6A6A2DB741BD3CA1840D57A3B2AAD16C6EF2BF55DCC11A55FB62D370925AB40C2129E1826859133EE6AC43E[7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075673178"},"policy":{"last_statistics_update":"13282995824436

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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9n:+Y66cR9
MD5:	7A9D405E9218ED86C7ED3BB729DAA896
SHA1:	E5BB69E833231B755B20E5A0C9B2392D8B923C66
SHA-256:	D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF
SHA-512:	F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1bbe55f4-1c2e-44d1-bbb4-4c4cb50a1048.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):	16608
Entropy (8bit):	5.579891333832027
Encrypted:	false
SSDEEP:	384:sZltfLlPMX11kXqKf/pUZNCgVLH2HfDkrUEAxAfyT4r:wLlm11kXqKf/pUZNCgVLH2HfgrUXxxTE
MD5:	3C85B38781F7C7D5980C3962280926BE
SHA1:	FC4FCFA8D7A370C92B5CF15A64B1CCAAE646B06F
SHA-256:	09033A4B809B5FC49EE39E33A6F9FFB47D018A80E6F8369767D9A1C669AC4BDC
SHA-512:	9F3D8BE4609559706A37AD5DD19F051EF770031AA99855211AB40BBB53F17CFC335CB6B79328116F39C097697D3259C881064BF4A8FB4D42091390E6F6453577
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1bbe55f4-1c2e-44d1-bbb4-4c4cb50a1048.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282995824689010","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c0d7484-4833-445a-809b-24a95c95cc49.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):	16607
Entropy (8bit):	5.5798491604600065
Encrypted:	false
SSDEEP:	384:sZltIlIPMX11kXqKf/pUZNCgVLH2HfDkrUEDuAfyT4X:tLlm11kXqKf/pUZNCgVLH2HfgrUauxTo
MD5:	878B52FB9F94C77F610112E53C37EC8F
SHA1:	5859058A56C5C2E03F0C5B04E315A2D9CEA0AADF
SHA-256:	4A0D503C7874482B123689F0C101DF0D9BE265147C3B68039CCAC2BD1485BDE7
SHA-512:	249B9A05E7920BD1FCFDC3744EC2F3E9D57CDF48A9995A1196F51AEF53CA62FF668507993AD73893B5C625CE0828BDB57A76A855077E762AD0A1F39AE632EFAD
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282995824689010","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\96705f55-d8b9-43dd-9a82-439aa8f978d6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1994
Entropy (8bit):	4.894512343567444
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zsGRsRZGsARLsvfArqXsqMHTYhbxD:JnxOTCXDH+zMnMK1rcG0hVD
MD5:	0F3CEAAE52AB02419C7EF6FF4EB85DF4
SHA1:	7EF7B7C38BF4347B25A02F231A38D73F8C0D5C54
SHA-256:	84586F25A3AADC7E9185691C99D8D460263E98C7794762551C586FA5251BC491
SHA-512:	1A6543ACEAB3D77982FA7F57D9C49F1EC5788157C8EE07630FAA5A2E8E73481859D7CFF5155CF6150546EFD7051C86F2F46DD5BF1713525A5F87664ED826F105
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285587827524442","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com"},{"alternative_service":[{"advert

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9fd10ed0-2cc3-437d-b195-bc8e1de11c4e.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):	4786
Entropy (8bit):	4.935943314151862
Encrypted:	false
SSDEEP:	48:YckpklSiklqicyqAPqqTlYclQKHoTw0pB1aPc8C1Nfct/9BhUJo3KhmeSnpNGz0p:n1rRrY9pSKlGIk0JCKL8xpbOTQVuwn
MD5:	A375C872766372415FAAAD364EF6B7C3
SHA1:	67F7B1C3E5AD90E8837A4111EC40EA67BDA4FA2D
SHA-256:	473A0DE1B02F4525894769BF53BF8263D55206183C62DF04C564D2FF342965AE
SHA-512:	F84F625CB4C6EB3ECD96E8B7CAB48B51875886607FA638EAC4A9CE79669C9925AF71E3BB96B49498FE8588F384281E65979A0B7F736BDD30A545392D28C81085
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9fd10ed0-2cc3-437d-b195-bc8e1de11c4e.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282995825308949","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.145584815839771
Encrypted:	false
SSDEEP:	6:mVYQF34q2P923iKKdK9RXXTZIFUtsYf3JZmweYf3DkwO923iKKdK9RXX5LJ:JQOv45Kk7XT2FUtvfZ/Rfz5L5Kk7XVJ
MD5:	7219484440261C3E69A4A1C3D56CDADF
SHA1:	09372AFF4CF3EAAF474ABD4A13065E053F900080
SHA-256:	F76BD4A27E2419436B7703175C247AD14FAE04F6BCA4C4674EAF27A354F68427
SHA-512:	373726DEEC8BB7A40B2546ECA1BA33F33476EFE18AAF26DB04B4B8E911A297D171322FF658A3E2C1E71856F05976EE1959E0D79131BEEEF84934C5C727288F1
Malicious:	false
Preview:	2021/12/03-01:03:52.392 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/12/03-01:03:52.395 1980 Recovering log #3.2021/12/03-01:03:52.395 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.145584815839771
Encrypted:	false
SSDEEP:	6:mVYQF34q2P923iKKdK9RXXTZIFUtsYf3JZmweYf3DkwO923iKKdK9RXX5LJ:JQOv45Kk7XT2FUtvfZ/Rfz5L5Kk7XVJ
MD5:	7219484440261C3E69A4A1C3D56CDADF
SHA1:	09372AFF4CF3EAAF474ABD4A13065E053F900080
SHA-256:	F76BD4A27E2419436B7703175C247AD14FAE04F6BCA4C4674EAF27A354F68427
SHA-512:	373726DEEC8BB7A40B2546ECA1BA33F33476EFE18AAF26DB04B4B8E911A297D171322FF658A3E2C1E71856F05976EE1959E0D79131BEEEF84934C5C727288F1
Malicious:	false
Preview:	2021/12/03-01:03:52.392 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/12/03-01:03:52.395 1980 Recovering log #3.2021/12/03-01:03:52.395 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.166545902252381
Encrypted:	false
SSDEEP:	6:mVYf834q2P923iKKdKyDZIFUtsY0cdvJZmweYSv3DkwO923iKKdKyJLJ:J0Iv45Kk02FUtv0cdh/RSvz5L5KkWJ
MD5:	3E452B04F6E987C8E3B56AB58399B3E3
SHA1:	02DAFBF89D7E9BB51BEF7FADD8B91B44D038F543
SHA-256:	716C6849E7C9D61A1E6E8A8D4B6592E8878CF31B069F37626E006AF3595B406A
SHA-512:	9D185C101BACC84D44EBAD2DA7DEEB34DEE3AAF1084553D3BAE79115F421F2834DF3E9794112386488865AEC5F4058C1C2A05AB5AF4781D4E15B57668754B3 7
Malicious:	false
Preview:	2021/12/03-01:03:52.385 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/12/03-01:03:52.386 1980 Recovering log #3.2021/12/03-01:03:52.387 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.166545902252381

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Encrypted:	false
SSDEEP:	6:mVYf834q2P923iKKdKyDZIFUtsY0cdvJZmweYSv3DkwO923iKKdKyJLJ:J0Iv45Kk02FUtv0cdh/RSvz5L5KkWJ
MD5:	3E452B04F6E987C8E3B56AB58399B3E3
SHA1:	02DAFBF89D7E9BB51BEF7FADD8B91B44D038F543
SHA-256:	716C6849E7C9D61A1E6E8A8D4B6592E8878CF31B069F37626E006AF3595B406A
SHA-512:	9D185C101BACC84D44EBAD2DA7DEEB34DEE3AAF1084553D3BAE79115F421F2834DF3E9794112386488865AEC5F4058C1C2A05AB5AF4781D4E15B57668754B36 7
Malicious:	false
Preview:	2021/12/03-01:03:52.385 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/12/03-01 :03:52.386 1980 Recovering log #3.2021/12/03-01:03:52.387 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.08256882712514144
Encrypted:	false
SSDEEP:	6:/FMe5b8kN6H+SfUb1gYMTxV0gC1CS51z3k/uutwH0KOcGVSHKRK+ikfFdJf+qiJW:dMYNFS8b6nspTz0uNqWHKRKlgviJW
MD5:	480785FBBE4EA0C38266D8250EFCF99B
SHA1:	1E65EABA7139F419B7B3E432E3B0FD562F043B9A
SHA-256:	4A1BF70E1C7FDB1D1431E939F9752D824A11256CA0BC56843FC3FC72F5BEC7B0
SHA-512:	13709B09F964627E947F92D4BF7178F0A0AAC45151E99CBE12850DEA9A273666FBACB683EC8CC195D68DC0A93BB69BEC662F85A1442477ED77048D1F36B9C84
Malicious:	false
Preview:	.....$..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.05858006261022855
Encrypted:	false
SSDEEP:	24:XzGwVcb8dCUUoxibZJqq9eBk+uCOYM7GmxRHOUS3df18ZFUP/MyeRVQtStj:JVFCgiDqq9eK+uMbmXHOUkdUFnVe
MD5:	63ED761B5DD01656F58A59DE49590B91
SHA1:	A96FEF297E3444F53177CFB08C4A4B4BDF367843
SHA-256:	21FA4202F16CF7EAA377DA5C78E5A8F267B4D70F2E28C505660182334C4A0525
SHA-512:	E889F91E175B4FE198E00D591486FD328115990E3BA8D5BAE6938730933FDAB005473DDDE3E726E0AA3C62D15A58468E6A39A38E3DA497B4F80A5FA002B623A1
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1056768
Entropy (8bit):	0.34472970102117234
Encrypted:	false
SSDEEP:	768:iQufIJtO+uO/JtYp5uQ+JtQ775ukpJtZJuO/Jt5uJlJt/uXyJt:izfjl+pC8TJcX
MD5:	701A4CC29D67D2D7D055522A27319F65
SHA1:	04017792F6E2CCD969E4DF09E04235A7E9ED674A
SHA-256:	4BE1D2B6A053ECCC8C43534CE7BEB4CF30D67AB23D9C622228A2D2B19AE69D07
SHA-512:	DAA14F8F9E338D704BACC3BAD7D2B69D53DFB9C0264EFC9FEF097D5DA28ADFCD65852090EAB7050C07236D4F18F39DD2300BD2685F2D7E520988A83787B043 E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2	
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4202496
Entropy (8bit):	0.08726857257153237
Encrypted:	false
SSDEEP:	768:muNL/1qLJt2umcJtIqu1JtRCdVSQvxb4E:dLq5m7gVS+4E
MD5:	09FC784FC06CB1206D77AFC0EE5D1909
SHA1:	B2E21FF915658E8523C03AF7CDAE0BB3A3B96203
SHA-256:	2A13485172653D573F6D5B5BD672F18116C35041A84E91BCB9202CFBB0604E83
SHA-512:	39C6CAC99A08A253600CD585073E795B6A0091D2C3B27575C518AA97AD6BBDF1A0C005555A0BA6DEE124EE112FD08A0C74D825CF9FB33DEC226C3125F74A4E8
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.5154898084991041
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwcQPx5fB:TekLLOpEO5J/Kn7U1uB
MD5:	861034A57F72A428F833D9A8C57FDB6C
SHA1:	FE4DE8A11179326A9123EE17DE6A7D05B1068EBB
SHA-256:	CD7D1643DE768BAC3214CDBCF0F5FB08C0FA9F4D81E3EF431CF98569E4165494
SHA-512:	036613279BCD2D8C54EA21C80BA93DCC4D3D23E835D2FD390690011F2679DADEDE3DECAA219D1749348DB859B6D211E325E5483740984BFBBA2A590E8BCA9C
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2279
Entropy (8bit):	3.39402278792876
Encrypted:	false
SSDEEP:	24:34S7HctlrlmbPwrclhSUSWRCDaN/PwryJc0w/PwoHwK/SWRCDaTpL0oCrgo/PwP:34uaxy4cKUS1+B4Oc0E9B/S1+T1ur94r
MD5:	5CDE41CDEF664C8797772849C5A517C4
SHA1:	06144CB58B53EBF7E9735441349DD50BB924C841
SHA-256:	61E9F61A8564716AC1697C93176351A4BD783CE69D18812650B47CD0059D7A63
SHA-512:	C4E7E121FCE0CF5505E022D871C5BA984E4C95F292299210E95B2075F907C406D088047E244289358CFD7B5591EC4D4AD4B0F02A54D1D5008BAB969FAE1AD12
Malicious:	false
Preview:	SNSS.....l.....1.,.....$...cc8be1dd_5612_4b9b_9aed_8197449d9390.....k..... .....l...file:///C:/Users/user/Desktop/lt.servicedesk-VoiceFax-723-2121-723.html.....h.....`..... .....F.8/:...G.8/:...@.....X.....l...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.l.t...s.e.r.v.i.c.e.d.e.s.k.-.V.o.i.c.e.F.a.x.-.7.2.3.-.2.1.2.1.-.7.2.3...h.t.m.l.....8.....0.....8..... .....l...file:///C:/Users/user/Desktop/lt.servicedesk-VoiceFax-723-2121-723.html.....w.0/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	297
Entropy (8bit):	3.5463808523880833
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCT5z/t2qoEwhXeLKI:qWWWWWWWWbopXeLKI
MD5:	746483D0FEBEDA6169B2CEB1EB3A0EF7
SHA1:	2304971D31B736FE61A32C0E3CF8B5CC5232E101
SHA-256:	62CC0023396BC8E5DBB1B6C4AB4E46FD7CA314096BB07593033DF3DB7E869B77
SHA-512:	7F22DE5E98DE8C9AF9D2990BF4F4F792240A7A01F32318C63EDF2AC9B6661D8C49ABFF0DC1AE6F0214607622451C187A551DDADCBC9248D726E829273D3BB6A
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.130118060659951
Encrypted:	false
SSDEEP:	6:mVYF+q2P923iKKdK8aPrqIFUtsYbZmweYrVkwO923iKKdK8amLJ:JF+v45KkL3FUtvb/RrV5L5KkQJ
MD5:	5C761395F83FA500796A4D4732FA4DED
SHA1:	3862E136E91C29F8E95FE5CCB1C4CCADD664394A
SHA-256:	D541D93C2C888CD2EA777E0B04F54BCF7D154E3BB2B9160E226BE53E76F73AB9
SHA-512:	D8354B7F2C693DA15755AF2C1F78C3CBBFC324F7C016C16AF1865C26A1C203D9A3A166DCFC7FF9CC0A28775F1187921AD110A0FBCBCB9FEDA381EA16D6663D2D
Malicious:	false
Preview:	2021/12/03-01:03:45.316 112c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/12/03-01:03:45.318 112c Recovering log #3.2021/12/03-01:03:45.318 112c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.oldx (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.130118060659951
Encrypted:	false
SSDEEP:	6:mVYF+q2P923iKKdK8aPrqIFUtsYbZmweYrVkwO923iKKdK8amLJ:JF+v45KkL3FUtvb/RrV5L5KkQJ
MD5:	5C761395F83FA500796A4D4732FA4DED
SHA1:	3862E136E91C29F8E95FE5CCB1C4CCADD664394A
SHA-256:	D541D93C2C888CD2EA777E0B04F54BCF7D154E3BB2B9160E226BE53E76F73AB9
SHA-512:	D8354B7F2C693DA15755AF2C1F78C3CBBFC324F7C016C16AF1865C26A1C203D9A3A166DCFC7FF9CC0A28775F1187921AD110A0FBCBCB9FEDA381EA16D6663D2D
Malicious:	false
Preview:	2021/12/03-01:03:45.316 112c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/12/03-01:03:45.318 112c Recovering log #3.2021/12/03-01:03:45.318 112c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWe:
MD5:	6C88FEEDEE47B405DCBB87ABEBC47027
SHA1:	C28B0EB68BAB44D7D6F514351A3BDFCD70A3941E
SHA-256:	153DDD24CD5DBCA43DC2071DDF4BE156DCBF32FB3338A2815023358A9740F708
SHA-512:	A78C7A534278ADF5D741C721D7109E0E421C3C43EF0E3E4265E9A9BA9AECD8E1FC14268183CE5CCA79523D1B1554AA29E708DF54023720D37929658359E242A
Malicious:	false
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5..... ....f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.134236451082993
Encrypted:	false
SSDEEP:	6:mVY2RGSQ+q2P923iKKdK8NIFUtsY2QIigZmweYoxSQVkwO923iKKdK8+eLJ:JBOv45KkpFUtv1IH/REF5L5KkqJ
MD5:	F9764ED5AC08176DC9BEE441958D9EF3
SHA1:	A14BC63926EFB366930AD14F002F52280402D186
SHA-256:	5AEC637116AEB07D7689EEE079752C79864448C7FD170BF40B72F3F10558E5A3
SHA-512:	CC040EE3D6B0CD7B7722889F5B65A823020A77B9229B106DEDFCDB1FC25CE028662968C025E999596FA00F9906C686C540B0B19654A3D1552C9793BB75799B4I
Malicious:	false
Preview:	2021/12/03-01:03:47.134 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/12/03-0 1:03:47.135 1408 Recovering log #3.2021/12/03-01:03:47.142 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.oldMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.134236451082993
Encrypted:	false
SSDEEP:	6:mVY2RGSQ+q2P923iKKdK8NIFUtsY2QIigZmweYoxSQVkwO923iKKdK8+eLJ:JBOv45KkpFUtv1IH/REF5L5KkqJ
MD5:	F9764ED5AC08176DC9BEE441958D9EF3
SHA1:	A14BC63926EFB366930AD14F002F52280402D186
SHA-256:	5AEC637116AEB07D7689EEE079752C79864448C7FD170BF40B72F3F10558E5A3
SHA-512:	CC040EE3D6B0CD7B7722889F5B65A823020A77B9229B106DEDFCDB1FC25CE028662968C025E999596FA00F9906C686C540B0B19654A3D1552C9793BB75799B4I
Malicious:	false
Preview:	2021/12/03-01:03:47.134 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/12/03-0 1:03:47.135 1408 Recovering log #3.2021/12/03-01:03:47.142 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.217518321530676
Encrypted:	false
SSDEEP:	6:mVYBLhcMM+q2P923iKKdK25+Xqx8chI+IFUtsYBLPhZmweYBLbzMVkwO923iKKdP:JBxM+v45KkTXfchI3FUtvBDh/RBbMV5Y
MD5:	4268D523EA1C9DB5C64382E0E8CECCFB
SHA1:	CE45F2FDAE6764B8C3B0AC83B16006AA60AD7D17
SHA-256:	80C4E03DD5B2A193960A99BD28504E1D56A3818F38D66BCFD79A065EF8E75FAE
SHA-512:	BA1E51B39F00212475F3FFD3C60F43280072C327339BE165FB99DFD54F4966C10A59C00213DC753590BB9DBCF4379ADFC4292D6D7946D3F0D27104464925C42D
Malicious:	false
Preview:	2021/12/03-01:03:51.863 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/03-01:03:51.866 128c Recovering log #3.2021/12/03-01:03:51.869 128c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.217518321530676
Encrypted:	false
SSDEEP:	6:mVYBLhcMM+q2P923iKKdK25+Xqx8chI+IFUtsYBLPhZmweYBLbzMVkwO923iKKdP:JBxM+v45KkTXfchI3FUtvBDh/RBbMV5Y
MD5:	4268D523EA1C9DB5C64382E0E8CECCFB
SHA1:	CE45F2FDAE6764B8C3B0AC83B16006AA60AD7D17
SHA-256:	80C4E03DD5B2A193960A99BD28504E1D56A3818F38D66BCFD79A065EF8E75FAE
SHA-512:	BA1E51B39F00212475F3FFD3C60F43280072C327339BE165FB99DFD54F4966C10A59C00213DC753590BB9DBCF4379ADFC4292D6D7946D3F0D27104464925C42D
Malicious:	false
Preview:	2021/12/03-01:03:51.863 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/03-01:03:51.866 128c Recovering log #3.2021/12/03-01:03:51.869 128c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.158964945255967
Encrypted:	false
SSDEEP:	6:mVYBLM0M+q2P923iKKdK25+XuoIFUtsYBLmhZmweYBLm0MVkwO923iKKdK25+Xu6:JBlM+v45KkTXYFUtvBKh/RBK0MV5L5Ky
MD5:	EB8895129CB203119C84B964224374AD
SHA1:	960198C871B04C53937438B4C2083D29D30CB050
SHA-256:	23D57DFAC245D41B6FF34043E916560954C254C9D031A011BD9EE2C682A8292A
SHA-512:	887D9D5236990E04F1E4870D9F945B7BB59760934DB70D2C5E0C73C49A44D16A1A1130883517652A1F95B9D25B78C85B3C5DE45002D8671843CE21C5C6735A4C
Malicious:	false
Preview:	2021/12/03-01:03:51.852 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/12/03-01:03:51.854 128c Recovering log #3.2021/12/03-01:03:51.854 128c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.158964945255967
Encrypted:	false
SSDEEP:	6:mVYBLM0M+q2P923iKKdK25+XuoIFUtsYBLmhZmweYBLm0MVkwO923iKKdK25+Xu6:JBlM+v45KkTXYFUtvBKh/RBK0MV5L5Ky
MD5:	EB8895129CB203119C84B964224374AD
SHA1:	960198C871B04C53937438B4C2083D29D30CB050

