ID: 635117
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 14:30:25
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

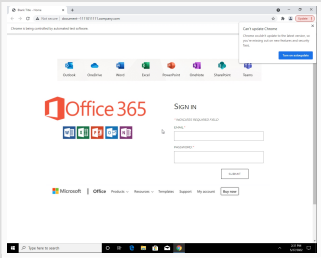
Windows Analysis Report

http://document--1111011111.company.com/

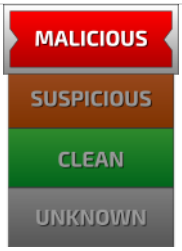
Overview

General Information

Sample URL:	http://document--1111011111.company.com/
Analysis ID:	635117
Infos:	



Detection



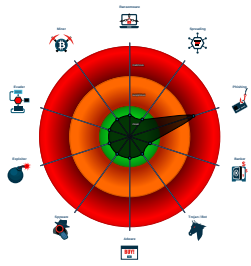
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish20

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 7668 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument http://document--1111011111.company.com/ MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 7404 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1740,10588110985535776619,16488514565616499681,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2108 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
25855.0.pages.csv	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

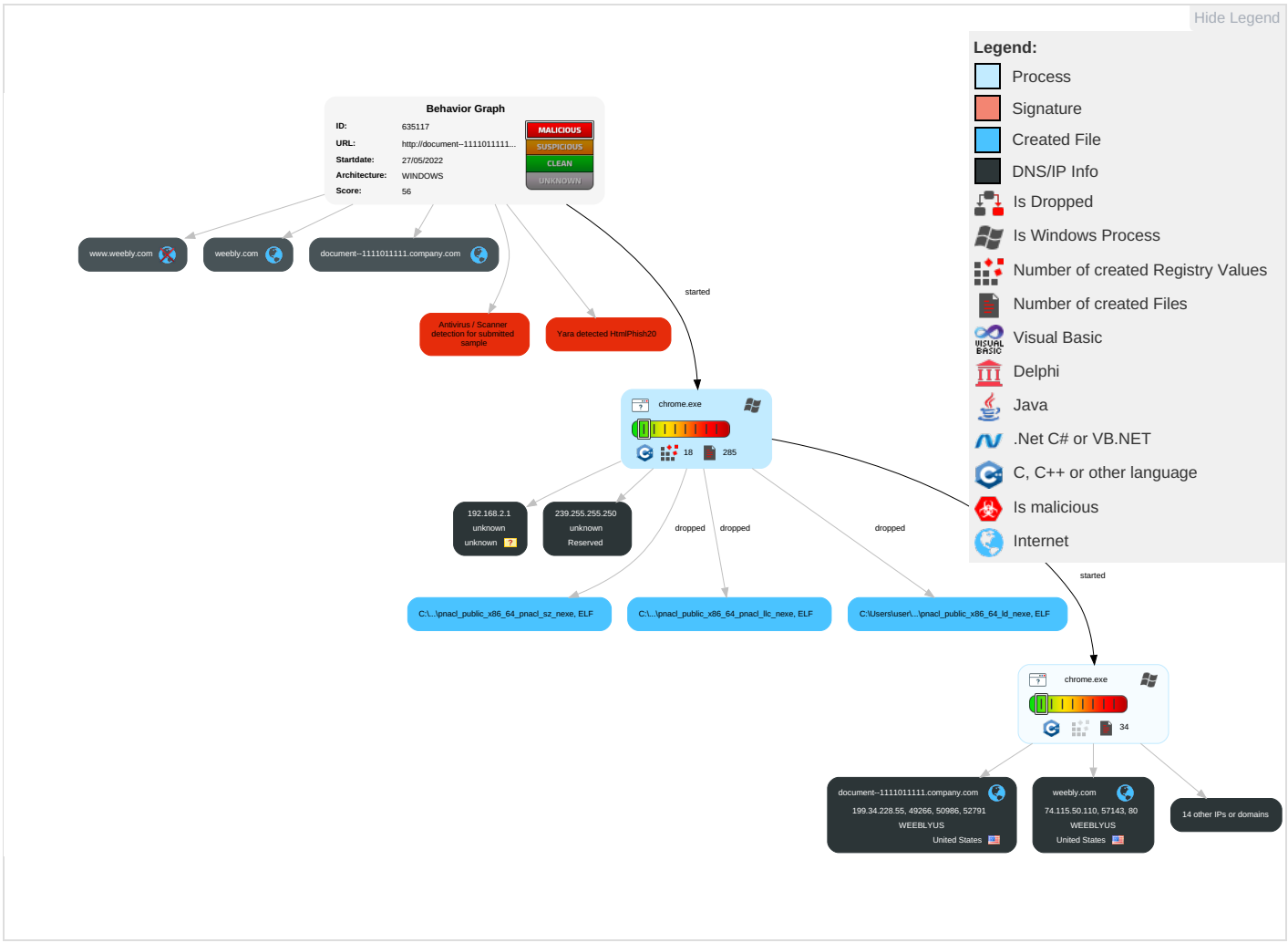
Phishing

Yara detected HtmlPhish20

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	5 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	6 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

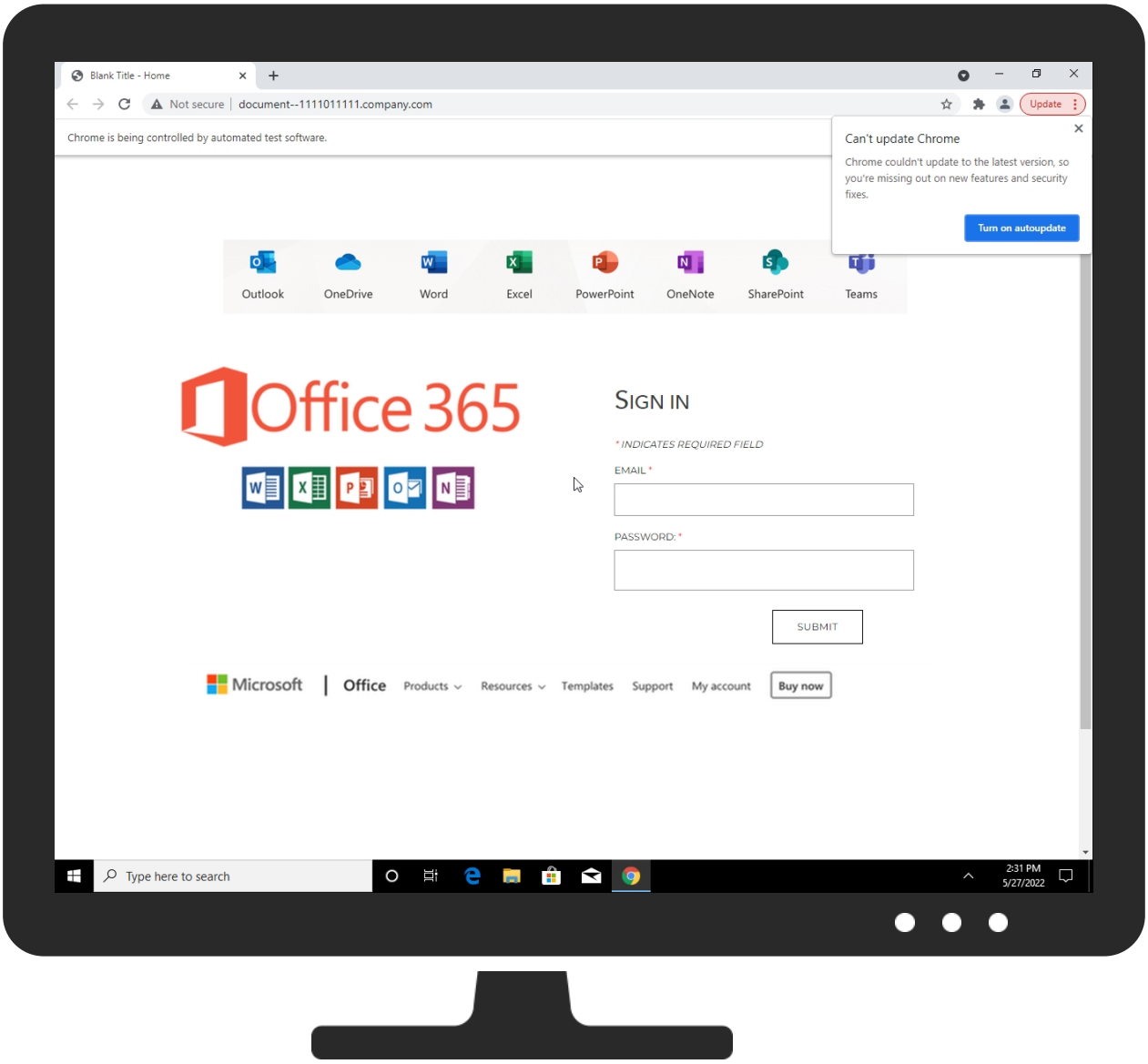
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://document--1111011111.company.com/	0%	Virustotal		Browse
http://document--1111011111.company.com/	0%	Avira URL Cloud	safe	
http://document--1111011111.company.com/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
weebly.map.fastly.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.185.99	true	false		high
company.com	35.71.162.193	true	false		high
accounts.google.com	142.250.185.141	true	false		high
www-google-analytics.l.google.com	142.250.185.174	true	false		high
sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	52.25.131.159	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.251.37.100	true	false		high
clients.l.google.com	142.250.185.174	true	false		high
weebly.com	74.115.50.110	true	false		high
document--1111011111.company.com	199.34.228.55	true	false		high
www.company.com	unknown	unknown	false		high
ec.editmysite.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
www.weebly.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://document--1111011111.company.com/files/theme/fonts/2cd55546-ec00-4af9-aeca-4a3cd186da53.woff2?1652461604	false		high
http://document--1111011111.company.com/	false		high
http://document--1111011111.company.com/files/theme/fonts/2e3f5cb9-101f-46cf-a7b3-dfaa58261e03.woff2?1652461604	false		high
http://document--1111011111.company.com/files/theme/fonts/63a74598-733c-4d0c-bd91-b01bffcd6e69.ttf?1652461604	false		high
http://document--1111011111.company.com/files/theme/fonts/627fbb5a-3bae-4cd9-b617-2f923e29d55e.woff2?1652461604	false		high
http://cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1651866883	false		high
http://www.weebly.com/uploads/reseller/assets/356764895-favicon.ico	false		high
http://cdn2.editmysite.com/css/old/fancybox.css?1651866883	false		high
http://cdn2.editmysite.com/js/lang/en/stl.js?buildTime=1651866883&	false		high
http://document--1111011111.company.com/	false		high
http://ec.editmysite.com/com.snowplowanalytics.snowplow/tp2	false		high
http://cdn2.editmysite.com/css/social-icons.css?buildtime=1651866883	false		high
http://document--1111011111.company.com/uploads/1/4/1/8/141840186/editor/2screenshot-2021-04-26-at-19-59-12-orig-orig.png?1652460803	false		high