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
SHA-256:	23D57DFAC245D41B6FF34043E916560954C254C9D031A011BD9EE2C682A8292A
SHA-512:	887D9D5236990E04F1E4870D9F945B7BB59760934DB70D2C5E0C73C49A44D16A1A1130883517652A1F95B9D25B78C85B3C5DE45002D8671843CE21C5C6735A4C
Malicious:	false
Preview:	2021/12/03-01:03:51.852 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/12/03-01:03:51.854 128c Recovering log #3.2021/12/03-01:03:51.854 128c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.203397943221925
Encrypted:	false
SSDEEP:	6:mVYBLKd4q2P923iKKdKWT5g1IdqIFUtsYBL3FnVNJZmweYBL3sv3DkwO923iKKd6:JB7v45Kkg5gSRFUtvBJVX/RBz8z5L5Kg
MD5:	1FCFFC170C9BA1026686EB7C9131FD49
SHA1:	B52F243BBF447D65FE7E436956C802E804A4E057
SHA-256:	3D5FF43746FB94581F1446C3CFC70CA075A1AFA1AEDF254ABD85E9CD559A4112
SHA-512:	E133C9F22A511683B28C3A18278117CE3D426DF6093ADF92CEFB275EFDD2B1693CB29CE1E24AE9ECA9282DA70E7C435A39B8190FCD6EFD140C1321CF0B0342 7
Malicious:	false
Preview:	2021/12/03-01:03:51.683 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/12/03-01:03:51.684 1980 Recovering log #3.2021/12/03-01:03:51.685 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.203397943221925
Encrypted:	false
SSDEEP:	6:mVYBLKd4q2P923iKKdKWT5g1IdqIFUtsYBL3FnVNJZmweYBL3sv3DkwO923iKKd6:JB7v45Kkg5gSRFUtvBJVX/RBz8z5L5Kg
MD5:	1FCFFC170C9BA1026686EB7C9131FD49
SHA1:	B52F243BBF447D65FE7E436956C802E804A4E057
SHA-256:	3D5FF43746FB94581F1446C3CFC70CA075A1AFA1AEDF254ABD85E9CD559A4112
SHA-512:	E133C9F22A511683B28C3A18278117CE3D426DF6093ADF92CEFB275EFDD2B1693CB29CE1E24AE9ECA9282DA70E7C435A39B8190FCD6EFD140C1321CF0B0342 7
Malicious:	false
Preview:	2021/12/03-01:03:51.683 1980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/12/03-01:03:51.684 1980 Recovering log #3.2021/12/03-01:03:51.685 1980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4777368640486825
Encrypted:	false
SSDEEP:	96:F/tReU+bDoYysX0uhnydVjN9DLjGQLBE3uY:F/rt+bDo3irhnydVj3XBBE3uY
MD5:	17524EC978DB165AF7EFBFBC8329741F
SHA1:	C9AB59306A73A99380CA0B5CFA79B22945BEF38E
SHA-256:	510C78D11B2373CFC01455F7A134D95EA3B900497A83AFC3788B152D88A7DBF2
SHA-512:	68E9F0AAB33830ED40BFD7521F647FF3ADA3A456CDE103ADA3E26E2D09BC6FAB51EB855713E4BCA97D958DE707C9560765DCD4093D2547E40F890F1F97AAC6 B9
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Category:	dropped
Size (bytes):	803
Entropy (8bit):	5.341662597164978
Encrypted:	false
SSDEEP:	24:LPCZsVv22FBhFdXAwwDY78BJgskfa9yBDOnWJ/PwY/CAB:jCSQ2FBdXgHUBr/CAB
MD5:	0E4EA2548313FF7661D888A686522284
SHA1:	F377F164F8F7018B5203079B9216C3AC5FC506D6
SHA-256:	2ACFC7AAAB19AF3ACD3F38BEC1C9DD6C6E92B273C1662D5324C8997C05BF003F
SHA-512:	52846CDD10180098D67918D114CFC27A1034D6DE3AFF4C7DA5A57BFD49EC8F4C4A9CD2BAD941DEEED68F3B299D5EE6DD00D2CBD298842BCD75AC9F14E0F104B
Malicious:	false
Preview:	....."a....2121..723..user..c..desktop..file..html..it..login..microsoft..servicedesk..users..voicefax*.....2121.....723.....user.....c.....desktop.....file.....html.....it.....login.....microsoft.....servicedesk.....users.....voicefax..2.....1.....2.....3.....7.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....x...:w.....B.....~..... .....*Ifile:///C:/Users/user/Desktop/It.servicedesk-VoiceFax-723-2121-723.html2.Microsoft | Login:.....J..... #/8<AE....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	0.21903356807606275
Encrypted:	false
SSDEEP:	3:Xh5lln3lljq7A/mhWJFuQ3yy7IOWUnC9ol/dweytllrE9SFcTp4AGZVV9RUIR:x5vs75fOs+/d0Xi99pG/H
MD5:	CD321F42A252D63BA3C2EBC4AC683642
SHA1:	D290EE4D8252AB10A83327CFE68ACA78B0EB77E5
SHA-256:	E04538A94259B1F20D0B86E26E3B2EE7F1C94A770E6F9E602B127599DDEBF7DD
SHA-512:	76258E074BDE6186A97FD7F6619C80AF33CC7CC97387979A202038EE6E4D267E2D99A47FCC97CB5A9CEA759F337B5388B0F5AF1E04AED4A461C9A4323B2F8EE
Malicious:	false
Preview:	.....}/..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session e (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2279
Entropy (8bit):	3.39402278792876
Encrypted:	false
SSDEEP:	24:34S7HctlrImb/PwrclhSUSWRCDaN/PwryJc0w/PwoHwK/SWRCDaTpL0oCrgo/PwP:34uaxy4cKUS1+B4Oc0E9B/S1+T1ur94r
MD5:	5CDE41CDEF664C8797772849C5A517C4
SHA1:	06144CB58B53EBF7E9735441349DD50BB924C841
SHA-256:	61E9F61A8564716AC1697C93176351A4BD783CE69D18812650B47CD0059D7A63
SHA-512:	C4E7E121FCE0CF5505E022D871C5BA984E4C95F292299210E95B2075F907C406D088047E244289358CFD7B5591EC4D4AD4B0F02A54D1D5008BAB969FAE1AD12
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...cc8be1dd_5612_4b9b_9aed_8197449d9390.....k..... .....I...file:///C:/Users/user/Desktop/It.servicedesk-VoiceFax-723-2121-723.html.....h.....`..... .....F.8/:...G.8/:...@.....X.....I...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.I.t...s.e.r.v.i.c.e.d.e.s.k.-.V.o.i.c.e.F.a.x.-.7.2.3.-.2.1.2.1.-.7.2.3...h.t.m.l.....8.....0.....8..... .....I...file:///C:/Users/user/Desktop/It.servicedesk-VoiceFax-723-2121-723.html.....w.0/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.098923727172943
Encrypted:	false
SSDEEP:	6:mVYHOq2P923iKKdK8a2jMGIFUtsYjOZmweYBuXkwO923iKKdK8a2jMmLJ:Juv45Kk8EFUtv6/RBuX5L5Kk8bJ
MD5:	BF924293F07C79A4A4B297C24980BA51
SHA1:	94AE280186D7F7649EF1E1FAFC30C1B9B3A7AC4F
SHA-256:	E623CDC4207D61DA48CC81D0FEE8BDDBC6543A842B5BC36A1E3E4E4999FBBB04
SHA-512:	5622B481F147A35C68012C818D10C3A3836D5E3B201CFF26DE83971CE445892022A058E05BFAF52F83F741EE23E0E23EEF035FCB087441982491FD411B76D119
Malicious:	false
Preview:	2021/12/03-01:03:44.711 1f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/12/03-01:03:44.718 1f0 Recovering log #3.2021/12/03-01:03:44.721 1f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.098923727172943
Encrypted:	false
SSDEEP:	6:mVYHOq2P923iKKdK8a2jMGIFUtsYjOZmweYBuXkwO923iKKdK8a2jMmLJ:Juv45Kk8EFUtv6/RBuX5L5Kk8bJ
MD5:	BF924293F07C79A4A4B297C24980BA51
SHA1:	94AE280186D7F7649EF1E1FAFC30C1B9B3A7AC4F
SHA-256:	E623CDC4207D61DA48CC81D0FEE8BDDBC6543A842B5BC36A1E3E4E4999FBBB04
SHA-512:	5622B481F147A35C68012C818D10C3A3836D5E3B201CFF26DE83971CE445892022A058E05BFAF52F83F741EE23E0E23EEF035FCB087441982491FD411B76D119
Malicious:	false
Preview:	2021/12/03-01:03:44.711 1f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/12/03-01:03:44.718 1f0 Recovering log #3.2021/12/03-01:03:44.721 1f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent 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):	1994
Entropy (8bit):	4.894512343567444
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zsGRsRZGsARLsvfArqXsqMHTYhbxD:JnxOTCXDH+zMnMK1rcG0hVD
MD5:	0F3CEAAE52AB02419C7EF6FF4EB85DF4
SHA1:	7EF7B7C38BF4347B25A02F231A38D73F8C0D5C54
SHA-256:	84586F25A3AADC7E9185691C99D8D460263E98C7794762551C586FA5251BC491
SHA-512:	1A6543ACEAB3D77982FA7F57D9C49F1EC5788157C8EE07630FAA5A2E8E73481859D7CFF5155CF6150546EFD7051C86F2F46DD5BF1713525A5F87664ED826F105
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285587827524442","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com"},{"alternative_service":[{"advert

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent 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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.165325189638236
Encrypted:	false
SSDEEP:	6:mVYhQ+q2P923iKKdKgXz4rRIFUtsY6QgZmweYnQVkwO923iKKdKgXz4q8LJ:Jbv45KkgXiuFUtv65/RI5L5KkgX2J
MD5:	945309F4149DE03AA998C3FE842311C2
SHA1:	BE93F1189D553EC739CDE4AA75BF524EFE360481
SHA-256:	18A90B54D32F2E1667D17F0D691C3E81E3D41EE743AD97DEE0CA0B9DE5AD68E8
SHA-512:	86AC417B93739AEE7661D19AB63952CA3CD00549C47FC71CB63EDD235701ADE5866C781A0C44F51DE20B8CDCC2C9B92F9E9135865B75E7316BFD5D1E7C0F3AD4
Malicious:	false
Preview:	2021/12/03-01:03:45.388 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/12/03-01:03:45.393 1408 Recovering log #3.2021/12/03-01:03:45.395 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old:u (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.165325189638236
Encrypted:	false
SSDEEP:	6:mVYhQ+q2P923iKKdKgXz4rRIFUtsY6QgZmweYnQVkwO923iKKdKgXz4q8LJ:Jbv45KkgXiuFUtv65/RI5L5KkgX2J
MD5:	945309F4149DE03AA998C3FE842311C2
SHA1:	BE93F1189D553EC739CDE4AA75BF524EFE360481
SHA-256:	18A90B54D32F2E1667D17F0D691C3E81E3D41EE743AD97DEE0CA0B9DE5AD68E8
SHA-512:	86AC417B93739AEE7661D19AB63952CA3CD00549C47FC71CB63EDD235701ADE5866C781A0C44F51DE20B8CDCC2C9B92F9E9135865B75E7316BFD5D1E7C0F3AD4
Malicious:	false
Preview:	2021/12/03-01:03:45.388 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/12/03-01:03:45.393 1408 Recovering log #3.2021/12/03-01:03:45.395 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

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):	4786
Entropy (8bit):	4.935943314151862
Encrypted:	false
SSDEEP:	48:YckpklSiklqicyqAPqqTlYclQKHoTw0pB1aPc8C1Nfct/9BhUJo3KhmeSnpNGz0p:n1rRrY9pSKIGIk0JCKL8xpbOTQVuwn
MD5:	A375C872766372415FAAAD364EF6B7C3
SHA1:	67F7B1C3E5AD90E8837A4111EC40EA67BDA4FA2D
SHA-256:	473A0DE1B02F4525894769BF53BF8263D55206183C62DF04C564D2FF342965AE
SHA-512:	F84F625CB4C6EB3ECD96E8B7CAB48B51875886607FA638EAC4A9CE79669C9925AF71E3BB96B49498FE8588F384281E65979A0B7F736BDD30A545392D28C81085
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13282995825308949","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

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):	4876
Entropy (8bit):	4.945955386789302
Encrypted:	false
SSDEEP:	48:YckpklSiklqic6bhqAPqqTlYclQKHoTw0pB1aPc8C1Nfct/9BhUJo3KhmeSnpNGb:n1rRtY9pSKIGIk0JCKL8xObOTQVuwn
MD5:	802A61A91A79CF8F88B65E4DF2F23EB8
SHA1:	11D3B00D2AD32356E4E33DBA809B1229BC915933
SHA-256:	4B1B9037F8A291AB10C1C3834EB167A9C78FBBF5D744FC14892C2ADC0506D55B
SHA-512:	1B42CB195A2C12DD04C33548C9235C1455C4F621DCB298D382CC452053D1331A8404DCC773C7F2114DBA804450315D3DD42CDDA0812F64ED8DCEB0B8870788
Malicious:	false
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13282995825308949","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	0.9522710417512729
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU1cEB0dWGI0jEe:wIElwQF8mpcSasx0obFh0Pb7/dvsl7w1
MD5:	EBC2626C53C8EF6DEA5ECC13DD88B945
SHA1:	A55DB1F654AD17980E919B6F40A476E708D1DD09
SHA-256:	2CE0C35CA1D7E42FA4A7533BC6552200E097C7C050E631B0724422005A4BE63A
SHA-512:	5F7E538AC15DE8EA25A8A68503A464C286EFA426DE313EAA72068BB1F2E1F2D4107B5F3C1647DC8233C751DE0E3965AB2D6B35E59010427A5E9EE7DBABE8528 B
Malicious:	false
Preview:	

SQLite format 3......@ ....C..........g...^.........j..
....
....
....