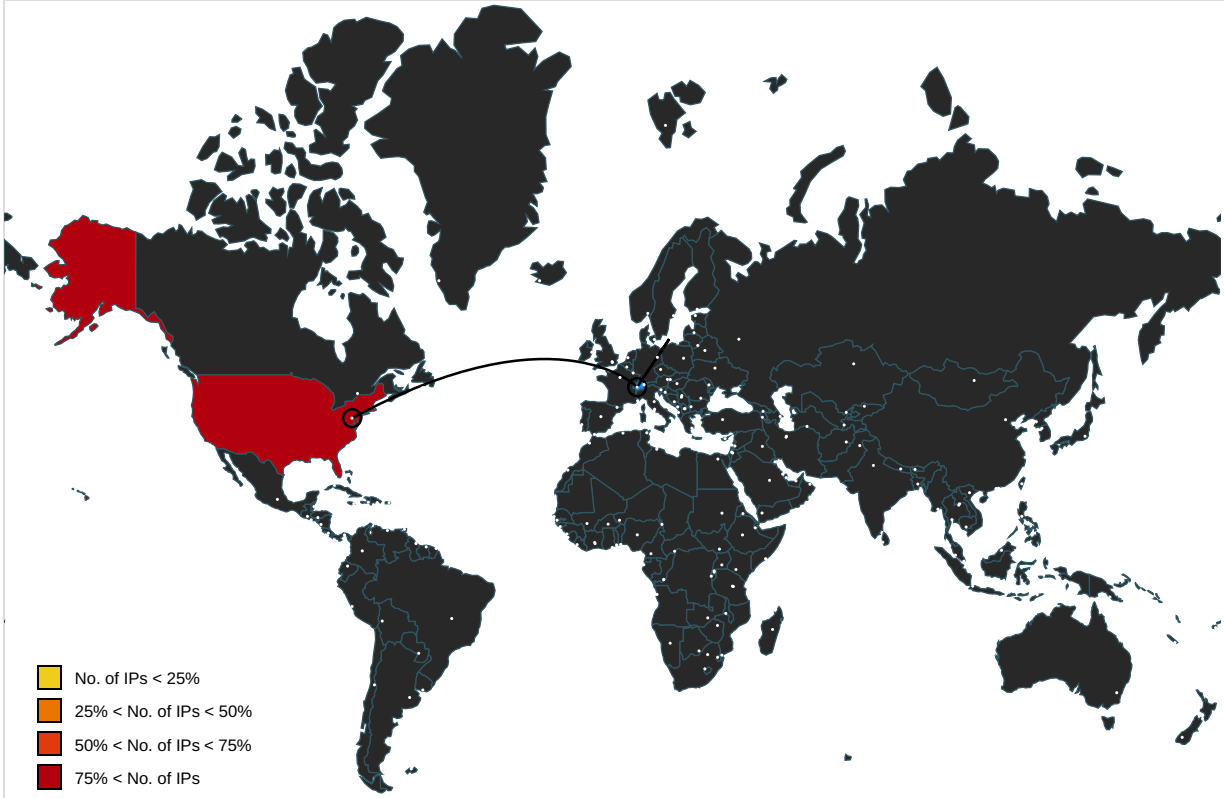
Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://document--1111011111.company.com/files/main_style.css?1652461604	false		high
http://document--1111011111.company.com/files/theme/plugins.js?1565969634	false		high
http://cdn2.editmysite.com/js/wsnbn/snowday262.js	false		high
http://cdn2.editmysite.com/css/sites.css?buildTime=1651866883	false		high
http://document--1111011111.company.com/uploads/1/4/1/8/141840186/3pdp-orig-orig_orig.png	false		high
http://document--1111011111.company.com/uploads/1/4/1/8/141840186/1screenshot-2021-04-26-at-19-59-20-orig-orig-orig_orig.png	false		high
http://document--1111011111.company.com/files/theme/fonts/6de0ce4d-9278-467b-b96f-c1f5f0a4c375.ttf?1652461604	false		high
http://document--1111011111.company.com/files/theme/fonts/46cf1067-688d-4aab-b0f7-bd942af6efd8.ttf?1652461604	false		high
http://document--1111011111.company.com/ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails]	false		high
http://document--1111011111.company.com/files/theme/fonts/f26faddb-86cc-4477-a253-1e1287684336.woff?1652461604	false		high
http://document--1111011111.company.com/files/theme/custom.js?1565969634	false		high
http://document--1111011111.company.com/files/theme/fonts/1e9892c0-6927-4412-9874-1b82801ba47a.woff?1652461604	false		high
http://document--1111011111.company.com/files/theme/fonts/fa19948e-5e38-4909-b31e-41acd170d6f2.woff?1652461604	false		high
http://cdn2.editmysite.com/js/site/main.js?buildTime=1651866883	false		high
http://https://www.google.com/recaptcha/api.js?_=1653687066398	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/cleardot.gif	craw_window.js.1.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.1.dr	false		high
http://https://www.google.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high
http://https://accounts.google.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high
http://https://apis.google.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.1.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://clients2.google.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.1.dr	false		high
http://https://ogs.google.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high
http://document--1111011111.company.com/2	History Provider Cache.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libcrt_platform_a.1.dr, pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.1.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.1.dr, pnacl_public_x86_64_pnacl_llc_nexe.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.1.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://clients2.googleusercontent.com	326a7714-6c2f-4802-b696-f5cb4eb8e13f.tmp.3.dr, 2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.tmp.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://document--1111011111.company.com:80	67268b83-2658-4083-928c-f181c95a7676.tmp.1.dr, a2acd1b4-60a6-4573-adf6-b0849a814490.tmp.1.dr	false		high
http://https://www.google.com/	manifest.json.1.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libcrt_platform_a.1.dr, pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.1.dr, manifest.json0.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.115.50.110	weebly.com	United States		27647	WEEBLYUS	false
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
199.34.228.55	document--1111011111.company.com	United States		27647	WEEBLYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.141	accounts.google.com	United States		15169	GOOGLEUS	false
52.25.131.159	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.251.37.100	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635117