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):	16608
Entropy (8bit):	5.579891333832027
Encrypted:	false
SSDEEP:	384:sZltfLlPMX11kXqKf/pUZNCgVLH2HfDkrUEAxAfyT4r:wLlm11kXqKf/pUZNCgVLH2HfgrUXxxTE
MD5:	3C85B38781F7C7D5980C3962280926BE
SHA1:	FC4FCFA8D7A370C92B5CF15A64B1CCAAE646B06F
SHA-256:	09033A4B809B5FC49EE39E33A6F9FFB47D018A80E6F8369767D9A1C669AC4BDC
SHA-512:	9F3D8BE4609559706A37AD5DD19F051EF770031AA99855211AB40BBB53F17CFC335CB6B79328116F39C097697D3259C881064BF4A8FB4D42091390E6F6453577
Malicious:	false
Preview:	

{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy
stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":
[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282995824689010","location":5,"manifest":{"a
pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and
themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt
l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG
ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencest (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):	16607
Entropy (8bit):	5.5798491604600065
Encrypted:	false
SSDEEP:	384:sZltILlPMX11kXqKf/pUZNCgVLH2HfDkrUEDuAfyT4X:tLlm11kXqKf/pUZNCgVLH2HfgrUauxTo
MD5:	878B52FB9F94C77F610112E53C37EC8F
SHA1:	5859058A56C5C2E03F0C5B04E315A2D9CEA0AADF
SHA-256:	4A0D503C7874482B123689F0C101DF0D9BE265147C3B68039CCAC2BD1485BDE7
SHA-512:	249B9A05E7920BD1FCFDC3744EC2F3E9D57CDF48A9995A1196F51AEF53CA62FF668507993AD73893B5C625CE0828BDB57A76A855077E762AD0A1F39AE632EFA D
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282995824689010","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	308
Entropy (8bit):	2.564952422771833
Encrypted:	false
SSDEEP:	6:S85aEFljljljljljljljljljljljljljljl:S+a8ljljljljljljljljljljljl
MD5:	4E7982B86B3D7D916B7722AA3B3F0669
SHA1:	CE4E874903CB71D9012CC7654CA7A6BA5E4F7EFD
SHA-256:	CBEE1100A2C9ADD47776B7E416B58A809F6FEB9FE458BEF8185B0C176B5DB340
SHA-512:	C4DDA8B36E90A327061DAB901730F47FC23CCA129B02A157F1ED0C566A1D6DDDF272A4E74D3ACBF14EB3A7FAC0820387A584DB9E19CA299724ED7F3030F891 BB
Malicious:	false
Preview:	*...#.....version.1..namespace-...&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.... .....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.1213791930070665
Encrypted:	false
SSDEEP:	6:mVY2CM4q2P923iKKdKrQMxIFUtsY21j3JZmweY22HDkwO923iKKdKrQMFLJ:J2CM4v45KkCFUtv2hJ/R22HD5L5KktJ
MD5:	61312AEDF540232E727A4C7A6172648B
SHA1:	D467321FA5A696690671F9245BED3526991AFFED
SHA-256:	64C1518556BA8F1756E7CDD3B096A63A5509420DC686C157A561F31C5A5534A6
SHA-512:	142498BF887F2B7EC1AEC166A38CA870BE514E62C1859C54D5E5972B108C9199A9894A20E3F8201EB046132F4C3E0021E462E88FE00EA735C109DDFCB27C3C0
Malicious:	false
Preview:	2021/12/03-01:03:45.262 11b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/12/03-0 1:03:45.264 11b4 Recovering log #3.2021/12/03-01:03:45.245 11b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.1213791930070665
Encrypted:	false
SSDEEP:	6:mVY2CM4q2P923iKKdKrQMxIFUtsY21j3JZmweY22HDkwO923iKKdKrQMFLJ:J2CM4v45KkCFUtv2hJ/R22HD5L5KktJ
MD5:	61312AEDF540232E727A4C7A6172648B
SHA1:	D467321FA5A696690671F9245BED3526991AFFED

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
SHA-256:	64C1518556BA8F1756E7CDD3B096A63A5509420DC686C157A561F31C5A5534A6
SHA-512:	142498BF887F2B7EC1AEC166A38CA870BE514E62C1859C54D5E5972B108C9199A9894A20E3F8201EB046132F4C3E0021E462E88FE00EA735C109DDFCB27C3C0
Malicious:	false
Preview:	2021/12/03-01:03:45.262 11b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/12/03-01:03:45.264 11b4 Recovering log #3.2021/12/03-01:03:45.245 11b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.082546288533411
Encrypted:	false
SSDEEP:	6:mVYs4q2P923iKKdK7Uh2ghZIFUtsY7BJZmweYhNxNDkwO923iKKdK7Uh2gnLJ:Js4v45KklhHh2FUtvdJ/RhNrD5L5KkIT
MD5:	1A2973C3C831C004820F589A493AC9CD
SHA1:	BEEF4268EB5E9199F9E5DAA6EC140DBCD0707484
SHA-256:	09641EF0ED39AC8DDC86359D41F3EA4B5443F742B37B6B4FBB4FD9883F00801D
SHA-512:	9D71E91C5A66FD1454CDDA0767A28903578CA6B127E66300D352CF06AC90DAEE0B16125FF6905AA2FC7BBE8A4AB427864835D1124C10D87C92D5F576A17123A
Malicious:	false
Preview:	2021/12/03-01:03:44.700 11b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/12/03-01:03:44.710 11b4 Recovering log #3.2021/12/03-01:03:44.712 11b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.082546288533411
Encrypted:	false
SSDEEP:	6:mVYs4q2P923iKKdK7Uh2ghZIFUtsY7BJZmweYhNxNDkwO923iKKdK7Uh2gnLJ:Js4v45KklhHh2FUtvdJ/RhNrD5L5KkIT
MD5:	1A2973C3C831C004820F589A493AC9CD
SHA1:	BEEF4268EB5E9199F9E5DAA6EC140DBCD0707484
SHA-256:	09641EF0ED39AC8DDC86359D41F3EA4B5443F742B37B6B4FBB4FD9883F00801D
SHA-512:	9D71E91C5A66FD1454CDDA0767A28903578CA6B127E66300D352CF06AC90DAEE0B16125FF6905AA2FC7BBE8A4AB427864835D1124C10D87C92D5F576A17123A
Malicious:	false
Preview:	2021/12/03-01:03:44.700 11b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/12/03-01:03:44.710 11b4 Recovering log #3.2021/12/03-01:03:44.712 11b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\03d04461-d71d-46ec-acdf-72cb337dcb02.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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 58
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.172504790837028
Encrypted:	false
SSDEEP:	6:mVY++q2P923iKKdKusNpV/2jMGIFUtsYqUpXZmweYEOiVkwO923iKKdKusNpV/23:J++v45KkFFUtvvpX/RoV5L5KkOJ
MD5:	D7674D5F53210AFC499213794FA5CEDC
SHA1:	DBEE83C804B87AF6B9A9BF1A279AAB0377991212
SHA-256:	9A0D5AA40364A78A0F953454CAADD3C0929489871643B75C4994C24B0C73C041
SHA-512:	7C77B28496135F95C336261D2227F73FB8E6356FFBE3C581D541C76587531848E2ACF7417E14C20C42CB439A553112865C056F06F34837C7041211A758D1A92E
Malicious:	false
Preview:	2021/12/03-01:03:45.300 112c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/12/03-01:03:45.301 112c Recovering log #3.2021/12/03-01:03:45.302 112c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.172504790837028
Encrypted:	false
SSDEEP:	6:mVY++q2P923iKKdKusNpV/2jMGIFUtsYqUpXZmweYEOiVkwO923iKKdKusNpV/23:J++v45KkFFUtvvpX/RoV5L5KkOJ
MD5:	D7674D5F53210AFC499213794FA5CEDC
SHA1:	DBEE83C804B87AF6B9A9BF1A279AAB0377991212
SHA-256:	9A0D5AA40364A78A0F953454CAADD3C0929489871643B75C4994C24B0C73C041
SHA-512:	7C77B28496135F95C336261D2227F73FB8E6356FFBE3C581D541C76587531848E2ACF7417E14C20C42CB439A553112865C056F06F34837C7041211A758D1A92E
Malicious:	false
Preview:	2021/12/03-01:03:45.300 112c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/12/03-01:03:45.301 112c Recovering log #3.2021/12/03-01:03:45.302 112c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent 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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.273290675505093
Encrypted:	false
SSDEEP:	6:mVYjQ+q2P923iKKdKusNpqz4rRIFUtsYGpgZmweYiQVkwO923iKKdKusNpqz4q8d:JjQ+v45KkmiuFUtvGpg/RiQV5L5Kkm2J
MD5:	5BB15F34818A15B69CBA57B8556D1AF3
SHA1:	5893DDD753D4D1CF98FD8A9575C805A9AC3C7346
SHA-256:	0CC49B7C91B2684CFEF1C5F51D58022E8081220313BC5EFEE5EB3109AEC0EC09
SHA-512:	653F2FB525C67B36C3B5C042E862E49F914CA6C6E44A5960C9B526D88E1AF3A9E383ED22F75BF7C5EB42BF2E6D0F735865C831AE4E8E20CA1B780A3CF1FDB6 7
Malicious:	false
Preview:	2021/12/03-01:03:45.379 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/12/03-01:03:45.387 15dc Recovering log #3.2021/12/03-01:03:45.389 15dc Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old]a (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.273290675505093
Encrypted:	false
SSDEEP:	6:mVYjQ+q2P923iKKdKusNpqz4rRIFUtsYGpgZmweYiQVkwO923iKKdKusNpqz4q8d:JjQ+v45KkmiuFUtvGpg/RiQV5L5Kkm2J
MD5:	5BB15F34818A15B69CBA57B8556D1AF3
SHA1:	5893DDD753D4D1CF98FD8A9575C805A9AC3C7346
SHA-256:	0CC49B7C91B2684CFEF1C5F51D58022E8081220313BC5EFEE5EB3109AEC0EC09
SHA-512:	653F2FB525C67B36C3B5C042E862E49F914CA6C6E44A5960C9B526D88E1AF3A9E383ED22F75BF7C5EB42BF2E6D0F735865C831AE4E8E20CA1B780A3CF1FDB6 7
Malicious:	false
Preview:	2021/12/03-01:03:45.379 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/12/03-01:03:45.387 15dc Recovering log #3.2021/12/03-01:03:45.389 15dc Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E6 67
Malicious:	false
Preview:	*...#.....version.1..namespace-...&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.202652584970189
Encrypted:	false
SSDEEP:	6:mVgGQ+q2P923iKKdKusNpZQMxIFUtsgIgZmweg/LQVkwO923iKKdKusNpZQMFLJ:kQ+v45KkMFUtsg/BQV5L5KkTJ
MD5:	7280A3CAE62A756BB3307F1D24829387
SHA1:	40B06565336BC76AE3C74151BB88BAE6A1FBC211
SHA-256:	F2AE9205C1B3834B54503B05BD5DD1AF9C2A001755C3689C8AE524F694302AFA
SHA-512:	6A20321F8889C2DB9A6D6C80547A5523DBD8612F52CF5278A8D3360BD840740C0930368167FD4F70DD44555740F01788AF7D31D89F285667163DCEDD7CDEDF8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Malicious:	false
Preview:	2021/12/03-01:04:01.353 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/12/03-01:04:01.355 15dc Recovering log #3.2021/12/03-01:04:01.356 15dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldcm (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.202652584970189
Encrypted:	false
SSDEEP:	6:mVgGQ+q2P923iKKdKusNpZQMxIFUtsgIgZmweg/LQVkwO923iKKdKusNpZQMFLJ:kQ+v45KkMFUtsg/BQV5L5KkTJ
MD5:	7280A3CAE62A756BB3307F1D24829387
SHA1:	40B06565336BC76AE3C74151BB88BAE6A1FBC211
SHA-256:	F2AE9205C1B3834B54503B05BD5DD1AF9C2A001755C3689C8AE524F694302AFA
SHA-512:	6A20321F8889C2DB9A6D6C80547A5523DBD8612F52CF5278A8D3360BD840740C0930368167FD4F70DD44555740F01788AF7D31D89F285667163DCEDD7CDEDF8
Malicious:	false
Preview:	2021/12/03-01:04:01.353 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/12/03-01:04:01.355 15dc Recovering log #3.2021/12/03-01:04:01.356 15dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	160
Entropy (8bit):	3.0217164415295743
Encrypted:	false
SSDEEP:	3:sLollttz6sjlGXU2tk0lkGgGgGgGg:qolXtWswXU2tkEtttt
MD5:	DE92AD90BE6D3364745B2F73F4C3CF73
SHA1:	9158681463BD30E5AF4DDA4BAAC81F93CEDBDA77
SHA-256:	0025A3E0D3B834401B3B5F820E1991EF7E810D9A4B8B6B579E6301C94E7031A0
SHA-512:	9E81CEFC195439439F4B23EE7696309D7BC3C08E5B444D2ABDE26D2F12B2D3BCFD124FB9A2D40C6389E9F787741676FAD366A2E9982674E7B931028C014D8A7
Malicious:	false
Preview:	...n'....._mts_schema_descriptor.....F.....F.....F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.183693152743056
Encrypted:	false
SSDEEP:	6:mVY2Eq2P923iKKdKpIFUtsYQiZmweYSOkwO923iKKdKa/WLJ:J2Ev45KkmFUtvL/RSO5L5KkaUJ
MD5:	B32CD37459933FE9409F543671026D9F
SHA1:	EA82CDDD3F03C6138EB62DF83F90E6526A364744
SHA-256:	1E74A83A8DFA8ACFBC1C54C55882B230F1A9BCEA603194766DE89663C213BB6F
SHA-512:	05951C6B8A375313B9DCF9E58A7647E38A7331234032DA0532532D7F11409B830F884B3011D40AD3AA13BDDA69CDE636EBB619D18F58C50ADF04ABD1413BE27
Malicious:	false
Preview:	2021/12/03-01:03:44.688 1134 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/12/03-01:03:44.694 1134 Recovering log #3.2021/12/03-01:03:44.696 1134 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.183693152743056
Encrypted:	false
SSDEEP:	6:mVY2Eq2P923iKKdKpIFUtsYQiZmweYSOkwO923iKKdKa/WLJ:J2Ev45KkmFUtvL/RSO5L5KkaUJ
MD5:	B32CD37459933FE9409F543671026D9F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old. (copy)	
SHA1:	EA82CDDD3F03C6138EB62DF83F90E6526A364744
SHA-256:	1E74A83A8DFA8ACFBC1C54C55882B230F1A9BCEA603194766DE89663C213BB6F
SHA-512:	05951C6B8A375313B9DCF9E58A7647E38A7331234032DA0532532D7F11409B830F884B3011D40AD3AA13BDDA69CDE636EBB619D18F58C50ADF04ABD1413BE27
Malicious:	false
Preview:	2021/12/03-01:03:44.688 1134 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/12/03-01:03:44.694 1134 Recovering log #3.2021/12/03-01:03:44.696 1134 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0033616753448762224
Encrypted:	false
SSDEEP:	3:ImtVu9c8tllrtYrXl:IiVuRl8r
MD5:	B226A1BE2BCF9694AF3797EAFA283847
SHA1:	446A65CC07B17E318B01A270A556DDC78B7216D4
SHA-256:	2F898E669AA70B4C2008BFB179A241D8DF597152F192177C90C2FA0A95440E85
SHA-512:	DC02EF946DD3A7CE189A654AA4002F3E8C5427AB7ED00800466571151F064A25BE5B9B30F65A852083928C7AD5A89F676FD3B5D4951706D3FCB2733744A99C42
Malicious:	false
Preview:	VLnk.....?.....B..%$U..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8951853-febc-4f8d-9063-24c2b14eeca0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.361127798472093
Encrypted:	false
SSDEEP:	3:tUKwYBLDsvJZmwv2tYBLJXcLH1V8ttYBLJXcLH1WGv:mVYBLqJZmweYBLJgVV+YBLJgVtv
MD5:	D7E5A107D181CC2126FCE9AF5DB8EE2B
SHA1:	CD35B666AF494419DE2FB4341D2BCAA77A94F802
SHA-256:	A094D810651CAB12D4CCAADD4738DF705843BDD1E0FF71133F899492E038904E
SHA-512:	00E05B6C132CD6A9F20D03667B3CA784F211496F34814DBDE7D9D2CE2B455C0144E03863D7C3604C1ADE15642E478C968428927D6D9BA0DC165E9659C989794
Malicious:	false
Preview:	2021/12/03-01:03:51.036 1980 Recovering log #3.2021/12/03-01:03:51.593 1980 Delete type=0 #3.2021/12/03-01:03:51.593 1980 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old34 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.361127798472093
Encrypted:	false
SSDEEP:	3:tUKwYBLDsvJZmwv2tYBLJXcLH1V8ttYBLJXcLH1WGv:mVYBLqJZmweYBLJgVV+YBLJgVtv
MD5:	D7E5A107D181CC2126FCE9AF5DB8EE2B
SHA1:	CD35B666AF494419DE2FB4341D2BCAA77A94F802
SHA-256:	A094D810651CAB12D4CCAADD4738DF705843BDD1E0FF71133F899492E038904E
SHA-512:	00E05B6C132CD6A9F20D03667B3CA784F211496F34814DBDE7D9D2CE2B455C0144E03863D7C3604C1ADE15642E478C968428927D6D9BA0DC165E9659C989794
Malicious:	false
Preview:	2021/12/03-01:03:51.036 1980 Recovering log #3.2021/12/03-01:03:51.593 1980 Delete type=0 #3.2021/12/03-01:03:51.593 1980 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e1b6a832-8e99-404f-a129-58a683b9e8b9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e1b6a832-8e99-404f-a129-58a683b9e8b9.tmp	
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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e55e62ec-a8a7-45f0-a165-82b1a9de5095.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):	4876
Entropy (8bit):	4.945955386789302
Encrypted:	false
SSDEEP:	48:YckpklSiklqic6bhqAPqqTlYclQKHoTw0pB1aPc8C1Nfct/9BhUJo3KhmeSnpNGb:n1rRtY9pSKIGIk0JCKL8xObOTQVuwn
MD5:	802A61A91A79CF8F88B65E4DF2F23EB8
SHA1:	11D3B00D2AD32356E4E33DBA809B1229BC915933
SHA-256:	4B1B9037F8A291AB10C1C3834EB167A9C78FBBF5D744FC14892C2ADC0506D55B
SHA-512:	1B42CB195A2C12DD04C33548C9235C1455C4F621DCB298D382CC452053D1331A8404DCC773C7F2114DBA804450315D3DD42CDDA0812F64ED8DCEB0B8870788
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282995825308949","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.1604559498472025
Encrypted:	false
SSDEEP:	6:mVY1CoQQ+q2P923iKKdKfrzAdIFUtsY1QTgZmweY1FQVkwO923iKKdKfrzILJ:J1CRv45Kk9FUtv1H/R1O5L5Kk2J
MD5:	3E39472DF36B55A96E83CDF4A738D86A
SHA1:	9BE2E6CD697116A3B8200791E8D0175969F8983A
SHA-256:	8622EED2F5CE4FD1E5FB89E532C8A75560A8438B7BD3A65C40CEC0CFBA176E37
SHA-512:	0DDDDFB481E09AEDEE962961F7BF906E3FBCF5D7E3C774A5FC9592ABCF0821DA04F26332C42D5502BD8C43D482334924182D0BA38044CAD858CFA2A83A3302 8
Malicious:	false
Preview:	2021/12/03-01:03:52.413 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/12/03-01:03:52.415 1408 Recovering log #3.2021/12/03-01:03:52.416 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.1604559498472025
Encrypted:	false
SSDEEP:	6:mVY1CoQQ+q2P923iKKdKfrzAdIFUtsY1QTgZmweY1FQVkwO923iKKdKfrzILJ:J1CRv45Kk9FUtv1H/R1O5L5Kk2J
MD5:	3E39472DF36B55A96E83CDF4A738D86A
SHA1:	9BE2E6CD697116A3B8200791E8D0175969F8983A
SHA-256:	8622EED2F5CE4FD1E5FB89E532C8A75560A8438B7BD3A65C40CEC0CFBA176E37
SHA-512:	0DDDDFB481E09AEDEE962961F7BF906E3FBCF5D7E3C774A5FC9592ABCF0821DA04F26332C42D5502BD8C43D482334924182D0BA38044CAD858CFA2A83A3302 8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old (copy)	
Malicious:	false
Preview:	2021/12/03-01:03:52.413 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/12/03-01:03:52.415 1408 Recovering log #3.2021/12/03-01:03:52.416 1408 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

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):	390414
Entropy (8bit):	6.021396811511392
Encrypted:	false
SSDEEP:	6144:95xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:/kxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	082AE0CE62E93A47426749924CB95D81
SHA1:	A5EAC43BA202F1197114BB263095D1BF9560F031
SHA-256:	F56223625A2140037A45CDE8F1A177CFE08BA8D170FF8B32882863EA16C94BDC
SHA-512:	478D66DAF9791A217F542715D115C2635B271A50F2A5BD44212C48CE6D65B30C0E5A41B7B04EE2D4F0DF547615CEC177B5B6586E4504A8AE5C3799EB3B5A61B
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RF BBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1Qfjo KlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05 zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_man ager":{"os_password_blank":true,"os_password_last_changed":"13245950075673178"},"plugins":{"resource_cache_update":"1638522285.338

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statet (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):	388256
Entropy (8bit):	6.014556387062204
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statet (copy)	
SSDEEP:	6144:l5xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:3kxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	900E887068A5EE636B7A76DB8EADC03D
SHA1:	79AB3F5C61E130EBAD3A781694C6F9B4DFF18A71
SHA-256:	33E5B34D7BB16B16707405C9B93C3B5797BFCEAB83AD8140A152642B755ADBDF
SHA-512:	93314373A19076B52D1A55560CBAE0A4A41140B6A6A2DB741BD3CA1840D57A3B2AAD16C6EF2BF55DCC11A55FB62D370925AB40C2129E1826859133EE6AC43E 7
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075673178"},"policy":{"last_statistics_update":"13282995824436

C:\Users\user\AppData\Local\Google\Chrome\User Data\db070a2c-ded7-4a98-a37d-75c85fef00aa.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):	388256
Entropy (8bit):	6.014556486745422
Encrypted:	false
SSDEEP:	6144:p5xe1jxhfMp3ylJ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB5:jkxhailOxzurRDn9nfNxF4ijZVtilB5
MD5:	D44CF65B90315911CDEB0536FA72EA07
SHA1:	1233E0BD5997DB1D9510924D5C77DF129B0C4E05
SHA-256:	232C2A7F86E54E7379322AFC70419992E137D0AF3FA012355D759557F421A582
SHA-512:	249020C69D91B34B304C5E203831C448E11CF955F4729ABE94534CC08F61BC01B4FDF591718D50BFC9CF048297958273FB674A21F3AECCC5E9650F16D10747C7
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638522227168702e+12,"network":1.638489829e+12,"ticks":119158074.0,"uncertainty":4797837.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13282995824436

Static File Info

General

File type:	HTML document, ASCII text, with very long lines
Entropy (8bit):	5.094520199896907
TrID:	• HyperText Markup Language (12001/1) 51.06% • HyperText Markup Language (11501/1) 48.94%
File name:	It.servicedesk-VoiceFax-723-2121-723.html
File size:	297333
MD5:	53621f89e50983193a3c6761dce91f0e
SHA1:	218d9d6fc72c73d8ea299967ebfe8edf6150d8b5
SHA256:	a76c9007fd100fe51a069435c52818b191ca62b127f7e7e86a48794335e69adf
SHA512:	a9e87b66ffdd84b36c68beaa82270c99595e6f49d66e76865eb640b6ab7bcf41629d895de6cd5892df4bd14aa141f27a388f633f576f015b17cbee3982674018
SSDEEP:	3072:tSXeDuSj+Yrj0Y5CZiw4MRRJyyNJ4MbLD2jDyFjSj9q2qltJq1pxmo:tSXwuSj+Yrj0Y5MiwJyrJ
File Content Preview:	<!doctype html>.<html lang="en">. <head>. <script>. var file = "https://dietcare.us/next.php";. </script>. < script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>. <script src="https://code.jque

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2021 01:03:47.109793901 CET	192.168.2.5	8.8.8.8	0xbee9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:47.155973911 CET	192.168.2.5	8.8.8.8	0xa101	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:47.167249918 CET	192.168.2.5	8.8.8.8	0x28c1	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.784579992 CET	192.168.2.5	8.8.8.8	0xeee	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.786704063 CET	192.168.2.5	8.8.8.8	0x603a	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.788470984 CET	192.168.2.5	8.8.8.8	0x8507	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:49.546499014 CET	192.168.2.5	8.8.8.8	0xb48c	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 01:03:47.131166935 CET	8.8.8.8	192.168.2.5	0xbee9	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:47.184053898 CET	8.8.8.8	192.168.2.5	0xa101	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:03:47.184053898 CET	8.8.8.8	192.168.2.5	0xa101	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:47.184290886 CET	8.8.8.8	192.168.2.5	0x28c1	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:03:48.805239916 CET	8.8.8.8	192.168.2.5	0xeee	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.805239916 CET	8.8.8.8	192.168.2.5	0xeee	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.808727980 CET	8.8.8.8	192.168.2.5	0x603a	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.808727980 CET	8.8.8.8	192.168.2.5	0x603a	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:48.822454929 CET	8.8.8.8	192.168.2.5	0x8507	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:03:49.578035116 CET	8.8.8.8	192.168.2.5	0xb48c	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:03:49.578035116 CET	8.8.8.8	192.168.2.5	0xb48c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.9	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:49.578035116 CET	8.8.8.8	192.168.2.5	0xb48c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.78	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:49.578035116 CET	8.8.8.8	192.168.2.5	0xb48c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.75	A (IP address)	IN (0x0001)
Dec 3, 2021 01:03:49.578035116 CET	8.8.8.8	192.168.2.5	0xb48c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- cdnjs.cloudflare.com
- maxcdn.bootstrapcdn.com
- logo.clearbit.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49739	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:48 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=85.0.4183.121&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-85.0.4183.121 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/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-12-03 00:03:48 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-7s2GzLg8gejJt7TWvgFoxA' 'unsafe-inline' 'strict-dynamic' https: 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: Fri, 03 Dec 2021 00:03:48 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5449 X-Daystart: 57828 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
2021-12-03 00:03:48 UTC	2	IN	Data Raw: 35 31 65 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 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 34 34 39 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 37 38 32 38 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: 51e<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5449" elapsed_seconds="57828"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2021-12-03 00:03:48 UTC	2	IN	Data Raw: 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 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2021-12-03 00:03:48 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	192.168.2.5	49738	172.217.168.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:48 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/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-12-03 00:03:48 UTC	1	OUT	Data Raw: 20 Data Ascii:
2021-12-03 00:03:48 UTC	3	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: Fri, 03 Dec 2021 00:03:48 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Content-Security-Policy: script-src 'report-sample' 'nonce-Z94ZK3nFD0Jyu5AlLY1Aaw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-Z94ZK3nFD0Jyu5AlLY1Aaw' '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 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-03 00:03:48 UTC	4	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",[]]
2021-12-03 00:03:48 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49745	104.16.19.94	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	4	OUT	GET /ajax/libs/popper.js/1.12.9/umd/popper.min.js HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	5	IN	HTTP/1.1 200 OK Date: Fri, 03 Dec 2021 00:03:49 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=30672000 ETag: W/"5eb03fa9-4af4" Last-Modified: Mon, 04 May 2020 16:15:37 GMT cf-cdnjs-via: cfworker/kv Cross-Origin-Resource-Policy: cross-origin Timing-Allow-Origin: * X-Content-Type-Options: nosniff Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" CF-Cache-Status: HIT Age: 879391 Expires: Wed, 23 Nov 2022 00:03:49 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5a7fLdmvxIDG%2Fc0uDFNTJbAEB9xLr3%2Fpdd4Z0XM%2F4cwO5jdfuKrWPomnqrqhQjpec4J9Yr0G%2FN5FJih1DzX6rcqRVwMhf46Jr4xtKadiFWOE1wdKhmcv25YH3%2BqqLAjghkHmECYo"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800} Strict-Transport-Security: max-age=15780000 Server: cloudflare CF-RAY: 6b7888b83fda4e43-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-12-03 00:03:49 UTC	6	IN	Data Raw: 39 36 37 0d 0a 2f 2a 0a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 46 65 64 65 72 69 63 6f 20 5a 69 76 6f 6c 6f 20 32 30 31 37 0a 20 44 69 73 74 72 69 62 75 74 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 28 6c 69 63 65 6e 73 65 20 74 65 72 6d 73 20 61 72 65 20 61 74 20 68 74 74 70 3a 2f 2f 6f 70 65 6e 73 6f 75 72 63 65 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 4d 49 54 29 2e 0a 20 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 27 6f 62 6a 65 63 74 27 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 26 26 27 75 6e 64 65 66 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3a 27 66 75 6e 63 74 69 Data Ascii: 967/* Copyright (C) Federico Zivolo 2017 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT). */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'functi
2021-12-03 00:03:49 UTC	7	IN	Data Raw: 6f 6e 27 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 74 29 3a 65 2e 50 6f 70 70 65 72 3d 74 28 29 7d 29 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 27 75 73 65 20 73 74 72 69 63 74 27 3b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 27 5b 6f 62 6a 65 63 74 20 46 75 6e 63 74 69 6f 6e 5d 27 3d 3d 3d 7b 7d 2e 74 6f 53 74 72 69 6e 67 2e 63 61 6c 6c 28 65 29 7d 66 75 6e 63 74 69 6f 6e 20 74 28 65 2c 74 29 7b 69 66 28 31 21 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 72 65 74 75 72 6e 5b 5d 3b 76 61 72 20 6f 3d 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 65 2c 6e 75 6c 6c 29 3b 72 65 74 75 72 6e 20 74 3f 6f 5b 74 5d 3a 6f 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b Data Ascii: on'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){
2021-12-03 00:03:49 UTC	8	IN	Data Raw: 54 6f 70 27 3a 27 73 63 72 6f 6c 6c 4c 65 66 74 27 2c 69 3d 65 2e 6e 6f 64 65 4e 61 6d 65 3b 69 66 28 27 42 4f 44 59 27 3d 3d 3d 69 7c 7c 27 48 54 4d 4c 27 3d 3d 3d 69 29 7b 76 61 72 20 6e 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 72 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 73 63 72 6f 6c 6c 69 6e 67 45 6c 65 6d 65 6e 74 7c 7c 6e 3b 72 65 74 75 72 6e 20 72 5b 6f 5d 7d 72 65 74 75 72 6e 20 65 5b 6f 5d 7d 66 75 6e 63 74 69 6f 6e 20 6c 28 65 2c 74 29 7b 76 61 72 20 6f 3d 32 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 32 5d 2c 69 3d 61 28 74 2c 27 74 6f 70 27 29 2c 6e 3d 61 28 74 2c Data Ascii: Top':'scrollLeft',i=e.nodeName;if('BODY'===i||'HTML'===i){var n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||n;return r[o]}return e[o]}function l(e,t){var o=2<arguments.length&&void 0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,
2021-12-03 00:03:49 UTC	9	IN	Data Raw: 34 31 38 64 0d 0a 2c 77 69 64 74 68 3a 6d 28 27 57 69 64 74 68 27 2c 65 2c 74 2c 6f 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 63 28 65 29 7b 72 65 74 75 72 6e 20 73 65 28 7b 7d 2c 65 2c 7b 72 69 67 68 74 3a 65 2e 6c 65 66 74 2b 65 2e 77 69 64 74 68 2c 62 6f 74 74 6f 6d 3a 65 2e 74 6f 70 2b 65 2e 68 65 69 67 68 74 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 67 28 65 29 7b 76 61 72 20 6f 3d 7b 7d 3b 69 66 28 69 65 28 29 29 74 72 79 7b 6f 3d 65 2e 67 65 74 42 6f 75 6e 64 69 6e 67 43 6c 69 65 6e 74 52 65 63 74 28 29 3b 76 61 72 20 69 3d 61 28 65 2c 27 74 6f 70 27 29 2c 6e 3d 61 28 65 2c 27 6c 65 66 74 27 29 3b 6f 2e 74 6f 70 2b 3d 69 2c 6f 2e 6c 65 66 74 2b 3d 6e 2c 6f 2e 62 6f 74 74 6f 6d 2b 3d 69 2c 6f 2e 72 69 67 68 74 2b 3d 6e 7d 63 61 74 63 68 28 65 29 7b 7d 65 6c 73 Data Ascii: 418d,width:m('Width',e,t,o)}}function c(e){return se({},e,{right:e.left+e.width,bottom:e.top+e.height})}function g(e){var o={};if(ie())try{o=e.getBoundingClientRect();var i=a(e,'top'),n=a(e,'left');o.top+=i,o.left+=n,o.bottom+=i,o.right+=n}catch(e){}els
2021-12-03 00:03:49 UTC	10	IN	Data Raw: 78 65 64 27 3d 3d 3d 74 28 65 2c 27 70 6f 73 69 74 69 6f 6e 27 29 7c 7c 77 28 6f 28 65 29 29 7d 66 75 6e 63 74 69 6f 6e 20 79 28 65 2c 74 2c 69 2c 72 29 7b 76 61 72 20 70 3d 7b 74 6f 70 3a 30 2c 6c 65 66 74 3a 30 7d 2c 73 3d 64 28 65 2c 74 29 3b 69 66 28 27 76 69 65 77 70 6f 72 74 27 3d 3d 3d 72 29 70 3d 62 28 73 29 3b 65 6c 73 65 7b 76 61 72 20 61 3b 27 73 63 72 6f 6c 6c 50 61 72 65 6e 74 27 3d 3d 3d 72 3f 28 61 3d 6e 28 6f 28 74 29 29 2c 27 42 4f 44 59 27 3d 3d 3d 61 2e 6e 6f 64 65 4e 61 6d 65 26 26 28 61 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 29 3a 27 77 69 6e 64 6f 77 27 3d 3d 3d 72 3f 61 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 3a 61 3d Data Ascii: xed'===t(e,'position')||w(o(e))}function y(e,t,i,r){var p={top:0,left:0},s=d(e,t);if('viewport'===r)p=b(s);else{var a;'scrollParent'===r?(a=n(o(t)),'BODY'===a.nodeName&&(a=e.ownerDocument.documentElement)):'window'===r?a=e.ownerDocument.documentElement:a=
2021-12-03 00:03:49 UTC	11	IN	Data Raw: 74 75 72 6e 20 6e 7d 66 75 6e 63 74 69 6f 6e 20 78 28 65 29 7b 76 61 72 20 74 3d 7b 6c 65 66 74 3a 27 72 69 67 68 74 27 2c 72 69 67 68 74 3a 27 6c 65 66 74 27 2c 62 6f 74 74 6f 6d 3a 27 74 6f 70 27 2c 74 6f 70 3a 27 62 6f 74 74 6f 6d 27 7d 3b 72 65 74 75 72 6e 20 65 2e 72 65 70 6c 61 63 65 28 2f 6c 65 66 74 7c 72 69 67 68 74 7c 62 6f 74 74 6f 6d 7c 74 6f 70 2f 67 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 5b 65 5d 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 53 28 65 2c 74 2c 6f 29 7b 6f 3d 6f 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 3b 76 61 72 20 69 3d 4c 28 65 29 2c 6e 3d 7b 77 69 64 74 68 3a 69 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 69 2e 68 65 69 67 68 74 7d 2c 72 3d 2d 31 21 3d 3d 5b 27 72 69 67 68 74 27 2c 27 6c 65 66 74 27 5d 2e 69 Data Ascii: turn n}function x(e){var t={left:'right',right:'left',bottom:'top',top:'bottom'};return e.replace(/left|right|bottom|top/g,function(e){return t[e]})}function S(e,t,o){o=o.split('-')[0];var i=L(e),n={width:i.width,height:i.height},r=-1!==['right','left'].i