Start date and time: 27/05/202214:30:25	2022-05-27 14:30:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://document--1111011111.company.com/
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@26/127@10/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, CompPkgSrv.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.185.195, 142.250.185.238, 142.250.185.234, 142.250.185.106, 74.125.108.199, 142.250.185.99, 142.250.185.174, 172.217.23.106, 142.250.181.227, 142.250.185.67, 172.217.18.99, 172.217.16.142, 142.250.186.42
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fonts.googleapis.com, r2.sn-1gi7znek.gvt1.com, fs.microsoft.com, content-autofill.googleapis.com, slscr.update.microsoft.com, ajax.googleapis.com, fonts.gstatic.com, ctldl.windowsupdate.com, clientservices.googleapis.com, r2---sn-1gi7znek.gvt1.com, arc.msn.com, r5---sn-1gi7znek.gvt1.com, ris.api.iris.microsoft.com, redirector.gvt1.com, login.live.com, update.googleapis.com, safebrowsing.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, nexusrules.officeapps.live.com, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\499806a5-d09f-49ac-abc4-ab4becf5f9d4.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):	105175
Entropy (8bit):	6.035164642099087
Encrypted:	false
SSDEEP:	1536:IGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:I7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	0BA35633508CFBDF33CB751D882F8CD1
SHA1:	ECE810FC9214D2FFB14069F95F43CF444486709A
SHA-256:	0ED3A61FA1F92BFA7BF2833206E10C4AF495F8BDF7783E0C29FE64274CDEB63F
SHA-512:	6737D55EB32A48ED0A95FD6C2AED7EAC44EDEA0F1BB01A03B938EE71D969253ADB92707174C3C2083E948B0E9C8A13954FCE70411F768C6783A0C135B6C17D D6
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user ":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_ key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcO PsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2llZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362 cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"poli cy":{"last_statistics_update":"13298160661097806"},"profile":{"info_cache":{"Default":{"active_time":1653687062.997598,"avatar_icon":"chrome

C:\Users\user\AppData\Local\Google\Chrome\User Data\4eb1b1cd-c449-40dc-9516-10535441562b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.7572167763384026
Encrypted:	false
SSDEEP:	384:2rn3M2IyM7QjCUYOSNB9YT/g5qHfgluJnqOMgMC27MikxbvCjr2k8Q0eb5CfhgQw:4GgSjbo7/AV7Al+RHKCGdQF
MD5:	3E78A1C4ACBE4D45570F6548A10F8A2F
SHA1:	6698ABC23ED159C58653AE2C013A2D83B00CBFD4
SHA-256:	97D0793FBAE298FE73E1C0C4415233C25F322C4E9935F43AA0A67859D9970C58
SHA-512:	F39838D396EA5B5B2F491063368B21AAA138EA47BE0E8CFFB88FA9C01E9267FA1C3D95AD9D11CBCADBE18FAAD200406255B4CB5F0494B4D0CA8C81AB9B528 E3C
Malicious:	false
Reputation:	low
Preview:	4}.....T...C.:\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA... c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. . O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O. n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...m]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p. \.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....m]8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e11aab8-c49c-4022-a59f-5e45fdc69027.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):	109669
Entropy (8bit):	6.065193133645291
Encrypted:	false
SSDEEP:	1536:dGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:d7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	1F566330D7C8C2072DFEC5E764F7A094
SHA1:	E7C578908DB21772E37D6DB9A3EE4D61389357CD
SHA-256:	D466799A5C571540141376019C2FCA46B654E532C6051FA2AFF1B465FA7905B6
SHA-512:	455B8F006DCEFCC1BDB25763FE0FF6EFCC42570F61B6A103F6230E9085050BD197942106DF4849290F186BCF5740641A4ACB1CB072F2B61FCEB9F0E464D2A7C5
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\727fce5a-1a3e-4378-b9b1-ddb83343e565.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96852
Entropy (8bit):	3.757322555673529
Encrypted:	false
SSDEEP:	384:Ofrn3M2IyM7QjCUYOSNB9YT/g5qHfgluJnqOMgMC27MikxbvCjr2k00eb5CfhgQI:qGgSjgo7/AV7Al+RHKCGdQF
MD5:	654A824A16BF922B536AC5B18F077C05
SHA1:	382094896D065FA5360E73B3656D149707B09AEB
SHA-256:	F8FC7A5E5364A52D8986E2DF4AC4D4B162E876D293EE1752AD3B9E4333ADA465
SHA-512:	958E88F9DC06EAE39D1D7F399EC9BAB33AE5BF3AE9F7EC51C900C408E2155B08909103267D7607DAF559F03DADBE60E08FE285FA24511D87527704F04C16DB4
Malicious:	false
Reputation:	low
Preview:	Pz.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...m]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....m]8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\7e38bfa8-be9b-4562-a91f-0b9502d1d361.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):	109763
Entropy (8bit):	6.065481482032037
Encrypted:	false
SSDEEP:	1536:lGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:l7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	4383B706518AA2B70528158AC26FBF6A
SHA1:	234E3F32F73D75633A125AE09088176F6C131A09
SHA-256:	A024DA314A790568D18A6E81A64E11CB2F1A94E2141DBAC3F598661651597BA9
SHA-512:	A78B00BA56509CD4D284E53FF1941B47ABCAA862CBBBCB6233189CAAA77FFC77A09FE1DE3F236F41DDB2D7A1E69BA180CB3EAAF710C0C032724C56B9F7CFD742
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXSoWA0:+g
MD5:	FA7200D6F80CD1757911C45559E59C0E
SHA1:	89C6E99BAEC4EBB3E9A97B928FB473D1498EBA88
SHA-256:	D9779EA4D6DD544A23C2A1C53146B6A4E596927F47DFA0680B0A7EE751D43BB2
SHA-512:	71D9B2DA8EAF404063D918812BA61C3EFB6A23A283B0332180A38C8137FBB21D7977C008D5A57A74469776945CD4ED42C0BCC09F923EDEC52D8F7FE90FA2D14
Malicious:	false
Reputation:	low
Preview:	sdPC.....A.>'..M..,,.-.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c99278d-fcc2-4dcb-a5ed-5b75bc43e837.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15765
Entropy (8bit):	5.572985860329377
Encrypted:	false
SSDEEP:	384:+dVtMLlhXO1kXqKf/pUZNCgVLH2HfEorUS45A4E:tLllO1kXqKf/pUZNCgVLH2Hf5rUBAr
MD5:	523B28EF06B1DBB3D1C5CE0A04026AFE
SHA1:	3C76EAF30B91F980D48CBE108284EDCF2B142ECC
SHA-256:	743979B73444728A1673627F7EE8E1513F8BE59CB33CFF7494CC0C4BE849A83D
SHA-512:	C15A6ED6D9857B86C8F6606634E648714F77250D0E21BA045B56F9C2FB46E4312126FF65D3603C2BAA802D660C965DB044CA24A06F38E862A02F34E6BD853BAE
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1d3b1e1c-593f-48c0-84a3-231da72d3e94.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):	18395
Entropy (8bit):	5.555374007132332
Encrypted:	false
SSDEEP:	384:+b3tqLlhXr1kXqKf/pUZNCgVLH2HfE4rUTHGohAA4q:rLllr1kXqKf/pUZNCgVLH2HfjrUzGnA1
MD5:	5BDB71CEF4214F72C166E77373338076
SHA1:	BE7E57D1787FD2DA92DB0C33707115C44D46E5BA
SHA-256:	F3EB18327FE2BFE5765C53EDB549A423FDB8B88D9E3EFDA30818065DC1D58613
SHA-512:	7ACAAAF9718B910B4E2688EDC58496698BBFF15953C776484C5AA969597CC2BB2810CC36F765BF42095E79F1250CF98292C5ADCAD4F5ECCC0CC94FD13331585
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\20b3f0bc-ad58-4855-bb18-1da675183ef2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	1536:avbYFOZyYb37psk2SVlfN/qskVMxoZ51+XBY95/E5cCDd4QAOXxfzUBn2Y2l3P:a8Y7wqFTkVMO51+XBY96Nd4ByVuV2l3P
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``... .....N..... .(....D..... .2v...M..(..... ....]..X\.).H...>..Z.....\...._...V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[....z...`...J.....9...E...k...R.D.....G...A.....;...E...h..XKd..KW.....D...>...=..X.... GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`..\...K...D...A...;.....3...\...e... V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...I..U].M.5@.....6...C...@..T....EW..LX..=K..O b..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2cea7aa6-e8dc-403b-8fb0-13dc2cb9b77c.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):	2401
Entropy (8bit):	4.970081574688563
Encrypted:	false
SSDEEP:	48:Y2twDHXPqyv3zsOcTDsXmZRLsVlRs2X5so8jPQSsmhPYhbD:JODHXi+2/2VD0ghH
MD5:	DE37D147F5065E1B35362AE2F4C2B922
SHA1:	31D1640A16F13EC7DAC1515DD5C8A518406A054A
SHA-256:	871E788C1D1AC32D41FC63A1309B48E874180718EAD5EA90EA66BE01F40618AF
SHA-512:	7304DFE39D284D170D06BA43B98AB3067E93790F0399BA45859E1403028A8FB9FBC291E56EEA536B3876A631E87A5946AF39FA93522E68B51BEB42C200EB5725
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://update.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13300752665178232","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13300752665178234","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13300752665198628","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13300752665198630","port":443,