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	13	IN	Data Raw: 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2e 70 6f 73 69 74 69 6f 6e 3d 27 61 62 73 6f 6c 75 74 65 27 2c 65 3d 43 28 74 68 69 73 2e 6d 6f 64 69 66 69 65 72 73 2c 65 29 2c 74 68 69 73 2e 73 74 61 74 65 2e 69 73 43 72 65 61 74 65 64 3f 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 6e 55 70 64 61 74 65 28 65 29 3a 28 74 68 69 73 2e 73 74 61 74 65 2e 69 73 43 72 65 61 74 65 64 3d 21 30 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 6e 43 72 65 61 74 65 28 65 29 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 6b 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 65 2e 73 6f 6d 65 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 65 2e 6e 61 6d 65 2c 69 3d 65 2e 65 6e 61 62 6c 65 64 3b 72 65 74 75 72 6e 20 69 26 26 Data Ascii: ference,e.placement),e.offsets.popper.position='absolute',e=C(this.modifiers,e),this.state.isCreated?this.options.onUpdate(e):(this.state.isCreated=!0,this.options.onCreate(e))}}function k(e,t){return e.some(function(e){var o=e.name,i=e.enabled;return i&&
2021-12-03 00:03:49 UTC	14	IN	Data Raw: 65 74 75 72 6e 20 42 28 65 29 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 72 65 73 69 7a 65 27 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 29 2c 74 2e 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 73 63 72 6f 6c 6c 27 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 29 7d 29 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 3d 6e 75 6c 6c 2c 74 2e 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 3d 5b 5d 2c 74 2e 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 21 31 2c 74 7d 66 75 6e 63 74 69 6f 6e 20 52 28 29 7b 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 Data Ascii: eturn B(e).removeEventListener('resize',t.updateBound),t.scrollParents.forEach(function(e){e.removeEventListener('scroll',t.updateBound)}),t.updateBound=null,t.scrollParents=[],t.scrollElement=null,t.eventsEnabled=!1,t}function R(){this.state.eventsEnable
2021-12-03 00:03:49 UTC	15	IN	Data Raw: 7d 76 61 72 20 64 3d 63 28 73 29 3b 72 65 74 75 72 6e 20 64 5b 74 5d 2f 31 30 30 2a 72 7d 69 66 28 27 76 68 27 3d 3d 3d 70 7c 7c 27 76 77 27 3d 3d 3d 70 29 7b 76 61 72 20 61 3b 72 65 74 75 72 6e 20 61 3d 27 76 68 27 3d 3d 3d 70 3f 4a 28 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 63 6c 69 65 6e 74 48 65 69 67 68 74 2c 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 48 65 69 67 68 74 7c 7c 30 29 3a 4a 28 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 63 6c 69 65 6e 74 57 69 64 74 68 2c 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 57 69 64 74 68 7c 7c 30 29 2c 61 2f 31 30 30 2a 72 7d 72 65 74 75 72 6e 20 72 7d 66 75 6e 63 74 69 6f 6e 20 7a 28 65 2c 74 2c 6f 2c 69 29 7b 76 61 72 20 6e 3d 5b 30 2c 30 5d 2c 72 3d 2d 31 21 Data Ascii: }var d=c(s);return d[t]/100*r}if('vh'===p||'vw'===p){var a;return a='vh'===p?J(document.documentElement.clientHeight,window.innerHeight||0):J(document.documentElement.clientWidth,window.innerWidth||0),a/100*r}return r}function z(e,t,o,i){var n=[0,0],r=-1!
2021-12-03 00:03:49 UTC	17	IN	Data Raw: 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 64 6f 63 75 6d 65 6e 74 2c 5a 3d 5b 27 45 64 67 65 27 2c 27 54 72 69 64 65 6e 74 27 2c 27 46 69 72 65 66 6f 78 27 5d 2c 24 3d 30 2c 65 65 3d 30 3b 65 65 3c 5a 2e 6c 65 6e 67 74 68 3b 65 65 2b 3d 31 29 69 66 28 51 26 26 30 3c 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 5a 5b 65 65 5d 29 29 7b 24 3d 31 3b 62 72 65 61 6b 7d 76 61 72 20 69 2c 74 65 3d 51 26 26 77 69 6e 64 6f 77 2e 50 72 6f 6d 69 73 65 2c 6f 65 3d 74 65 3f 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 21 31 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 74 7c 7c 28 74 3d 21 30 2c 77 69 6e 64 6f 77 2e 50 72 6f 6d 69 73 65 2e 72 65 73 6f 6c 76 65 28 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e Data Ascii: ined'!=typeof document,Z=['Edge','Trident','Firefox'],$=0,ee=0;ee<Z.length;ee+=1)if(Q&&0<=navigator.userAgent.indexOf(Z[ee])){$=1;break}var i,te=Q&&window.Promise,oe=te?function(e){var t=!1;return function(){t||(t=!0,window.Promise.resolve().then(function
2021-12-03 00:03:49 UTC	18	IN	Data Raw: 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 3f 61 72 67 75 6d 65 6e 74 73 5b 32 5d 3a 7b 7d 3b 6e 65 28 74 68 69 73 2c 74 29 2c 74 68 69 73 2e 73 63 68 65 64 75 6c 65 55 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 72 65 71 75 65 73 74 41 6e 69 6d 61 74 69 6f 6e 46 72 61 6d 65 28 6e 2e 75 70 64 61 74 65 29 7d 2c 74 68 69 73 2e 75 70 64 61 74 65 3d 6f 65 28 74 68 69 73 2e 75 70 64 61 74 65 2e 62 69 6e 64 28 74 68 69 73 29 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 73 65 28 7b 7d 2c 74 2e 44 65 66 61 75 6c 74 73 2c 72 29 2c 74 68 69 73 2e 73 74 61 74 65 3d 7b 69 73 44 65 73 74 72 6f 79 65 64 3a 21 31 2c 69 73 43 72 65 61 74 65 64 3a 21 31 2c 73 63 72 6f 6c 50 61 72 Data Ascii: ments.length&&void 0!==arguments[2]?arguments[2]:{};ne(this,t),this.scheduleUpdate=function(){return requestAnimationFrame(n.update)},this.update=oe(this.update.bind(this)),this.options=se({},t.Defaults,r),this.state={isDestroyed:!1,isCreated:!1,scrollPar
2021-12-03 00:03:49 UTC	19	IN	Data Raw: 3a 7b 6f 72 64 65 72 3a 31 30 30 2c 65 6e 61 62 6c 65 64 3a 21 30 2c 66 6e 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2c 6f 3d 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 2c 69 3d 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 31 5d 3b 69 66 28 69 29 7b 76 61 72 20 6e 3d 65 2e 6f 66 66 73 65 74 73 2c 72 3d 6e 2e 72 65 66 65 72 65 6e 63 65 2c 70 3d 6e 2e 70 6f 70 70 65 72 2c 73 3d 2d 31 21 3d 3d 5b 27 62 6f 74 74 6f 6d 27 2c 27 74 6f 70 27 5d 2e 69 6e 64 65 78 4f 66 28 6f 29 2c 64 3d 73 3f 27 6c 65 66 74 27 3a 27 74 6f 70 27 2c 61 3d 73 3f 27 77 69 64 74 68 27 3a 27 68 65 69 67 68 74 27 2c 6c 3d 7b 73 74 61 72 74 3a 70 65 28 7b 7d 2c 64 2c 72 5b 64 5d 29 2c 65 6e 64 3a 70 65 28 7b 7d 2c 64 2c 72 5b 64 5d 2b 72 5b 61 Data Ascii: :{order:100,enabled:!0,fn:function(e){var t=e.placement,o=t.split('-')[0],i=t.split('-')[1];if(i){var n=e.offsets,r=n.reference,p=n.popper,s=-1!==['bottom','top'].indexOf(o),d=s?'left':'top',a=s?'width':'height',l={start:pe({},d,r[d]),end:pe({},d,r[d]+r[a
2021-12-03 00:03:49 UTC	21	IN	Data Raw: 26 28 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 64 5d 3d 72 28 69 5b 73 5d 29 29 2c 65 7d 7d 2c 61 72 72 6f 77 3a 7b 6f 72 64 65 72 3a 35 30 30 2c 65 6e 61 62 6c 65 64 3a 21 30 2c 66 6e 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 6f 29 7b 76 61 72 20 69 3b 69 66 28 21 46 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 69 65 72 73 2c 27 61 72 72 6f 77 27 2c 27 6b 65 65 70 54 6f 67 65 74 68 65 72 27 29 29 72 65 74 75 72 6e 20 65 3b 76 61 72 20 6e 3d 6f 2e 65 6c 65 6d 65 6e 74 3b 69 66 28 27 73 74 72 69 6e 67 27 3d 3d 74 79 70 65 6f 66 20 6e 29 7b 69 66 28 6e 3d 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 6e 29 2c 21 6e 29 72 65 74 75 72 6e 20 65 3b 7d 65 6c 73 65 20 69 66 28 21 65 2e 69 6e 73 74 61 6e Data Ascii: &(e.offsets.popper[d]=r(i[s])),e}},arrow:{order:500,enabled:!0,fn:function(e,o){var i;if(!F(e.instance.modifiers,'arrow','keepTogether'))return e;var n=o.element;if('string'==typeof n){if(n=e.instance.popper.querySelector(n),!n)return e;}else if(!e.instan
2021-12-03 00:03:49 UTC	22	IN	Data Raw: 53 45 3a 70 3d 71 28 69 2c 21 30 29 3b 62 72 65 61 6b 3b 64 65 66 61 75 6c 74 3a 70 3d 74 2e 62 65 68 61 76 69 6f 72 3b 7d 72 65 74 75 72 6e 20 70 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 73 2c 64 29 7b 69 66 28 69 21 3d 3d 73 7c 7c 70 2e 6c 65 6e 67 74 68 3d 3d 3d 64 2b 31 29 72 65 74 75 72 6e 20 65 3b 69 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 2c 6e 3d 78 28 69 29 3b 76 61 72 20 61 3d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 6c 3d 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 66 3d 58 2c 6d 3d 27 6c 65 66 74 27 3d 3d 3d 69 26 26 28 61 2e 72 69 67 68 74 29 3e 6e 26 26 28 61 2e 6c 65 66 74 29 3c 6e 28 6c 2e 72 69 Data Ascii: SE:p=q(i,!0);break;default:p=t.behavior;}return p.forEach(function(s,d){if(i!==s||p.length===d+1)return e;i=e.placement.split('-')[0],n=x(i);var a=e.offsets.popper,l=e.offsets.reference,f=X,m='left'===i&&f(a.right)>f(l.left)||'right'===i&&f(a.left)<f(l.ri

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	23	IN	Data Raw: 2e 6e 61 6d 65 7d 29 2e 62 6f 75 6e 64 61 72 69 65 73 3b 69 66 28 74 2e 62 6f 74 74 6f 6d 3c 6f 2e 74 6f 70 7c 7c 74 2e 6c 65 66 74 3e 6f 2e 72 69 67 68 74 7c 7c 74 2e 74 6f 70 3e 6f 2e 62 6f 74 74 6f 6d 7c 7c 74 2e 72 69 67 68 74 3c 6f 2e 6c 65 66 74 29 7b 69 66 28 21 30 3d 3d 3d 65 2e 68 69 64 65 29 72 65 74 75 72 6e 20 65 3b 65 2e 68 69 64 65 3d 21 30 2c 65 2e 61 74 74 72 69 62 75 74 65 73 5b 27 78 2d 6f 75 74 2d 6f 66 2d 62 6f 75 6e 64 61 72 69 65 73 27 5d 3d 27 27 7d 65 6c 73 65 7b 69 66 28 21 31 3d 3d 3d 65 2e 68 69 64 65 29 72 65 74 75 72 6e 20 65 3b 65 2e 68 69 64 65 3d 21 31 2c 65 2e 61 74 74 72 69 62 75 74 65 73 5b 27 78 2d 6f 75 74 2d 6f 66 2d 62 6f 75 6e 64 61 72 69 65 73 27 5d 3d 21 31 7d 72 65 74 75 72 6e 20 65 7d 7d 2c 63 6f 6d 70 75 74 65 Data Ascii: .name}).boundaries;if(t.bottom<o.top||t.left>o.right||t.top>o.bottom||t.right<o.left){if(!0===e.hide)return e;e.hide=!0,e.attributes['x-out-of-boundaries']=''}else{if(!1===e.hide)return e;e.hide=!1,e.attributes['x-out-of-boundaries']=!1}return e}}, compute
2021-12-03 00:03:49 UTC	25	IN	Data Raw: 69 62 75 74 65 73 29 2c 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 26 26 4f 62 6a 65 63 74 2e 6b 65 79 73 28 65 2e 61 72 72 6f 77 53 74 79 6c 65 73 29 2e 6c 65 6e 67 74 68 26 26 59 28 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 2c 65 2e 61 72 72 6f 77 53 74 79 6c 65 73 29 2c 65 7d 2c 6f 6e 4c 6f 61 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 2c 69 2c 6e 29 7b 76 61 72 20 72 3d 4f 28 6e 2c 74 2c 65 29 2c 70 3d 76 28 6f 2e 70 6c 61 63 65 6d 65 6e 74 2c 72 2c 74 2c 65 2c 6f 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6c 69 70 2e 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 2c 6f 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6c 69 70 2e 70 61 64 64 69 6e 67 29 3b 72 65 74 75 72 6e 20 74 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 27 78 2d 70 6c 61 63 65 6d 65 6e 74 27 2c Data Ascii: ibutes),e.arrowElement&&Object.keys(e.arrowStyles).length&&Y(e.arrowElement,e.arrowStyles),e},onLoad:function(e,t,o,i,n){var r=O(n,t,e),p=v(o.placement,r,t,e,o.modifiers.flip.boundariesElement,o.modifiers.flip.padding);return t.setAttribute('x-placement',
2021-12-03 00:03:49 UTC	25	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49746	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	5	OUT	GET /bootstrap/4.0.0/js/bootstrap.min.js HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-12-03 00:03:49 UTC	25	IN	HTTP/1.1 200 OK Date: Fri, 03 Dec 2021 00:03:49 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 Last-Modified: Mon, 25 Jan 2021 22:04:04 GMT CDN-CachedAt: 08/04/2021 00:04:37 CDN-EdgeStorageId: 601 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-ProxyVer: 1.0 CDN-Status: 200 CDN-RequestId: 12f24fb6bb63b28e0a69ad6a09c5937e CDN-Cache: HIT CF-Cache-Status: HIT Age: 8719822 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 6b7888b83c46073e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-12-03 00:03:49 UTC	26	IN	Data Raw: 34 32 38 66 0d 0a 2f 2a 21 0a 20 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 30 2e 30 20 28 68 74 74 70 73 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 67 72 61 70 68 73 2f 63 6f 6e 74 72 69 62 75 74 6f 72 73 29 0a 20 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 4d 49 54 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 4c 49 43 45 4e 53 45 29 0a 20 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 74 Data Ascii: 428f/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors) * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */!function(t

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	26	IN	Data Raw: 21 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 3f 65 28 65 78 70 6f 72 74 73 2c 72 65 71 75 69 72 65 28 22 6a 71 75 65 72 79 22 29 2c 72 65 71 75 69 72 65 28 22 70 6f 70 70 65 72 2e 6a 73 22 29 29 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 5b 22 65 78 70 6f 72 74 73 22 2c 22 6a 71 75 65 72 79 22 2c 22 70 6f 70 70 65 72 2e 6a 73 22 5d 2c 65 29 3a 65 28 74 2e 62 6f 6f 74 73 74 72 61 70 3d 7b 7d 2c 74 2e 6a 51 75 65 72 79 2c 74 2e 50 6f 70 70 65 72 29 7d 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 69 28 74 2c 65 29 7b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 65 2e 6c 65 6e 67 74 Data Ascii: !=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?defi ne(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.lengt
2021-12-03 00:03:49 UTC	28	IN	Data Raw: 64 28 69 29 2e 6c 65 6e 67 74 68 3e 30 3f 69 3a 6e 75 6c 6c 7d 63 61 74 63 68 28 74 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 7d 2c 72 65 66 6c 6f 77 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 74 2e 6f 66 66 73 65 74 48 65 69 67 68 74 7d 2c 74 72 69 67 67 65 72 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 74 28 6e 29 2e 74 72 69 67 67 65 72 28 65 2e 65 6e 64 29 7d 2c 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 42 6f 6f 6c 65 61 6e 28 65 29 7d 2c 69 73 45 6c 65 6d 65 6e 74 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 28 74 5b 30 5d 7c 7c 74 29 2e 6e 6f 64 65 54 79 70 65 7d 2c 74 79 70 65 43 68 65 63 6b 43 6f 6e 66 69 67 Data Ascii: d(i).length>0?i:null}catch(t){return null}},reflow:function(t){return t.offsetHeight},triggerTransitionEnd:function(n) {t(n).trigger(e.end)},supportsTransitionEnd:function(){return Boolean(e)},isElement:function(t){return(t[0]||t).nodeType },typeCheckConfig
2021-12-03 00:03:49 UTC	29	IN	Data Raw: 45 6c 65 6d 65 6e 74 28 74 29 2c 6e 3d 21 31 3b 72 65 74 75 72 6e 20 65 26 26 28 6e 3d 6f 28 65 29 5b 30 5d 29 2c 6e 7c 28 6e 3d 6f 28 74 29 2e 63 6c 6f 73 65 73 74 28 22 2e 22 2b 66 29 5b 30 5d 29 2c 6e 7d 2c 65 2e 5f 74 72 69 67 67 65 72 43 6c 6f 73 65 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 6f 2e 45 76 65 6e 74 28 75 2e 43 4c 4f 53 45 29 3b 72 65 74 75 72 6e 20 6f 28 74 29 2e 74 72 69 67 67 65 72 28 65 29 2c 65 7d 2c 65 2e 5f 72 65 6d 6f 76 65 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 6f 28 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 29 2c 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 6f 28 74 29 2e 68 61 73 43 6c 61 73 73 28 64 Data Ascii: Element(t),n=!1;return e&&(n=o(e)[0]),n||(n=o(t).closest("."+f)[0]),n},e._triggerCloseEvent=function(t){var e=o.Event(u.CLOSE);return o(t).trigger(e),e},e._removeElement=function(t){var e=this;o(t).removeClass(_),P.sup portsTransitionEnd()&&o(t).hasClass(d
2021-12-03 00:03:49 UTC	30	IN	Data Raw: 5b 30 5d 3b 69 66 28 69 29 7b 69 66 28 22 72 61 64 69 6f 22 3d 3d 3d 69 2e 74 79 70 65 29 69 66 28 69 2e 63 68 65 63 6b 65 64 26 26 70 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 43 29 29 74 3b 7d 69 66 28 69 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 43 29 7d 69 66 28 74 29 7b 69 66 28 69 2e 68 61 73 41 74 74 72 69 62 75 74 65 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 69 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 6e 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 6e 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 6e 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c Data Ascii: [0];if(i){if("radio"===i.type)if(i.checked&&p(this._element).hasClass(C))t=!1;else{var s=p(n).find(w)[0];s&& p(s).removeClass(C)}if(t){if(i.hasAttribute("disabled")||n.hasAttribute("disabled")||i.classList.contains("disabled")||n.classList .contains("disabl
2021-12-03 00:03:49 UTC	32	IN	Data Raw: 61 6e 22 7d 2c 68 3d 22 6e 65 78 74 22 2c 63 3d 22 70 72 65 76 22 2c 75 3d 22 6c 65 66 74 22 2c 66 3d 22 72 69 67 68 74 22 2c 64 3d 7b 53 4c 49 44 45 3a 22 73 6c 69 64 65 22 2b 69 2c 53 4c 49 44 3a 22 73 6c 69 64 22 2b 69 2c 4b 45 59 44 4f 57 4e 3a 22 6b 65 79 64 6f 77 6e 22 2b 69 2c 4d 4f 55 53 45 45 4e 54 45 52 3a 22 6d 6f 75 73 65 65 6e 74 65 72 22 2b 69 2c 4d 4f 55 53 45 4c 45 41 56 45 3a 22 6d 6f 75 73 65 6c 65 61 76 65 22 2b 69 2c 54 4f 55 43 48 45 4e 44 3a 22 74 6f 75 63 68 65 6e 64 22 2b 69 2c 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 3a 22 6c 6f 61 64 22 2b 69 2b 22 2e 64 61 74 61 2d 61 70 69 22 2c 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 3a 22 63 6c 69 63 6b 22 2b 69 2b 22 2e 64 61 74 61 2d 61 70 69 22 7d 2c 5f 3d 22 63 61 72 6f 75 73 65 6c 22 2c Data Ascii: an"},h="next",c="prev",u="left",f="right",d={SLIDE:"slide"+i,SLID:"slid"+i,KEYDOWN:"keydown"+i,MOU SEENTER:"mouseenter"+i,MOUSELEAVE:"mouseleave"+i,TOUCHEND:"touchend"+i,LOAD_DATA_API:"load"+i+".data-api",CLICK_DATA_API:"click"+i+".data-api"},_="carousel",
2021-12-03 00:03:49 UTC	33	IN	Data Raw: 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 7d 2c 43 2e 63 79 63 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 7c 7c 28 74 68 69 73 2e 5f 69 73 50 61 75 73 65 64 3d 21 31 29 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 26 26 28 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 29 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 29 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 69 6e 74 65 72 76 61 6c 26 26 21 74 68 69 73 2e 5f 69 73 50 61 75 73 65 64 26 26 28 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 73 65 74 49 6e 74 65 72 76 61 6c 28 28 64 6f 63 75 6d 65 6e 74 2e 76 69 73 69 62 69 6c 69 74 79 53 74 61 74 65 3f 74 68 69 73 2e 6e 65 78 74 57 68 65 6e 56 69 73 69 62 6c 65 3a 74 68 69 73 2e 6e 65 78 74 Data Ascii: his._interval=null},C.cycle=function(t){t||(this._isPaused=!1),this._interval&&(clearInterval(this._interval),this._in terval=null),this._config.interval&&!this._isPaused&&(this._interval=setInterval((document.visibilityState?this.nextWhen Visible:this.next
2021-12-03 00:03:49 UTC	34	IN	Data Raw: 6f 75 63 68 54 69 6d 65 6f 75 74 3d 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 2e 63 79 63 6c 65 28 74 29 7d 2c 35 30 30 2b 65 2e 5f 63 6f 6e 66 69 67 2e 69 6e 74 65 72 76 61 6c 29 7d 29 7d 2c 43 2e 5f 6b 65 79 64 6f 77 6e 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 21 2f 69 6e 70 75 74 7c 74 65 78 74 61 72 65 61 2f 69 2e 74 65 73 74 28 74 2e 74 61 72 67 65 74 2e 74 61 67 4e 61 6d 65 29 29 73 77 69 74 63 68 28 74 2e 77 68 69 63 68 29 7b 63 61 73 65 20 33 37 3a 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 74 68 69 73 2e 70 72 65 76 28 29 3b 62 72 65 61 6b 3b 63 61 73 65 20 33 39 3a 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 74 68 69 73 2e 6e 65 78 74 28 29 7d 7d 2c 43 2e 5f Data Ascii: ouchTimeout=setTimeout(function(t){return e.cycle(t)},500+e._config.interval)})},C._keydown=function(t){if(!/input|textarea/i.test(t.target.tagName))switch(t.which){case 37:t.preventDefault(),this.prev();break;case 39:t.prevent Default(),this.next()}},C._
2021-12-03 00:03:49 UTC	36	IN	Data Raw: 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 26 26 61 26 26 63 29 7b 74 68 69 73 2e 5f 69 73 53 6c 69 64 69 6e 67 3d 21 30 2c 43 26 26 74 68 69 73 2e 70 61 75 73 65 28 29 2c 74 68 69 73 2e 5f 73 65 74 41 63 74 69 76 65 49 6e 64 69 63 61 74 6f 72 45 6c 65 6d 65 6e 74 28 63 29 3b 76 61 72 20 49 3d 74 2e 45 76 65 6e 74 28 64 2e 53 4c 49 44 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 63 2c 64 69 72 65 63 74 69 6f 6e 3a 72 2c 66 72 6f 6d 3a 6c 2c 74 6f 3a 5f 7d 29 3b 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 70 29 3f 28 74 28 63 29 2e 61 64 64 43 6c 61 73 73 28 73 29 2c 50 2e 72 65 66 6c 6f 77 28 63 29 2c 74 28 61 29 2e 61 64 64 43 6c Data Ascii: efaultPrevented()&&a&&c){this._isSliding=!0,C&&this.pause(),this._setActiveIndicatorElement(c);var I=t.Event (d.SLID,{relatedTarget:c,direction:r,from:l,to:_});P.supportsTransitionEnd()&&t(this._element).hasClass(p)?(t(c).addClas s(s),P.reflow(c),t(a).addCl

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	37	IN	Data Raw: 61 7d 7d 5d 29 2c 6f 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 64 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 79 2e 44 41 54 41 5f 53 4c 49 44 45 2c 43 2e 5f 64 61 74 61 41 70 69 43 6c 69 63 6b 48 61 6e 64 6c 65 72 29 2c 74 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 64 2e 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 79 2e 44 41 54 41 5f 52 49 44 45 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 28 74 68 69 73 29 3b 43 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 65 2c 65 2e 64 61 74 61 28 29 29 7d 29 7d 29 2c 74 2e 66 6e 5b 65 5d 3d 43 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 5b 65 5d 2e 43 6f 6e 73 74 72 75 63 Data Ascii: a}}]),o}();return t(document).on(d.CLICK_DATA_API,y.DATA_SLIDE,C._dataApiClickHandler),t(window).o n(d.LOAD_DATA_API,function(){t(y.DATA_RIDE).each(function(){var e=t(this);C._jQueryInterface.call(e,e.data())})}),t.fn[e]=C._jQueryInterface,t.fn[e].Construc
2021-12-03 00:03:49 UTC	38	IN	Data Raw: 74 68 69 73 2e 68 69 64 65 28 29 3a 74 68 69 73 2e 73 68 6f 77 28 29 7d 2c 6f 2e 73 68 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 2c 73 2c 72 3d 74 68 69 73 3b 69 66 28 21 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 26 26 21 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 63 29 26 26 28 74 68 69 73 2e 5f 70 61 72 65 6e 74 26 26 30 3d 3d 3d 28 65 3d 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 74 68 69 73 2e 5f 70 61 72 65 6e 74 29 2e 66 69 6e 64 28 70 2e 41 43 54 49 56 45 53 29 2e 66 69 6c 74 65 72 28 27 5b 64 61 74 61 2d 70 61 72 65 6e 74 3d 22 27 2b 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 70 61 72 65 6e 74 2b 27 22 5d 27 29 29 29 2e 6c 65 6e 67 74 68 26 26 28 65 3d 6e 75 6c 6c 29 2c 21 28 65 26 Data Ascii: this.hide():this.show()},o.show=function(){var e,s,r=this;if(!this._isTransitioning&&!t(this._element).hasCl ass(c)&&(this._parent&&0===(e=t.makeArray(t(this._parent).find(p.ACTIVES).filter('[data-parent="'+this._config.parent+'" ']))).length&&(e=null),!(e&
2021-12-03 00:03:49 UTC	40	IN	Data Raw: 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 63 29 2c 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 2e 6c 65 6e 67 74 68 3e 30 29 66 6f 72 28 76 61 72 20 73 3d 30 3b 73 3c 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 2e 6c 65 6e 67 74 68 3b 73 2b 2b 29 7b 76 61 72 20 72 3d 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 5b 73 5d 2c 6f 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 72 29 3b 69 66 28 6e 75 6c 6c 21 3d 3d 6f 29 74 28 6f 29 2e 68 61 73 43 6c 61 73 73 28 63 29 7c 7c 74 28 72 29 2e 61 64 64 43 6c 61 73 73 28 64 29 2e 61 74 74 72 28 22 61 72 69 61 2d 65 78 70 61 6e 64 65 64 22 2c 21 31 29 7d 74 68 69 73 2e 73 65 74 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 28 21 30 29 3b 76 61 72 20 61 3d 66 75 6e 63 Data Ascii: .removeClass(c),this._triggerArray.length>0)for(var s=0;s<this._triggerArray.length;s++){var r=this._trigger Array[s],o=P.getSelectorFromElement(r);if(null!==o)t(o).hasClass(c)||t(r).addClass(d).attr("aria-expanded",!1)}this.setT ransitioning(!0);var a=func
2021-12-03 00:03:49 UTC	41	IN	Data Raw: 72 67 65 74 46 72 6f 6d 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6e 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 65 29 3b 72 65 74 75 72 6e 20 6e 3f 74 28 6e 29 5b 30 5d 3a 6e 75 6c 6c 7d 2c 69 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 73 3d 74 28 74 68 69 73 29 2c 6f 3d 73 2e 64 61 74 61 28 6e 29 2c 6c 3d 72 28 7b 7d 2c 61 2c 73 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 29 3b 69 66 28 21 6f 26 26 6c 2e 74 6f 67 67 6c 65 26 26 2f 73 68 6f 77 7c 68 69 64 65 2f 2e 74 65 73 74 28 65 29 26 26 28 6c 2e 74 6f 67 Data Ascii: rgetFromElement=function(e){var n=P.getSelectorFromElement(e);return n?t(n)[0]:null},i._jQueryInterface=func tion(e){return this.each(function(){var s=t(this),o=s.data(n),l=r({},a,s.data(),"object"==typeof e&&e);if(!o&&l.toggle&& /show|hide/.test(e)&&(l.tog
2021-12-03 00:03:49 UTC	42	IN	Data Raw: 49 3d 22 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 20 2e 64 72 6f 70 64 6f 77 6e 2d 69 74 65 6d 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 22 2c 41 3d 22 74 6f 70 2d 73 74 61 72 74 22 2c 62 3d 22 74 6f 70 2d 65 6e 64 22 2c 44 3d 22 62 6f 74 74 6f 6d 2d 73 74 61 72 74 22 2c 53 3d 22 62 6f 74 74 6f 6d 2d 65 6e 64 22 2c 77 3d 22 72 69 67 68 74 2d 73 74 61 72 74 22 2c 4e 3d 22 6c 65 66 74 2d 73 74 61 72 74 22 2c 4f 3d 7b 6f 66 66 73 65 74 3a 30 2c 66 6c 69 70 3a 21 30 2c 62 6f 75 6e 64 61 72 79 3a 22 73 63 72 6f 6c 6c 50 61 72 65 6e 74 22 7d 2c 6b 3d 7b 6f 66 66 73 65 74 3a 22 28 6e 75 6d 62 65 72 7c 73 74 72 69 6e 67 7c 66 75 6e 63 74 69 6f 6e 29 22 2c 66 6c 69 70 3a 22 62 6f 6f 6c 65 61 6e 22 2c 62 6f 75 6e 64 61 72 79 3a 22 28 73 74 72 69 6e 67 7c 65 6c Data Ascii: I=".dropdown-menu .dropdown-item:not(.disabled)",A="top-start",b="top-end",D="bottom-start",S="bottom- end",w="right-start",N="left-start",O={offset:0,flip:!0,boundary:"scrollParent"},k={offset:"(number|string|function)",flip:"bo olean",boundary:"(string|el
2021-12-03 00:03:49 UTC	43	IN	Data Raw: 37 63 61 31 0d 0a 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 66 69 67 28 65 29 2c 74 68 69 73 2e 5f 6d 65 6e 75 3d 74 68 69 73 2e 5f 67 65 74 4d 65 6e 75 45 6c 65 6d 65 6e 74 28 29 2c 74 68 69 73 2e 5f 69 6e 4e 61 76 62 61 72 3d 74 68 69 73 2e 5f 64 65 74 65 63 74 4e 61 76 62 61 72 28 29 2c 74 68 69 73 2e 5f 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 73 28 29 7d 76 61 72 20 6c 3d 61 2e 70 72 6f 74 6f 74 79 70 65 3b 72 65 74 75 72 6e 20 6c 2e 74 6f 67 67 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 21 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 64 69 73 61 62 6c 65 64 26 26 21 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 75 29 29 7b 76 61 72 20 65 3d 61 2e 5f 67 65 Data Ascii: 7ca1=null,this._config=this._getConfig(e),this._menu=this._getMenuElement(),this._inNavbar=this._d etectNavbar(),this._addEventListeners()}var l=a.prototype;return l.toggle=function(){if(!this._element.disabled&&!t(this ._element).hasClass(u)){var e=a._ge
2021-12-03 00:03:49 UTC	44	IN	Data Raw: 61 72 20 65 3d 74 68 69 73 3b 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 63 2e 43 4c 49 43 4b 2c 66 75 6e 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 74 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 2c 65 2e 74 6f 67 67 6c 65 28 29 7d 29 7d 2c 6c 2e 5f 67 65 74 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 72 65 74 75 72 6e 20 6e 3d 72 28 7b 7d 2c 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 65 66 61 75 6c 74 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 64 61 74 61 28 29 2c 6e 29 2c 50 2e 74 79 70 65 43 68 65 63 6b 43 6f 6e 66 69 67 28 65 2c 6e 2c 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 65 66 61 75 6c 74 54 79 70 65 29 2c 6e 7d 2c 6c 2e 5f 67 65 74 Data Ascii: ar e=this;t(this._element).on(c.CLICK,function(t){t.preventDefault(),t.stopPropagation(),e.toggle()})},l._ge tConfig=function(n){return n=r({},this.constructor.Default,t(this._element).data(),n),P.typeCheckConfig(e,n,this.constru ctor.DefaultType),n},l._get
2021-12-03 00:03:49 UTC	45	IN	Data Raw: 2c 73 3d 30 3b 73 3c 6e 2e 6c 65 6e 67 74 68 3b 73 2b 2b 29 7b 76 61 72 20 72 3d 61 2e 5f 67 65 74 50 61 72 65 6e 74 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 6e 5b 73 5d 29 2c 6f 3d 74 28 6e 5b 73 5d 29 2e 64 61 74 61 28 69 29 2c 6c 3d 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 6e 5b 73 5d 7d 3b 69 66 28 6f 29 7b 76 61 72 20 68 3d 6f 2e 5f 6d 65 6e 75 3b 69 66 28 74 28 72 29 2e 68 61 73 43 6c 61 73 73 28 66 29 26 26 21 28 65 26 26 28 22 63 6c 69 63 6b 22 3d 3d 65 2e 74 79 70 65 26 26 2f 69 6e 70 75 74 7c 74 65 78 74 61 72 65 61 2f 69 2e 74 65 73 74 28 65 2e 74 61 72 67 65 74 2e 74 61 67 4e 61 6d 65 29 7c 7c 22 6b 65 79 75 70 22 3d 3d 65 2e 74 79 70 65 26 26 39 3d 3d 65 2e 77 68 69 63 68 29 26 26 74 2e 63 6f 6e 74 61 69 6e 73 28 72 2c 65 2e 74 61 72 Data Ascii: ,s=0;s<n.length;s++){var r=a._getParentFromElement(n[s]),o=t(n[s]).data(i),l={relatedTarget:n[s]};if(o){var h=o._menu;if(t(r).hasClass(f)&&!(e&&("click"===e.type&&/input|textarea/i.test(e.target.tagName)||"keyup"===e.t ype&&9===e.which)&&t.contains(r,e.tar