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\326a7714-6c2f-4802-b696-f5cb4eb8e13f.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):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	48:YXsVVMHzzsmdAMHtKsyfDszmcQ/RLsOcXSsM1PzshVMH8sp1AAMHDysKGMHTFsB5:PGqGctrmKwGPTGD7GSGMphH
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\67268b83-2658-4083-928c-f181c95a7676.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):	4438
Entropy (8bit):	5.03525013446265
Encrypted:	false
SSDEEP:	96:nGhctKI1/GaRWMoiVmde/kPS1KVrMVXAiZw4:n3txWMPk6MVq
MD5:	49D66ABD349F5A0E235BFCD9E721C4F9
SHA1:	0FB6D446CCC8139253B7EF0EF506F381B6A5642E
SHA-256:	33CF52BF6C9C18D9E0C9AD9C0455E90A1CF9F0BEF7B1717204BBA67046861808
SHA-512:	111869DE7517D0D0F42C936281F8153AAD5B3E578ADFFA6B0F143CF7EE264636BC3148B6F55812C7B41E743369AB337424AC0C82F72BB233947CD509DF5C074
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298160663251179","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"49601082":3,"5151071":2,"54845618":24,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298160663247267"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653687065.188181,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85846f46-90c1-40dd-8abd-b654f55dc759.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):	3488
Entropy (8bit):	4.936099598577836
Encrypted:	false
SSDEEP:	48:YcLvl2rAUTxqwoTw0/ZxQ8cO1TSUQ/9BhUIEyMoI3HmeSye7peVGaQtqoonVuAip:nMhYn1/GaRWMoiVmdeMtMVuAip
MD5:	8145FE81D26AAEE8EC162625905D5E80
SHA1:	83C8495D8EEECAB0AED6F9485A4099445CF38D53
SHA-256:	39FDAE15A4FF45D4E3655EDBBA0A53658F96CDA383A75B110473D9B848363FA8
SHA-512:	2C1460E4E214E31BE74EE0E49EE96A107FC6323BDE0819939ED8B34C0A261CCCFCA662C9A35430C550849D0C04A3F31A67810EF33395AE7597A5EDDEFC142AAE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298160663251179","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298160663247267"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"0f4cafc2-cb8d-4b96-9034-7adc92b4ea3e"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"A65FFE166A4986229EECDE98A4723A16","engagement":{"schema_version":4}},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
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):	11336
Entropy (8bit):	6.0707244876366575
Encrypted:	false
SSDEEP:	192:AbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Ab+nldByaFx4toj8VEPT
MD5:	2E2110A99AD3AE9721A458C95C64C868
SHA1:	72AE17599EDC0B2DC61C41D946E3E296864F2CBA
SHA-256:	BB46BA705D5F6F43F66B07EA5DA4CC7CC0BF8FE635CCC4EBBA30A5D4A54158DE
SHA-512:	29D95D043F3E529DD33F73B3207A9167D479D9FC404209497B53229CF68AA634CB8A1FE3FD08512FD7F48AFB567144DB873FBBDAD8171D42968B97357F06BC1
Malicious:	false
Reputation:	low

Preview:	{"file_hashes":[{"block_hashes":["8D+nOE33nrpuAnTVcJlgMPWVo79reBkp3Z22WTJi5B8="],"block_size":4096,"path":"_locales/nb/messages.json"},{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpl0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	1536:avbYFOZyYb37psk2SVlfN/qskVMxoZ51+XBY95/E5cCDd4QAOXxfzUBn2Y2l3P:a8Y7wqFTkVMO51+XBY96Nd4ByVuV2l3P
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``... .....N..... .(....D..... .2v...M..(..... .....]..X\.).H...>..Z.....\...._...V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[....z...`...J.....9...E...k...R.D.....G...A....;...E...h..XKd..KW.....D...>...=..X....GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`...\...K...D...A...;.....3...\...e...V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...l..U].M.5@.....6...C...@..T....EW..LX..=K..Ob..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

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
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.1404917413331015
Encrypted:	false
SSDEEP:	12:h0uJEBurz/lvur6mRKhGfYpUoiBk778B/xgskZBGN2N3H2fQQX0xOz:iuK2z/lw4hC3/Y78BJgskfGN2NX2IQXL
MD5:	682329F1AE8519E4B1B369C263F2338A
SHA1:	F6DC1CEC35FEA30A28372812B9B308866EF7BC79
SHA-256:	FE67C664F35C2986C9054321BFB150E60542D93C66ADDB4AEE727D1F3DC48A5A
SHA-512:	E9EB4B9ADD65CCF9D1A1753CED149A389CDE65B4C3976E28BF22311777A9E4A8707C6295DE03F0F2AB120217E961E8EC5772B3A5CBE68558D516BD9508C1A954
Malicious:	false
Reputation:	low
Preview:	....."@....1111011111..blank..com..company..document..home..http..title*`.....1111011111.....blank.....com.....company.....document.....home.....http.....title..2.....0.....1.....a.....b.....c.....d.....e.....h.....i.....k.....l.....m.....n.....o.....p.....t.....u.....y...:J.....Bb...^..... .....*(http://document--1111011111.company.com/2.Blank Title - Home:.....J.....$.....

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):	2401
Entropy (8bit):	4.970081574688563
Encrypted:	false
SSDEEP:	48:Y2twDHXPqyv3zsOcTDsXmZRLsVlRs2X5so8jPQSsmhPYhbD:JODHXi+2/2VD0ghH
MD5:	DE37D147F5065E1B35362AE2F4C2B922
SHA1:	31D1640A16F13EC7DAC1515DD5C8A518406A054A
SHA-256:	871E788C1D1AC32D41FC63A1309B48E874180718EAD5EA90EA66BE01F40618AF
SHA-512:	7304DFE39D284D170D06BA43B98AB3067E93790F0399BA45859E1403028A8FB9FBC291E56EEA536B3876A631E87A5946AF39FA93522E68B51BEB42C200EB5725
Malicious:	false
Reputation:	low

Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://update.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13300752665178232","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13300752665178234","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13300752665198628","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13300752665198630","port":443,

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):	4438
Entropy (8bit):	5.03525013446265
Encrypted:	false
SSDEEP:	96:nGhctKI1/GaRWMoiVmde/kPS1KVrMVXAiZw4:n3txWMPk6MVq
MD5:	49D66ABD349F5A0E235BFCD9E721C4F9
SHA1:	0FB6D446CCC8139253B7EF0EF506F381B6A5642E
SHA-256:	33CF52BF6C9C18D9E0C9AD9C0455E90A1CF9F0BEF7B1717204BBA67046861808
SHA-512:	111869DE7517D0D0F42C936281F8153AAD5B3E578ADFFA6B0F143CF7EE264636BC3148B6F55812C7B41E743369AB337424AC0C82F72BB233947CD509DF5C074
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298160663251179","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"49601082":3,"5151071":2,"54845618":24,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298160663247267"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653687065.188181,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm

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):	18396
Entropy (8bit):	5.555380825923972
Encrypted:	false
SSDEEP:	384:+b3tqLlhXr1kXqKf/pUZNCgVLH2HfE4rUTHG/h/A4B0:rLllr1kXqKf/pUZNCgVLH2HfjrUzGtAB
MD5:	EB2C637FDC9552BA8F813F10C4C88EFA
SHA1:	F5DC02F999035D80762D487C43FE5F31F1F2B099
SHA-256:	06573A13A38E948AE3F987D0CEF93BA873EAE54333088D56DA6F87A052BCB251
SHA-512:	93A8F8212B6E4ADB0DD29CC6A416627A5902C1FF76C459A2370E0A292DD620928B575B0D9FBA1183A714BCB65DC875B8E867B350A9F1B7268F64C88C7A7BAE E
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\8a436e02-2cc8-482b-a1f3-19d163320340.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.762700853527964
Encrypted:	false
SSDEEP:	3:YLb9N+eAXRfHDH2LS7PMVKJqjn1KKtiKnMb1KKtiVY:YHpoeS7PMVKJw1K3KnMRK3VY
MD5:	038931FF72A0C6AA0695A404960B1B22
SHA1:	90802F36B75C3CA70FC8CD1CF8BDFBAE0E8723A4
SHA-256:	BEF93811AE263E2E9145A44205340015843B1D4485D084BB642EAEB500FE564C

SHA-512:	97903821D21BB748255C29BE83BCA5BE61E0E36719050D4BB780EBC35424202A23F3ED4EE0056833E7748F1D55D82A5F38476298C5012202776BEA411DA7001E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[],"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
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

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 no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.762700853527964
Encrypted:	false
SSDEEP:	3:YLb9N+eAXRfHDH2LS7PMVKJqjn1KKtiKnMb1KKtiVY:YHpoeS7PMVKJw1K3KnMRK3VY
MD5:	038931FF72A0C6AA0695A404960B1B22
SHA1:	90802F36B75C3CA70FC8CD1CF8BDFBAE0E8723A4
SHA-256:	BEF93811AE263E2E9145A44205340015843B1D4485D084BB642EAEB500FE564C
SHA-512:	97903821D21BB748255C29BE83BCA5BE61E0E36719050D4BB780EBC35424202A23F3ED4EE0056833E7748F1D55D82A5F38476298C5012202776BEA411DA7001E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[],"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\Session Storage\000001.dbtmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\CURRENT (copy)

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 75B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\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
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.762700853527964
Encrypted:	false
SSDEEP:	3:YLb9N+eAXRfHDH2LS7PMVKJqjn1KKtiKnMb1KKtiVY:YHpoeS7PMVKJw1K3KnMRK3VY
MD5:	038931FF72A0C6AA0695A404960B1B22
SHA1:	90802F36B75C3CA70FC8CD1CF8BDFBAE0E8723A4
SHA-256:	BEF93811AE263E2E9145A44205340015843B1D4485D084BB642EAEB500FE564C
SHA-512:	97903821D21BB748255C29BE83BCA5BE61E0E36719050D4BB780EBC35424202A23F3ED4EE0056833E7748F1D55D82A5F38476298C5012202776BEA411DA7001E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000001.dbtmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\CURRENT (copy)

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAlxQRDKlVjn:scoBY7jn

MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 75B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\c5fc1302-d5fd-4216-aa4a-f4f071904f83.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.762700853527964
Encrypted:	false
SSDEEP:	3:YLb9N+eAXRfHDH2LS7PMVKJqjn1KKtiKnMb1KKtiVY:YHpoeS7PMVKJw1K3KnMRK3VY
MD5:	038931FF72A0C6AA0695A404960B1B22
SHA1:	90802F36B75C3CA70FC8CD1CF8BDFBAE0E8723A4
SHA-256:	BEF93811AE263E2E9145A44205340015843B1D4485D084BB642EAEB500FE564C
SHA-512:	97903821D21BB748255C29BE83BCA5BE61E0E36719050D4BB780EBC35424202A23F3ED4EE0056833E7748F1D55D82A5F38476298C5012202776BEA411DA7001E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a2acd1b4-60a6-4573-adf6-b0849a814490.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):	4348
Entropy (8bit):	5.027207106142871
Encrypted:	false
SSDEEP:	96:n8hctKI1/GaRWMoiVmde/kPS1SVrMVXAiZw4:n1txWMPk6QVq
MD5:	4693CC13A2345DD7E016FAFD592315C0
SHA1:	BC70FD487D140640E7F5C352ABE0794595DD4CEB
SHA-256:	AD075F2E02C9DCA235CF5EA5D3343FFDE2D42C861CF16F65EDFE8E7A20503401
SHA-512:	87F16C333565080626E61A400134D0BA3AF0D9F9FE4DB5A91B3A1540D985DEC814B4E4BECD52A399F68D5183C24715558B7B77AB8D67558E6083B2A5DEA5D9A 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298160663251179","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"5151071":2,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298160663247267"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653687065.188181,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_su

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ca4ba07d-98ad-463d-afed-ceec1e048be7.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):	18396
Entropy (8bit):	5.555380825923972
Encrypted:	false
SSDEEP:	384:+b3tqLlhXr1kXqKf/pUZNCgVLH2HfE4rUTHG/h/A4B0:rLllr1kXqKf/pUZNCgVLH2HfjrUzGtAB
MD5:	EB2C637FDC9552BA8F813F10C4C88EFA
SHA1:	F5DC02F999035D80762D487C43FE5F31F1F2B099
SHA-256:	06573A13A38E948AE3F987D0CEF93BA873EAE54333088D56DA6F87A052BCB251

SHA-512:	93A8F8212B6E4ADB0DD29CC6A416627A5902C1FF76C459A2370E0A292DD620928B575B0D9FBA1183A714BCB65DC875B8E867B350A9F1B7268F64C88C7A7BAE E
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cfc18fbb-f0d3-42f4-81a4-e8618419cc32.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):	3488
Entropy (8bit):	4.935874445663314
Encrypted:	false
SSDEEP:	48:YcLvl2rAUTxqwoTw0/ZxQ8cO1TSUQ/9BhUIEyMoI3HmeSye7peVGaQtqoonVuzip:nMhYn1/GaRWMoiVmdeMtMVuzip
MD5:	552658F56B3C1947CB8C4C31A209D1A2
SHA1:	4D81BC5C1D47EED0F839808A6284256475E7F117
SHA-256:	03FCD1441AB6EB11AD5E031386622C9EABB68EDF5C6AEBB73E43DFD2A3F217C5
SHA-512:	64EA57F01CCD7D5F481DB42DFDCC3643ECC97F159F90C04B3F6E74B7E9B4029F1DE7CBED8A9DC0B920338ACFE2C1845A64CB264D4CC6AEF93C56AB2156F2 316
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298160663251179","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_remov ed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_righ t":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_rep orting_timestamp":"13298160663247267"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"prod uct_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"0f4cafc2-cb8d-4b96-9034-7adc92b4ea3e"}},"intl":{"selected_lang uages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"A65FFE166A4986229EE CDE98A4723A16","engagement":{"schema_version":4}},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d18e047f-30fc-45b3-b16a-fb20ae6500b8.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):	16306
Entropy (8bit):	5.567978711129164
Encrypted:	false
SSDEEP:	384:+b3tqLlhXr1kXqKf/pUZNCgVLH2HfE4rU6hCA42:rLllr1kXqKf/pUZNCgVLH2HfjrUjAx
MD5:	2DD3B13D40C16C98650E23BC99034905
SHA1:	526FADC9F8773D282D6C9FCA3F2C43CFC36335E9
SHA-256:	AD3EC5A28CF5F73CE3E2876927663F874B9E4A02CD9E0E7373E188F28A4602B5
SHA-512:	3ABD86D05E8CB5F9B648295D91C6A0C6B0FF27DE70F9438F983E92F848AF4E42F5D413E4C8FBAB527025AF961B2EB6EF338E9ADB5706DA5B6EE8C4A6798C99 A5
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d1e89f4b-7e1d-413c-9fbd-a8f908ec9df5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000006.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//Tv:1qIFj
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1(
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

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
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Tv:1qIFj
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1(
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e4fd2138-f319-4a7a-9d0b-926a20d0a893.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):	16305
Entropy (8bit):	5.568018094309993
Encrypted:	false
SSDEEP:	384:+b3tdLlhXr1kXqKf/pUZNCgVLH2HfE4rUuhCA4Q:6Llr1kXqKf/pUZNCgVLH2HfjrU3A/
MD5:	35CEBF0C546BB70985F6A3CEBB3FB800
SHA1:	E6D9F86AEC73DD2C911A175DFD28EA3B1AB9ABBD
SHA-256:	9066845D5DD0EFD3891DF735268DE8D13287033AFDF4C2FC27736C5DD3642317
SHA-512:	ACFC236B4D33FAB5030FB14A0D3F17B98D2579A488C2631DD051562B541C00F1C5141FFC8957C253B04F320CE8FBD109451C147A20ED85F54046AF9FBE477CE
Malicious:	false
Reputation:	low

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298160661453186","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
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):	2.873140679513133
Encrypted:	false
SSDEEP:	3:mB4:mu
MD5:	3A0E5D4F452CF99191634D0FFAB744A0
SHA1:	F115BBB898EEFF640D8D19AD44A86C3FCDFFC0AD
SHA-256:	B9D528D3AE283039F4700C7E4E790744C58A26353A91B536DD91CBA4F648A35F
SHA-512:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528A
Malicious:	false
Reputation:	low
Preview:	92.0.4515.107

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	109763
Entropy (8bit):	6.065481482032037
Encrypted:	false
SSDEEP:	1536:lGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:l7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	4383B706518AA2B70528158AC26FBF6A
SHA1:	234E3F32F73D75633A125AE09088176F6C131A09
SHA-256:	A024DA314A790568D18A6E81A64E11CB2F1A94E2141DBAC3F598661651597BA9
SHA-512:	A78B00BA56509CD4D284E53FF1941B47ABCAA862CBBBCB6233189CAAA77FFC77A09FE1DE3F236F41DDB2D7A1E69BA180CB3EAAF710C0C032724C56B9F7CFD742
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2llZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.7572167763384026
Encrypted:	false
SSDEEP:	384:2rn3M2IyM7QjCUYOSNB9YT/g5qHfgluJnqOMgMC27MikxbvCjr2k8Q0eb5CfhgQw:4GgSjbo7/AV7Al+RHKCGdQF
MD5:	3E78A1C4ACBE4D45570F6548A10F8A2F
SHA1:	6698ABC23ED159C58653AE2C013A2D83B00CBFD4
SHA-256:	97D0793FBAE298FE73E1C0C4415233C25F322C4E9935F43AA0A67859D9970C58
SHA-512:	F39838D396EA5B5B2F491063368B21AAA138EA47BE0E8CFFB88FA9C01E9267FA1C3D95AD9D11CBCADBE18FAAD200406255B4CB5F0494B4D0CA8C81AB9B528E3C
Malicious:	false
Reputation:	low
Preview:	4}.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...m]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....m]8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\a2403b9b-7004-4a7a-95ee-55d7bfa2c7dc.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):	109763
Entropy (8bit):	6.065481482032037
Encrypted:	false
SSDEEP:	1536:lGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:l7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	4383B706518AA2B70528158AC26FBF6A
SHA1:	234E3F32F73D75633A125AE09088176F6C131A09
SHA-256:	A024DA314A790568D18A6E81A64E11CB2F1A94E2141DBAC3F598661651597BA9
SHA-512:	A78B00BA56509CD4D284E53FF1941B47ABCAA862CBBBCB6233189CAAA77FFC77A09FE1DE3F236F41DDB2D7A1E69BA180CB3EAAF710C0C032724C56B9F7CFD742
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2llZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\aae121d2-04ba-4014-985f-a6ecaec89d8f.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):	105156
Entropy (8bit):	6.034857498003486
Encrypted:	false
SSDEEP:	1536:rGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:r7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	BBDA26C36C4FC378FABDE7E696E82B42
SHA1:	BEDB2B549AA2A3E934EA44C7F1AE7FA3807FAA88
SHA-256:	25F2F7BB32C401085756EC74DE28BCDD12A3BEA7A119161EF889416AE092333E
SHA-512:	CD5F15B153229A85F978580B525848219FD56D9DAFF528C0056BE9EA844FC0E805683EDAFEA6011EA2A5001FE87BA8707651C072E7097C01458A0D0DF3496C3(

Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2llZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"last_statistics_update":"13298160661097806"},"profile":{"info_cache":{"Default":{"active_time":1653687062.997598,"avatar_icon":"chrome

C:\Users\user\AppData\Local\Google\Chrome\User Data\cbbf4a0d-adf6-4d91-ac4e-bba7a2dfb889.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):	109669
Entropy (8bit):	6.065193133645291
Encrypted:	false
SSDEEP:	1536:dGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:d7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	1F566330D7C8C2072DFEC5E764F7A094
SHA1:	E7C578908DB21772E37D6DB9A3EE4D61389357CD
SHA-256:	D466799A5C571540141376019C2FCA46B654E532C6051FA2AFF1B465FA7905B6
SHA-512:	455B8F006DCEFCC1BDB25763FE0FF6EFCC42570F61B6A103F6230E9085050BD197942106DF4849290F186BCF5740641A4ACB1CB072F2B61FCEB9F0E464D2A7C5
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2llZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\e710675e-db93-44e8-9cc9-1408be8d0606.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94804
Entropy (8bit):	3.756684141315602
Encrypted:	false
SSDEEP:	384:lrn3M2IyM7XCVNB9YT/g5qHfgluJnqOMgMC27MikxbvCjr2k00eb5CfhgQM0qz/T:BgSjgo7/AV7Al+RHKCGdQ1
MD5:	5498B27520B32F08772E0733F3E83A82
SHA1:	6F00092105BF911F5A28E03AB4E964D8E69AB708
SHA-256:	91D5241B81409E53D1154041AE0694ACFE5376FFB24C6E25DB276105D21996C6
SHA-512:	5C2BCEFC8723FF8998FB7A697A86D1EE279F797D99104E2D297ED7A76C516A82DD6880010F45297B159C686CA073E96EBAA1C9F2291CA96769EB354800E9F70
Malicious:	false
Reputation:	low
Preview:	Pr.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...m]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....m]8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\ee67e556-b169-4ab0-9a9f-4ef379a7a09a.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):	105268
Entropy (8bit):	6.035753375418359
Encrypted:	false
SSDEEP:	1536:dGqu0XGM1CCHq42oiVfqchXJlAL3VYhLoAwgJyvjwfzhCsjUtjOjXMWw:d7XTCCHq44gMY3VYhtyUfdRgyjXs
MD5:	7EE59BB83670681BAA7B140EA47D2609
SHA1:	798AB5E71C69751879E1D2E435DAF4E3CE6DB766
SHA-256:	5653DD43D356DC20C4BCAD549624651B5ACC03F9A13B35E4C13B77B629F18E1C

SHA-512:	7FD23B58A45B090CA6811CC5B9E577BF44DAAB5285705C5AB433CC96A5CAD36D6ADCC95AB17C635AFB1FA5CF68C8B78F8FACFF062E63D5DF4A40A7C7D8C8727E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65368706422438e+12,"network":1.653654666e+12,"ticks":171137676.0,"uncertainty":3041156.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187421231"},"policy":{"last_statistics_update":"1329816066109780

C:\Users\user\AppData\Local\Temp\0e479653-eaf5-46cd-9f7a-a2120da53793.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\183bb6f2-8ab3-49e9-b97c-e56322ef6ad2.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	101891
Entropy (8bit):	**7.9971613680976565**
Encrypted:	**true**
SSDEEP:	3072:Xs4McBbhITdJs7qJdKpJcKdNd+HyEzEcl6dr:X7Bb4dJsOPKpJrv4tTl6dr
MD5:	173CA02E5B06065771DEB2F28E4E5A9E
SHA1:	20F1774FB280C94C13082A255C27D7A786EFD5C7
SHA-256:	634557AE2916F2FAA0CBF2557F8F96E26845ABE94D2784FD73B169EC5618B186
SHA-512:	D947E3ED56BE1F3C668943E8F066F39650D2E0D76BF64BAD167E100B8B1066B88D8E851346AFBD9777E90445F41C5108A0A2F1514A3F28F02D4EC39978121E71
Malicious:	false
Reputation:	low
Preview:	.....{..0.....&xqH.....zyIBv9....=...+.....I6....3#.l.@..9.s].W7...h4..H...7.^.....Bg.....`.;.S...P.....z.3.....9~.P..{..-.z.....b.:.....>..'....I8.....'v.M'E.?bA...N8.'.8I.._...<v&.pT{.L'Ne...#.S!].T.-+...r)5.j.U.8q....X..VPo.....F.o..A.~~.?.w.....eNJ..a)....i....:?._^..v.<=ei...i.....Q...8k.....~j.c.W.....~...Q.yq..^9..z.....S..b.E..L3|.9S.pa...a....5...J.\.2l..s..4.....S.u..o.|.Q.K.0.=.....0....xj.4....Mie..C..3..... .....WN.....4Vs.B..N.bD...VK%...mb...{{....pd..7..G.....}.J;"..4,.....A.R|0d..)..M.....;;.8.h.C.u..pkM..Z@.....r..U....H..],..l:~p..8`....3....5.*.t../S{.{`.^kB=f.....ZR..L.$t..D%I..xB../.{rb..h8.!.....Z.0.....{PuK%Vv...RR.*.....j.vw.[B..$..|&..eZEW.Z[&..d>.o.....@..t.z.O.12C.....Kk..oS.[.0.M...<.zq#*g.r....."0+.[.....Tb.E....F...U..U0...G.....t!.+...&K.@.N.#R.]...+.;.M[..x,...J.l.....&y.n.....j>..0.|W.+.S.0X.S.E..L....R.....W.u.g.S.&^.g..N/..

C:\Users\user\AppData\Local\Temp\18622864-0537-4583-84fc-877c68bf9f16.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	3110
Entropy (8bit):	7.933903341619943
Encrypted:	false
SSDEEP:	96:0MWjN1CDThRYxENcEvyGF/8WAr6Fv9MFghzqSl:0MWjN1gRYavR8WjMFQzqSl
MD5:	A83A2746B84F1CF573B02965B72ED592
SHA1:	85CC572D6F90029EB99AAFA56297D1BCA494313A
SHA-256:	DF4B53C1C7C48E80753D4945E6EC7847084F51BF57F0ED9D341326C74651D6EC
SHA-512:	C287F479EF572A06FF191C4E9A8A718507C97A2A45CB265D7DC65DD7922B80D36CE7660EC5D7EA9F3D1F1EF71C51C3E4F3D7973754F97A89B4F14D1B1FDE70E
Malicious:	false

Reputation:	low
Preview:	.....ko.7.....J...../..v..... ....zE.\+.T..f..%wW.$.....p8/.....z..\|a...}.#y.`.l..7Kr..T:'.UE,.&.i..Y.....h...B.....gJ....%.\.?.f]1R..@3.jHA..eHi&.Q..`....g.__?'3^...@~X..a8..... .....UN..%...&.F..K19".Y:.).L.L..WL..xxD>.P@ ...&'..j..)%.Q\..<!.3n.<#....;.gd2.LZ....x.m&.e.`&;.KX..."...<G....8.R.jsd....g.)..?.$=UVT...#.+g.!.....R..1..#D.k...3.Bj3iT.....*.M. .L....}..S.K.....zi..n.A{.....n..o.0j..q...w...3.7.N..].>...zK..sr1#.d..Tk..ckB...<....j.a.M1oe.9.jIQ.y+...6.....]....v.X.....q.....a>...2`.WV.v.'..~.3*.4.'8...hkT.H..9SOIF.%...;n.6.U.... i!...2v.9/.;.....R..8.(..L.b....aY2ps% ."...x.V..Y[.h.....^.....U.....p.'.&m.....6..%pWE....:..o.k...<.....5....j.I...*9...f..3.....-..0..D;.....*S.td/.....^_.v.)y ..Uf..q>.v2...0....o....Y %5;.5fn..{.....p_.....B..V.....D.Y.l....q 3...sm.b..!..E....a. &.w.-.s..>..M_...`.0..k.!<SH...9$.....V.\A$..}..8....#`...,...3.W..k...\..xH.1).~.Y.L1.O...\.....k.....s..i+.....).0

C:\Users\user\AppData\Local\Temp\4c2a4d8d-a8ae-41a8-b2ba-3b26fbbdd479.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	5168
Entropy (8bit):	7.956694278195136
Encrypted:	false
SSDEEP:	96:HLCk5oNLp/f4PvzusAnSWuaGqLiWuGVaNhZMHd0NJHp9873PDqQ7:H2vUv7AnSKnaNPM+4uA
MD5:	3E5CCD9B583763AF68E28C5101373167
SHA1:	2005CDC0A8070B65E321A197D576698ECC267496
SHA-256:	41412C0863920BA95E9FDBD3AF000CBE926A73C078997A233DF55379A5C4D274
SHA-512:	04BF4F7320326B085C40527797577D8770A30A1ED24A8587A000A5AE1D8F39E0B7F187DB14603295AC7A2901A4698683CC3BED2C2611539293A1927AB31BEAE1
Malicious:	false
Reputation:	low
Preview:	.....[ks.8..._.....#.,.G..8.;.55;.%..&5$e.....)..d._..%.....s.....+..Uv}...]rq.....luK.).zJh..3.&..Uu...W...s.H. .MV..\U3Ef.\.\|...TU.9.z)I...u.+.g3U`Zs.6d...JiJ.rU.IV.".'L\|8 .d..j.J..q.....O."..<,...n...~\|E.dV.u.O..'"...e.uyJ?..?]~.?.....M.,.7...j.,.fz].. >+o.gz....<^(5.Jg_.Ap.U.i.....?.8.....,.*.*./.iQ..8.....A.DO/....?.~..N.~a.-..g.N~.....o.^...L.mW.]:{..... ./.....[VkTu[wki.gK...;-.<...\.".3]..}V...)9i.V.P="m?.....V.i...7..S.U.d..(..\....g....bU.....}.....P9$.A...N..ckV..Qz..A....7..{pd.f.7....}6on.....7J;...Y..l>W...H.Z.....j..... Wk9vj+V.W.zAm.....P.oYo..|.....}.g.^.p...Z....l%cT|LN3..H.....{...~.J.%.!k.(.)..."....q.%.V.. d..MZ.`.....o..m3....1.../..jeH.....Q....X...j..o..|.o.r..nVw._...9 .....o...l....!...{....xU5.. }.x.I..3.vT%z.k..o.....^.S*.t(....+r\.u<...G.`.....g...r..?...}7.=.....c~.F.e..w.v$sC/.B.p.D~..J...:....7Vl3w...s.-"....]+..KO.~....%.I..?.&.o...\?.9..

C:\Users\user\AppData\Local\Temp\7668_1088337683_metadata\verified_contents.json

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):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 02
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIs nJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1l4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_pnacl_json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E

Malicious:	false
Reputation:	low
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<.....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl- clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_crtend_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low

Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@....`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... ... .@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@. A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E

SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `...;...|.....4...x..#...-...4I..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:....D...K...T ...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....__pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t''..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+I
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62 CFC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `.....__pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native _client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU- stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE

SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....!.....!.....'.....G.....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i.....0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."..."..."..."......@.....`..... ...@..`..... ...@..`..... ...@..`..... ...@..`.....`... ...@..`.....`..`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H...F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\7668_1088337683_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`.. ...@...@.....@.....@.....Y@.....p.....@.....?.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\7668_1088337683\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\7668_1088337683\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F

SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",.. "name": "PNaCl Translator Multi-CRX",.. "manifest_version": 2,.. "minimum_chrome_version": "30.0.0.0",.. "version": "0.57.44.2492",.. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\a0f69cf9-0a73-4e80-84ef-2c07da713d66.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	30948
Entropy (8bit):	**7.99105089802474**
Encrypted:	**true**
SSDEEP:	768:jElAfPryn5QzShaPuChbhFbHRu/llKGr7J9FwyllWg+S3:jElAfzyneSMPuKbvzUllKGzFDOWgv
MD5:	7F0FCE2F184F63FED8E9929FB106C282
SHA1:	0582EB5BFC7FCCCC1C77A860F00E351E61F5DC67
SHA-256:	7C33F333216849E50AFC9550DA7DA4450D221B837340716ACCEE3766FFD4A62B
SHA-512:	AD1CD5B804C08C4C25BD6F97153D3371156848A83682DF1829B0B113B60ED0B01D67B5CD737CB414C8B825E12C7E0D6B5F9B338F4AF7FC82BE8AAF4CA8E279BA
Malicious:	false
Reputation:	low
Preview:	.....y..../...*D4e.sH.v.{.....mv9MR...&..b.`.P."........r.....X...9s.s..w..;...>.}8...O.ep....O.]...$KO.tu...2?Yfi.'ove..T.....(.N7.R..<yr....t..}).....>[.....*."....../7.j.....#.n..e1..Fr.....j5xH.~.*...yvw....y.....vI.....IWT..)...|..\..<=.V.C..}.fF..T.....~.~..:).....i...2./D.}...]..<+3T..Z.Q9*0.....3..7.e..p.:..-.P..n.}j....U...."...|Gm...AdQ:*...gz%n..:...K.o[..."..n...(V..A...U.D.~x.Q..X.tw.F..,.Q...k.9.w.....2....t.....XF....E./...Hu.%..]....7.T...X.\$4.~.....`..e\....}.X...`A...J.....k...$IO..OS:...=...R...q.....FE.H.)M..WX/.....6..._..ry..J..`.q.'....x^..[r..Z.Y:..0..g.y....#.1.'...F7M.6...S....7.To.G.... `#.....-."...^....;..8..{.6VhL?%uU...K....O9.`Y....b.5.,zP.+\..!.1wK.j.P].....jW.!.j...i3.v.<..n.P..g....~.x..z.8...2^..U.f.bt#.+.U..N.....!.[.!#.C.A.xy.....p...n.mU,.....=.....h .ME..T/....IT\h,.U.....(.U ...Tf.?Zd8.2.V.....*..../....Oyh.j.._.I.k..u...).3.r.3...j.....O....+],...

C:\Users\user\AppData\Local\Temp\b8724d3c-a4d1-4bd6-b081-537cfbebc815.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	28748
Entropy (8bit):	**7.9918576871001425**
Encrypted:	**true**
SSDEEP:	384:SU7ZPeF1W3JgUrqaO/8dOcbwy59NjS5BMYGYycIfPhrVx2NtsEeSeFzVXe/rxd:H7peFkZL9RZSz3gnhhGcpXetd
MD5:	2A37AD0EC191D53104BB46953AC6C43C
SHA1:	FD23FFC5B7E4A6B45FBD88A486D15FAA51DC07AE
SHA-256:	51F075EB69486CB23B32A0776782B4A1B2AF204429AB94510469E02B115E56CC
SHA-512:	AEB91CB7902A800D7B0C43627EC2B52121BC41BA29A1B6ABEDBFCFA4802254A0594ED239EA7A3F8D40241E43D436428D1E4AC117BD97269D78460F82F9BDCF68
Malicious:	false
Reputation:	low
Preview:	.....Zms.6..._..p..[.(.b[...M....N{..t ...S.....v...H.q.g:....]...p..6I8_d...C.\p.X$.2.p.g.8I}8.".D)$<..O...}.J9.3..a.i.'...x.....5O...x.....I.M.!.'\.l.2.0.cN.fq....\.....7..,.....>.p...w&.KS.....(O.V>.....O.r..V~J.`....U(..Y..MIy..w..g0e.....D.,L..y..N.+..._....O.h.]...V....r.....O.|.:....Li..>COy.....N.h.....R....Q%.,Xr.y...G8=.A....!8(..L....c....sA....t.Vl:...v...G;...^.l...#.t.>...k..d..kr...B.....Pb.0*..!..;9.....:~....j;...j.*O..!B.....?....^.]...;...[.g.B...%..'.7;.9.>..gP. p8...:.5l.Y.....Jp..R,.?..b..8O.....h.X(..G.).Cz.C..%....x.ET.....AEi.../..0.. ....k.*t..wl..e...H.i.F.....?.....z...?.....(../.O..R.?.4..7...j ..Q.....l..ob!..A..j...@..!).....K...MW.U.N.....W..Bh'8.'.y....Y.[o...PI..W.*...i...r.e..=.k^.WC..Uy.j..687^.z.#u5.4O.....-j.j3..L.1..F...8.....@l.9.c.aGC.R.&..j.Q-av?...[4.E..T8....u..+9.<.n.Qw.D..N..S..3.D..... .%C.j.7.Y.s(.0wq.ZI.#"#..[K.GJ ....4.....?

C:\Users\user\AppData\Local\Temp\db51accb-af0b-4ca2-b5f5-32b7f2cf8aa1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82

SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BED8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "message": "......... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators

Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYlAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlakozzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223

Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....".. },.. "app_name": {.. "message": "Chrome ....".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..... ".. },.. "iap_unavailable": {.. "message": "..... ".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C

SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	501
Entropy (8bit):	4.804937629013952
Encrypted:	false
SSDEEP:	12:YGGYpB928UZjdyE9iDCiop8682fURHWO/NrnLAOK:YHYpXK/iOiop8NFHWOFvAOK
MD5:	8F0168B9A546D5A99FD8A262C975C80E
SHA1:	B0718071BD0B7251D4459E9C87DF50C14622FBD6
SHA-256:	F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F
SHA-512:	A1191CDC496DDD7470BDCFAF186BB9488767159E0CA6A6242D195FA3351704DC8F8BBD03DBEE57D37BBD897C9E8D14B7325FB37D58AC80DEC0F972FF89375B8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er utilgjengelig for \u00f8yeblikket."},"craw_connect_to_network":{"message":"Du m\u00e5 koble til et nettverk."},"app_name":{"message":"Chrome Nettmarked-betalinger"},"app_description":{"message":"Chrome Nettmarked-betalinger"},"iap_unavailable":{"message":"Betaling i app er ikke tilgjengelig for \u00f8yeblikket."},"please_sign_in":{"message":"Du m\u00e5 logge p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8AA7
Malicious:	false

Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "craw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir7668_510292319\CRX_INSTALL_locales\sk\messages.json

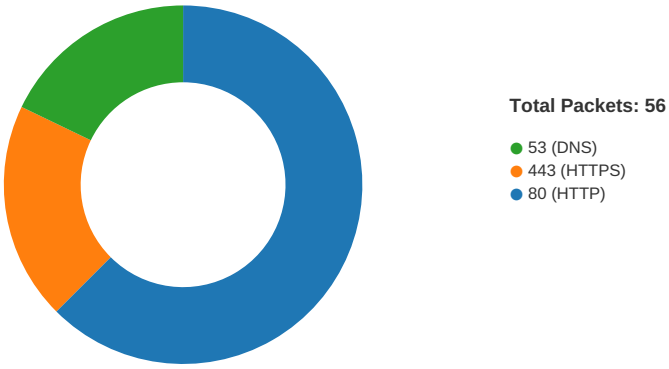
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:31:05.979557991 CEST	54558	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:05.980206966 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:05.980246067 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:05.980315924 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:05.981317043 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:05.982268095 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:05.982295036 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.048593998 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.128453970 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.148009062 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.148194075 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.148907900 CEST	80	54558	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.149068117 CEST	54558	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.195516109 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.195542097 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.196275949 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.199950933 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.200026989 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.200043917 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.305916071 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.306094885 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.306128979 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.306490898 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.356869936 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.357024908 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.357045889 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.357079983 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.357135057 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.362968922 CEST	80	52791	199.34.228.55	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:31:06.364705086 CEST	57477	443	192.168.2.3	142.250.185.141
May 27, 2022 14:31:06.364742994 CEST	443	57477	142.250.185.141	192.168.2.3
May 27, 2022 14:31:06.395495892 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395543098 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395581961 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395617962 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395654917 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395684958 CEST	80	52791	199.34.228.55	192.168.2.3
May 27, 2022 14:31:06.395724058 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.395792007 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.395802021 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.590301037 CEST	52791	80	192.168.2.3	199.34.228.55
May 27, 2022 14:31:06.627841949 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.628130913 CEST	54918	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.628695965 CEST	59531	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.629060984 CEST	58024	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.629606009 CEST	56565	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.643666983 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.643707991 CEST	80	54918	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.643825054 CEST	54918	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.643835068 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644011974 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644083977 CEST	80	59531	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.644171953 CEST	59531	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644438982 CEST	54918	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644556046 CEST	80	58024	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.644629955 CEST	59531	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644643068 CEST	58024	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.644948959 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.645047903 CEST	56565	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.645133018 CEST	58024	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.645284891 CEST	56565	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.659518957 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.659873009 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.659914970 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.659997940 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660037994 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660042048 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660077095 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660094023 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660145044 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660187960 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660223007 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660227060 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660264015 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660290003 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660294056 CEST	80	54918	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660332918 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660372019 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660393000 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660410881 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660440922 CEST	80	54918	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660480022 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660485983 CEST	80	54918	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660547972 CEST	54918	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660554886 CEST	80	59531	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660593033 CEST	80	59531	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660644054 CEST	80	59531	151.101.1.46	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:31:06.660682917 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660695076 CEST	59531	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660722971 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660773993 CEST	54965	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.660778999 CEST	80	54965	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660959959 CEST	80	58024	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.660988092 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.661016941 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.661159992 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.661201954 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.661231995 CEST	56565	80	192.168.2.3	151.101.1.46
May 27, 2022 14:31:06.661242008 CEST	80	56565	151.101.1.46	192.168.2.3
May 27, 2022 14:31:06.661303043 CEST	56565	80	192.168.2.3	151.101.1.46

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:31:05.883194923 CEST	65210	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:05.884046078 CEST	53720	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:05.884350061 CEST	61873	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:05.900770903 CEST	53	65210	1.1.1.1	192.168.2.3
May 27, 2022 14:31:05.901628971 CEST	53	61873	1.1.1.1	192.168.2.3
May 27, 2022 14:31:05.911932945 CEST	53	53720	1.1.1.1	192.168.2.3
May 27, 2022 14:31:06.577806950 CEST	57760	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:06.596599102 CEST	53	57760	1.1.1.1	192.168.2.3
May 27, 2022 14:31:07.268548012 CEST	49313	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:07.307064056 CEST	53	49313	1.1.1.1	192.168.2.3
May 27, 2022 14:31:07.551073074 CEST	64492	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:07.568718910 CEST	53	64492	1.1.1.1	192.168.2.3
May 27, 2022 14:31:07.782273054 CEST	53010	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:07.814630032 CEST	53	53010	1.1.1.1	192.168.2.3
May 27, 2022 14:31:09.287587881 CEST	54203	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:09.305732965 CEST	53	54203	1.1.1.1	192.168.2.3
May 27, 2022 14:31:10.628652096 CEST	64626	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:10.648143053 CEST	53	64626	1.1.1.1	192.168.2.3
May 27, 2022 14:31:10.704484940 CEST	57267	53