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	47	IN	Data Raw: 29 7b 72 65 74 75 72 6e 20 4f 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 54 79 70 65 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6b 7d 7d 5d 29 2c 61 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 63 2e 4b 45 59 44 4f 57 4e 5f 44 41 54 41 5f 41 50 49 2c 45 2c 4c 2e 5f 64 61 74 61 41 70 69 4b 65 79 64 6f 77 6e 48 61 6e 64 6c 65 72 29 2e 6f 6e 28 63 2e 4b 45 59 44 4f 57 4e 5f 44 41 54 41 5f 41 50 49 2c 79 2c 4c 2e 5f 64 61 74 61 41 70 69 4b 65 79 64 6f 77 6e 48 61 6e 64 6c 65 72 29 2e 6f 6e 28 63 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2b 22 20 22 2b 63 2e 4b 45 59 55 50 5f 44 41 54 41 5f 41 50 49 2c 4c 2e 5f 63 6c 65 61 72 4d 65 6e 75 73 29 2e 6f 6e 28 63 2e 43 4c 49 43 4b 5f 44 41 54 41 Data Ascii:){return O}},{key:"DefaultType",get:function(){return k}}]),a}();return t(document).on(c.KEYDOWN_DATA_API,E,L._dataApiKeydownHandler).on(c.KEYDOWN_DATA_API,y,L._dataApiKeydownHandler).on(c.CLICK_DATA_API+" "+c.KEYUP_DATA_API,L._clearMenus).on(c.CLICK_DATA
2021-12-03 00:03:49 UTC	48	IN	Data Raw: 43 6f 6e 66 69 67 28 6e 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 65 2c 74 68 69 73 2e 5f 64 69 61 6c 6f 67 3d 74 28 65 29 2e 66 69 6e 64 28 67 2e 44 49 41 4c 4f 47 29 5b 30 5d 2c 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 3d 21 31 2c 74 68 69 73 2e 5f 69 73 42 6f 64 79 4f 76 65 72 66 6c 6f 77 69 6e 67 3d 21 31 2c 74 68 69 73 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3d 21 31 2c 74 68 69 73 2e 5f 6f 72 69 67 69 6e 61 6c 42 6f 64 79 50 61 64 64 69 6e 67 3d 30 2c 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 3d 30 7d 76 61 72 20 70 3d 6f 2e 70 72 6f 74 6f 74 79 70 65 3b 72 65 74 75 72 6e 20 70 2e 74 6f 67 67 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 Data Ascii: Config(n),this._element=e,this._dialog=t(e).find(g.DIALOG)[0],this._backdrop=null,this._isShown=!1,this._isBodyOverflowing=!1,this._ignoreBackdropClick=!1,this._originalBodyPadding=0,this._scrollbarWidth=0}var p=o.prototype;return p.toggle=function(t){ret
2021-12-03 00:03:49 UTC	49	IN	Data Raw: 6d 65 6e 74 29 2e 6f 66 66 28 68 2e 46 4f 43 55 53 49 4e 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 68 2e 43 4c 49 43 4b 5f 44 49 53 4d 49 53 53 29 2c 74 28 74 68 69 73 2e 5f 64 69 61 6c 6f 67 29 2e 6f 66 66 28 68 2e 4d 4f 55 53 45 44 4f 57 4e 5f 44 49 53 4d 49 53 53 29 2c 73 3f 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 6e 2e 5f 68 69 64 65 4d 6f 64 61 6c 28 74 29 7d 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 33 30 30 29 3a 74 68 69 73 2e 5f 68 69 64 65 4d 6f 64 61 6c 28 29 7d 7d 7d Data Ascii: ment).off(h.FOCUSIN),t(this._element).removeClass(_),t(this._element).off(h.CLICK_DISMISS),t(this._dialog).off(h.MOUSEDOWN_DISMISS),s?t(this._element).one(P.TRANSITION_END,function(t){return n._hideModal(t)}).emulateTransitionEnd(300):this._hideModal()}}}
2021-12-03 00:03:49 UTC	51	IN	Data Raw: 55 53 49 4e 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 64 6f 63 75 6d 65 6e 74 21 3d 3d 6e 2e 74 61 72 67 65 74 26 26 65 2e 5f 65 6c 65 6d 65 6e 74 21 3d 3d 6e 2e 74 61 72 67 65 74 26 26 30 3d 3d 3d 74 28 65 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 28 6e 2e 74 61 72 67 65 74 29 2e 6c 65 6e 67 74 68 26 26 65 2e 5f 65 6c 65 6d 65 6e 74 2e 66 6f 63 75 73 28 29 7d 29 7d 2c 70 2e 5f 73 65 74 45 73 63 61 70 65 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 26 26 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6b 65 79 62 6f 61 72 64 3f 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 68 2e 4b 45 59 44 4f 57 4e 5f 44 49 53 4d 49 53 53 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 32 37 3d 3d 3d Data Ascii: USIN,function(n){document!==n.target&&e._element!==n.target&&0===t(e._element).has(n.target).length&&e._element.focus()})},p._setEscapeEvent=function(){var e=this;this._isShown&&this._config.keyboard?t(this._element).on(h.KEYDOWN_DISMISS,function(t){27===
2021-12-03 00:03:49 UTC	52	IN	Data Raw: 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2c 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 61 64 64 43 6c 61 73 73 28 5f 29 2c 21 65 29 72 65 74 75 72 6e 3b 69 66 28 21 73 29 72 65 74 75 72 6e 20 76 6f 69 64 20 65 28 29 3b 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 65 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 31 35 30 29 7d 65 6c 73 65 20 69 66 28 21 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 26 26 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 7b 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 29 3b 76 61 72 20 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 2e 5f 72 65 6d 6f 76 65 42 61 63 6b 64 72 6f 70 28 29 2c 65 26 Data Ascii: s._backdrop),t(this._backdrop).addClass(_),!e)return;if(!s)return void e();t(this._backdrop).one(P.TRANSITION_END,e).emulateTransitionEnd(150)}else if(!this._isShown&&this._backdrop){t(this._backdrop).removeClass(_);var r=function(){n._removeBackdrop(),e&
2021-12-03 00:03:49 UTC	53	IN	Data Raw: 74 28 72 29 2d 65 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 2b 22 70 78 22 29 7d 29 2c 74 28 67 2e 4e 41 56 42 41 52 5f 54 4f 47 47 4c 45 52 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 69 29 7b 76 61 72 20 73 3d 74 28 69 29 5b 30 5d 2e 73 74 79 6c 65 2e 6d 61 72 67 69 6e 52 69 67 68 74 2c 72 3d 74 28 69 29 2e 63 73 73 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 29 3b 74 28 69 29 2e 64 61 74 61 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 2c 73 29 2e 63 73 73 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 2c 70 61 72 73 65 46 6c 6f 61 74 28 72 29 2b 65 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 2b 22 70 78 22 29 7d 29 3b 76 61 72 20 6e 3d 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 73 74 79 6c 65 2e 70 61 64 64 69 6e 67 52 69 67 68 74 2c Data Ascii: t(r)-e._scrollbarWidth+"px")}),t(g.NAVBAR_TOGGLER).each(function(n,i){var s=t(i)[0].style.marginRight,r=t(i).css("margin-right");t(i).data("margin-right",s).css("margin-right",parseFloat(r)+e._scrollbarWidth+"px")});var n=document.body.style.paddingRight,
2021-12-03 00:03:49 UTC	55	IN	Data Raw: 29 7d 2c 73 28 6f 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 30 2e 30 22 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 7d 7d 5d 29 2c 6f 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 68 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 67 2e 44 41 54 41 5f 54 4f 47 47 4c 45 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 69 2c 73 3d 74 68 69 73 2c 6f 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 74 68 69 73 29 3b 6f 26 26 28 69 3d 74 28 6f 29 5b 30 5d 29 3b 76 61 72 20 61 3d 74 28 69 29 2e 64 61 74 61 28 6e 29 3f 22 74 6f Data Ascii:)},s(o,null,[{key:"VERSION",get:function(){return"4.0.0"}},{key:"Default",get:function(){return a}}]),o}();return t(document).on(h.CLICK_DATA_API,g.DATA_TOGGLE,function(e){var i,s=this,o=P.getSelectorFromElement(this);o&&(i=t(o)[0]);var a=t(i).data(n)?"to
2021-12-03 00:03:49 UTC	56	IN	Data Raw: 50 6c 61 63 65 6d 65 6e 74 3a 22 66 6c 69 70 22 2c 62 6f 75 6e 64 61 72 79 3a 22 73 63 72 6f 6c 6c 50 61 72 65 6e 74 22 7d 2c 66 3d 22 73 68 6f 77 22 2c 64 3d 22 6f 75 74 22 2c 5f 3d 7b 48 49 44 45 3a 22 68 69 64 65 22 2b 6f 2c 48 49 44 44 45 4e 3a 22 68 69 64 64 65 6e 22 2b 6f 2c 53 48 4f 57 3a 22 73 68 6f 77 22 2b 6f 2c 53 48 4f 57 4e 3a 22 73 68 6f 77 6e 22 2b 6f 2c 49 4e 53 45 52 54 45 44 3a 22 69 6e 73 65 72 74 65 64 22 2b 6f 2c 43 4c 49 43 4b 3a 22 63 6c 69 63 6b 22 2b 6f 2c 46 4f 43 55 53 49 4e 3a 22 66 6f 63 75 73 69 6e 22 2b 6f 2c 46 4f 43 55 53 4f 55 54 3a 22 66 6f 63 75 73 6f 75 74 22 2b 6f 2c 4d 4f 55 53 45 45 4e 54 45 52 3a 22 6d 6f 75 73 65 65 6e 74 65 72 22 2b 6f 2c 4d 4f 55 53 45 4c 45 41 56 45 3a 22 6d 6f 75 73 65 6c 65 61 76 65 22 2b 6f Data Ascii: Placement:"flip",boundary:"scrollParent"},f="show",d="out",_={HIDE:"hide"+o,HIDDEN:"hidden"+o,SHOW:"show"+o,SHOWN:"shown"+o,INSERTED:"inserted"+o,CLICK:"click"+o,FOCUSIN:"focusin"+o,FOCUSOUT:"focusout"+o,MOUSEENTER:"mouseenter"+o,MOUSELEAVE:"mouseleave"+o

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	58	IN	Data Raw: 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 56 45 4e 54 5f 4b 45 59 29 2c 74 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 2e 63 6c 6f 73 65 73 74 28 22 2e 6d 6f 64 61 6c 22 29 2e 6f 66 66 28 22 68 69 64 65 2e 62 73 2e 6d 6f 64 61 6c 22 29 2c 74 68 69 73 2e 74 69 70 26 26 74 28 74 68 69 73 2e 74 69 70 29 2e 72 65 6d 6f 76 65 28 29 2c 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 74 69 6d 65 6f 75 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 68 6f 76 65 72 53 74 61 74 65 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 3d 6e 75 6c 6c 2c 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 74 68 69 73 2e 5f 70 6f 70 70 65 72 2e 64 65 73 74 72 6f 79 28 29 2c 74 68 69 73 2e 5f 70 6f 70 70 65 72 Data Ascii: is.constructor.EVENT_KEY),t(this.element).closest(".modal").off("hide.bs.modal"),this.tip&&t(this.tip).remov e(),this._isEnabled=null,this._timeout=null,this._hoverState=null,this._activeTrigger=null,null!==this._popper&&this._po pper.destroy(),this._popper
2021-12-03 00:03:49 UTC	59	IN	Data Raw: 70 3a 7b 62 65 68 61 76 69 6f 72 3a 74 68 69 73 2e 63 6f 6e 66 69 67 2e 66 61 6c 6c 62 61 63 6b 50 6c 61 63 65 6d 65 6e 74 7d 2c 61 72 72 6f 77 3a 7b 65 6c 65 6d 65 6e 74 3a 76 7d 2c 70 72 65 76 65 6e 74 4f 76 65 72 66 6c 6f 77 3a 7b 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 3a 74 68 69 73 2e 63 6f 6e 66 69 67 2e 62 6f 75 6e 64 61 72 79 7d 7d 2c 6f 6e 43 72 65 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 2e 6f 72 69 67 69 6e 61 6c 50 6c 61 63 65 6d 65 6e 74 21 3d 3d 74 2e 70 6c 61 63 65 6d 65 6e 74 26 26 65 2e 5f 68 61 6e 64 6c 65 50 6f 70 70 65 72 50 6c 61 63 65 6d 65 6e 74 43 68 61 6e 67 65 28 74 29 7d 2c 6f 6e 55 70 64 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 65 2e 5f 68 61 6e 64 6c 65 50 6f 70 70 65 72 50 6c 61 63 65 6d 65 6e 74 Data Ascii: p:{behavior:this.config.fallbackPlacement},arrow:{element:v},preventOverflow:{boundariesElement:this.config. boundary}},onCreate:function(t){t.originalPlacement!==t.placement&&e._handlePopperPlacementChange(t)},onUpdate :function(t){e._handlePopperPlacement
2021-12-03 00:03:49 UTC	60	IN	Data Raw: 6f 76 65 72 53 74 61 74 65 3d 22 22 29 7d 2c 49 2e 75 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 74 68 69 73 2e 5f 70 6f 70 70 65 72 2e 73 63 68 65 64 75 6c 65 55 70 64 61 74 65 28 29 7d 2c 49 2e 69 73 57 69 74 68 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 42 6f 6f 6c 65 61 6e 28 74 68 69 73 2e 67 65 74 54 69 74 6c 65 28 29 29 7d 2c 49 2e 61 64 64 41 74 74 61 63 68 6d 65 6e 74 43 6c 61 73 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 2e 61 64 64 43 6c 61 73 73 28 22 62 73 2d 74 6f 6f 6c 74 69 70 2d 22 2b 65 29 7d 2c 49 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e Data Ascii: overState=""")},I.update=function(){null!==this._popper&&this._popper.scheduleUpdate()},I.isWithContent=funct ion(){return Boolean(this.getTitle())},I.addAttachmentClass=function(e){t(this.getTipElement()).addClass("bs-tooltip-"+e)},I.getTipElement=function
2021-12-03 00:03:49 UTC	62	IN	Data Raw: 73 65 73 74 28 22 2e 6d 6f 64 61 6c 22 29 2e 6f 6e 28 22 68 69 64 65 2e 62 73 2e 6d 6f 64 61 6c 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 65 2e 68 69 64 65 28 29 7d 29 7d 29 2c 74 68 69 73 2e 63 6f 6e 66 69 67 2e 73 65 6c 65 63 74 6f 72 3f 74 68 69 73 2e 63 6f 6e 66 69 67 3d 72 28 7b 7d 2c 74 68 69 73 2e 63 6f 6e 66 69 67 2c 7b 74 72 69 67 67 65 72 3a 22 6d 61 6e 75 61 6c 22 2c 73 65 6c 65 63 74 6f 72 3a 22 22 7d 29 3a 74 68 69 73 2e 5f 66 69 78 54 69 74 6c 65 28 29 7d 2c 49 2e 5f 66 69 78 54 69 74 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 74 79 70 65 6f 66 20 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 6f 72 69 67 69 6e 61 6c 2d 74 69 74 6c 65 22 29 3b 28 74 68 69 73 Data Ascii: sest(".modal").on("hide.bs.modal",function(){return e.hide()})}),this.config.selector?this.config=r({},this.config,{tr igger:"manual",selector:""}):this._fixTitle()},I._fixTitle=function(){var t=typeof this.element.getAttribute("data-original-title"); (this
2021-12-03 00:03:49 UTC	63	IN	Data Raw: 74 69 6f 6e 28 29 7b 66 6f 72 28 76 61 72 20 74 20 69 6e 20 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 29 69 66 28 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 74 5d 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 49 2e 5f 67 65 74 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 72 65 74 75 72 6e 22 6e 75 6d 62 65 72 22 3d 3d 74 79 70 65 6f 66 28 6e 3d 72 28 7b 7d 2c 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 65 66 61 75 6c 74 2c 74 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 2e 64 61 74 61 28 29 2c 6e 29 29 2e 64 65 6c 61 79 26 26 28 6e 2e 64 65 6c 61 79 3d 7b 73 68 6f 77 3a 6e 2e 64 65 6c 61 79 2c 68 69 64 65 3a 6e 2e 64 65 6c 61 79 7d 29 2c 22 6e 75 6d 62 65 72 22 3d 3d 74 79 70 65 6f 66 20 6e Data Ascii: tion(){for(var t in this._activeTrigger)if(this._activeTrigger[t])return!0;return!1},I._getConfig=function(n){return"n umber"==typeof(n=r({},this.constructor.Default,t(this.element).data(),n)).delay&&(n.delay={show:n.delay,hide:n.delay})," number"==typeof n
2021-12-03 00:03:49 UTC	64	IN	Data Raw: 22 34 2e 30 2e 30 22 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 75 7d 7d 2c 7b 6b 65 79 3a 22 4e 41 4d 45 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 65 7d 7d 2c 7b 6b 65 79 3a 22 44 41 54 41 5f 4b 45 59 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 69 7d 7d 2c 7b 6b 65 79 3a 22 45 76 65 6e 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 5f 7d 7d 2c 7b 6b 65 79 3a 22 45 56 45 4e 54 5f 4b 45 59 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6f 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 54 79 70 65 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 68 Data Ascii: "4.0.0"}},{key:"Default",get:function(){return u}},{key:"NAME",get:function(){return e}},{key:"DATA_KEY",get :function(){return i}},{key:"Event",get:function(){return _}},{key:"EVENT_KEY",get:function(){return o}},{key:"DefaultTy pe",get:function(){return h
2021-12-03 00:03:49 UTC	66	IN	Data Raw: 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 74 69 70 3d 74 68 69 73 2e 74 69 70 7c 7c 74 28 74 68 69 73 2e 63 6f 6e 66 69 67 2e 74 65 6d 70 6c 61 74 65 29 5b 30 5d 2c 74 68 69 73 2e 74 69 70 7d 2c 6d 2e 73 65 74 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 3b 74 68 69 73 2e 73 65 74 45 6c 65 6d 65 6e 74 43 6f 6e 74 65 6e 74 28 65 2e 66 69 6e 64 28 66 29 2c 74 68 69 73 2e 67 65 74 54 69 74 6c 65 28 29 29 3b 76 61 72 20 6e 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 74 65 6e 74 28 29 3b 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 6e 26 26 28 6e 3d 6e 2e 63 61 6c 6c 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 Data Ascii: lement=function(){return this.tip=this.tip||t(this.config.template)[0],this.tip},m.setContent=function(){var e=t(this. getTipElement());this.setElementContent(e.find(f),this.getTitle());var n=this._getContent();"function"==typeof n&&(n=n.c all(this.element)
2021-12-03 00:03:49 UTC	67	IN	Data Raw: 22 2c 74 61 72 67 65 74 3a 22 22 7d 2c 6c 3d 7b 6f 66 66 73 65 74 3a 22 6e 75 6d 62 65 72 22 2c 6d 65 74 68 6f 64 3a 22 73 74 72 69 6e 67 22 2c 74 61 72 67 65 74 3a 22 28 73 74 72 69 6e 67 7c 65 6c 65 6d 65 6e 74 29 22 7d 2c 68 3d 7b 41 43 54 49 56 41 54 45 3a 22 61 63 74 69 76 61 74 65 22 2b 69 2c 53 43 52 4f 4c 4c 3a 22 73 63 72 6f 6c 6c 22 2b 69 2c 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 3a 22 6c 6f 61 64 22 2b 69 2b 22 2e 64 61 74 61 2d 61 70 69 22 7d 2c 63 3d 22 64 72 6f 70 64 6f 77 6e 2d 69 74 65 6d 22 2c 75 3d 22 61 63 74 69 76 65 22 2c 66 3d 7b 44 41 54 41 5f 53 50 59 3a 27 5b 64 61 74 61 2d 73 70 79 3d 22 73 63 72 6f 6c 6c 22 5d 27 2c 41 43 54 49 56 45 3a 22 2e 61 63 74 69 76 65 22 2c 4e 41 56 5f 4c 49 53 54 5f 47 52 4f 55 50 3a 22 2e 6e 61 76 2c Data Ascii: ",target:""},l={offset:"number",method:"string",target:"(string|element)"},h={ACTIVATE:"activate"+i,SCROLL:" scroll"+i,LOAD_DATA_API:"load"+i+".data-api"},c="dropdown-item",u="active",f={DATA_SPY:'[data-spy="scroll"]',A CTIVE:".active",NAV_LIST_GROUP:".nav,

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	68	IN	Data Raw: 72 6e 20 6e 75 6c 6c 7d 29 2e 66 69 6c 74 65 72 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 74 7d 29 2e 73 6f 72 74 28 66 75 6e 63 74 69 6f 6e 28 74 2c 65 29 7b 72 65 74 75 72 6e 20 74 5b 30 5d 2d 65 5b 30 5d 7d 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 65 2e 5f 6f 66 66 73 65 74 73 2e 70 75 73 68 28 74 5b 30 5d 29 2c 65 2e 5f 74 61 72 67 65 74 73 2e 70 75 73 68 28 74 5b 31 5d 29 7d 29 7d 2c 67 2e 64 69 73 70 6f 73 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 6e 29 2c 74 28 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 69 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 73 63 72 6f Data Ascii: rn null}).filter(function(t){return t}).sort(function(t,e){return t[0]-e[0]}).forEach(function(t){e._offsets.push(t[0]),e._targets.push(t[1])})},g.dispose=function(){t.removeData(this._element,n),t(this._scrollElement).off(i),this._element=null,this._scro
2021-12-03 00:03:49 UTC	70	IN	Data Raw: 76 6f 69 64 20 74 68 69 73 2e 5f 63 6c 65 61 72 28 29 3b 66 6f 72 28 76 61 72 20 73 3d 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 2e 6c 65 6e 67 74 68 3b 73 2d 2d 3b 29 7b 74 68 69 73 2e 5f 61 63 74 69 76 65 54 61 72 67 65 74 21 3d 3d 74 68 69 73 2e 5f 74 61 72 67 65 74 73 5b 73 5d 26 26 74 3e 3d 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 5b 73 5d 26 26 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 5b 73 2b 31 5d 7c 7c 74 3c 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 5b 73 2b 31 5d 29 26 26 74 68 69 73 2e 5f 61 63 74 69 76 61 74 65 28 74 68 69 73 2e 5f 74 61 72 67 65 74 73 5b 73 5d 29 7d 7d 7d 2c 67 2e 5f 61 63 74 69 76 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 68 69 73 2e 5f 61 63 74 69 76 65 54 61 72 Data Ascii: void this._clear();for(var s=this._offsets.length;s--;){this._activeTarget!==this._targets[s]&&t>=this._offsets[s]&&("undefined"==typeof this._offsets[s+1]||t<this._offsets[s+1])&&this._activate(this._targets[s])}},g._activate=function(e){this._activeTar
2021-12-03 00:03:49 UTC	71	IN	Data Raw: 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 2e 66 6e 5b 65 5d 3d 6f 2c 67 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 7d 2c 67 7d 28 65 29 2c 56 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 22 62 73 2e 74 61 62 22 2c 6e 3d 22 2e 22 2b 65 2c 69 3d 74 2e 66 6e 2e 74 61 62 2c 72 3d 7b 48 49 44 45 3a 22 68 69 64 65 22 2b 6e 2c 48 49 44 44 45 4e 3a 22 68 69 64 64 65 6e 22 2b 6e 2c 53 48 4f 57 3a 22 73 68 6f 77 22 2b 6e 2c 53 48 4f 57 4e 3a 22 73 68 6f 77 6e 22 2b 6e 2c 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 3a 22 63 6c 69 63 6b 2e 62 73 2e 74 61 62 2e 64 61 74 61 2d 61 70 69 22 7d 2c 6f 3d 22 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 22 2c 61 3d 22 61 63 74 69 76 65 22 2c 6c 3d 22 64 69 73 61 62 6c 65 64 22 2c 68 3d 22 66 Data Ascii: t=function(){return t.fn[e]=o,g._jQueryInterface},g}(e),V=function(t){var e="bs.tab",n="."+e,i=t.fn.tab,r={HIDE:"hide"+n,HIDDEN:"hidden"+n,SHOW:"show"+n,SHOWN:"shown"+n,CLICK_DATA_API:"click.bs.tab.data-api"},o="dropdown-menu",a="active",l="disabled",h="f
2021-12-03 00:03:49 UTC	72	IN	Data Raw: 63 74 69 6f 6e 28 65 2c 6e 2c 69 29 7b 76 61 72 20 73 3d 74 68 69 73 2c 72 3d 28 22 55 4c 22 3d 3d 3d 6e 2e 6e 6f 64 65 4e 61 6d 65 3f 74 28 6e 29 2e 66 69 6e 64 28 5f 29 3a 74 28 6e 29 2e 63 68 69 6c 64 72 65 6e 28 64 29 29 5b 30 5d 2c 6f 3d 69 26 26 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 72 26 26 74 28 72 29 2e 68 61 73 43 6c 61 73 73 28 68 29 2c 61 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 73 2e 5f 74 72 61 6e 73 69 74 69 6f 6e 43 6f 6d 70 6c 65 74 65 28 65 2c 72 2c 69 29 7d 3b 72 26 26 6f 3f 74 28 72 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 61 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 31 35 30 29 3a 61 28 29 7d 2c 69 2e 5f 74 72 61 6e 73 69 Data Ascii: ction(e,n,i){var s=this,r=("UL"===n.nodeName?t(n).find(_):t(n).children(d))[0],o=i&&P.supportsTransitionEnd()&&r&&t(r).hasClass(h),a=function(){return s._transitionComplete(e,r,i)};r&&o?t(r).one(P.TRANSITION_END,a).emulateTransitionEnd(150):a()},i._transi
2021-12-03 00:03:49 UTC	74	IN	Data Raw: 63 72 69 70 74 2e 22 29 3b 76 61 72 20 65 3d 74 2e 66 6e 2e 6a 71 75 65 72 79 2e 73 70 6c 69 74 28 22 20 22 29 5b 30 5d 2e 73 70 6c 69 74 28 22 2e 22 29 3b 69 66 28 65 5b 30 5d 3c 32 26 26 65 5b 31 5d 3c 39 7c 7c 31 3d 3d 3d 65 5b 30 5d 26 26 39 3d 3d 3d 65 5b 31 5d 26 26 65 5b 32 5d 3c 31 7c 7c 65 5b 30 5d 3e 3d 34 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 61 74 20 6c 65 61 73 74 20 6a 51 75 65 72 79 20 76 31 2e 39 2e 31 20 62 75 74 20 6c 65 73 73 20 74 68 61 6e 20 76 34 2e 30 2e 30 22 29 7d 28 65 29 2c 74 2e 55 74 69 6c 3d 50 2c 74 2e 41 6c 65 72 74 3d 4c 2c 74 2e 42 75 74 74 6f 6e 3d 52 2c 74 2e 43 61 72 6f 75 73 65 6c 3d 6a 2c 74 2e 43 6f 6c 6c Data Ascii: cript.");var e=t.fn.jquery.split(" ")[0].split(".");if(e[0]<2&&e[1]<9||1===e[0]&&9===e[1]&&e[2]<1||e[0]>=4)throw new Error("Bootstrap's JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")}(e),t.Util=P,t.Alert=L,t.Button=R,t.Carousel=j,t.Coll
2021-12-03 00:03:49 UTC	74	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49750	13.224.189.9	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	74	OUT	GET /ovolohotels.com HTTP/1.1 Host: logo.clearbit.com Connection: keep-alive Accept: */* User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Origin: null Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-12-03 00:03:49 UTC	74	IN	HTTP/1.1 200 OK Content-Type: image/png Transfer-Encoding: chunked Connection: close Date: Fri, 03 Dec 2021 00:03:49 GMT access-control-allow-origin: * Cache-Control: public, max-age=2592000 Server: envoy X-Cache: Miss from cloudfront Via: 1.1 0f538ee832e11056490 39b38ce89e883.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA2-C1 X-Amz-Cf-Id: 7v4sgpdx9Q_PpUE8e9RRwdfynnhOlPreWvfiJQfmq4zIpUvAHuzdYA==

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:03:49 UTC	75	IN	Data Raw: 64 64 61 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 80 00 00 00 80 08 02 00 00 00 4c 5c f6 9c 00 00 1d 39 49 44 41 54 78 9c ec 7d 07 58 14 d7 fa f7 79 cf ec 82 10 40 7a 53 93 28 c5 12 95 45 04 54 4c 6c 74 ec b1 82 3d c5 68 ec 49 4c d4 d8 92 ab 26 96 88 8a c9 cd bd c6 48 6c 60 d4 5c 13 41 b0 c6 dc bf 4a 53 8a 68 2c 88 1a 95 0e 16 24 12 d8 39 ef f7 cc 99 05 11 2c 6c 72 2f bb 7e 77 7f 8f 0f c2 ce cc 99 99 f3 3b e7 3d 6f 3d ab 68 eb e2 48 0c d0 1d a8 ae 1f e0 7f 1d 06 02 74 0c 03 01 3a 86 81 00 1d c3 40 80 8e 61 20 40 c7 30 10 a0 63 18 08 d0 31 0c 04 e8 18 06 02 74 0c 03 01 3a 86 81 00 1d c3 40 80 8e 61 20 40 c7 30 10 a0 63 18 08 d0 31 0c 04 e8 18 06 02 74 0c 03 01 3a 86 42 d7 0f d0 78 40 cd 2f f8 c8 7f 0f 8f 61 cd af d0 e0 b8 fe e2 39 22 Data Ascii: ddaPNGIHDRL\9IDATx}Xy@zS(ETLlt=hIL&Hl`\AJSh,$9,lr/~w;=o=hHt:@a @0c1t:@a @0c1t:Bx@/a9"
2021-12-03 00:03:49 UTC	78	IN	Data Raw: 66 39 38 0d 0a 54 66 d7 13 32 80 0f ab 30 1a d1 fb b5 fe 68 5d 4f 94 e7 89 80 06 19 6d 0d c4 92 16 6d b1 a7 35 d5 84 78 3e 54 85 ff 02 58 9d e2 7a 5d e2 7f 96 00 59 52 01 22 20 d3 65 27 fc cf 12 40 11 29 13 29 10 05 10 05 8f 39 eb 06 7f 7a 0d a8 5d ef b0 fe 47 4f 03 3e dc d4 01 6b 05 71 bd a5 53 73 4e 23 5a 7b 8c b2 2f 2b 4b cf cc 7f e6 8e 6b c5 b6 98 18 6f ef ee d2 73 e0 83 76 ee ae f4 d9 b7 d4 ec 03 d2 40 1d 78 f4 0d b4 c1 9f 26 80 97 99 68 bd 74 3d 7c d6 86 9d 57 a7 b1 67 37 5d db 07 f5 c2 eb 8d 34 c0 38 45 80 44 20 54 e0 72 c0 98 80 82 a0 5a 33 30 ea 9d fd d0 b0 90 ff 3d 52 e4 21 9b 7e 7f 3a ca af 2d 01 b5 11 25 c6 28 27 5f 8b 3b d7 5e 2b 09 5e 04 04 54 d4 7c 42 ea 10 20 4b c5 67 08 05 d0 98 c8 5c fd ac 99 30 f2 c0 e7 89 57 7f be 47 9e f8 e0 9a 67 ab Data Ascii: f98Tf20h]Omm5x>TXz]YR" e'@))9z]GO>kqSsN#Z{/+Kkosv@x&ht=|Wg7]48ED TrZ30=R!~:-%('_;^+^T|B Kg\0WGg
2021-12-03 00:03:49 UTC	82	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5808 Parent PID: 4756

General

Start time:	01:03:43
Start date:	03/12/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\It.servicedesk-VoiceFax-723-2121-723.html
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: chrome.exe PID: 4904 Parent PID: 5808

General

Start time:	01:03:44
Start date:	03/12/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,2614049055858890495,17816619576725297410,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1552 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis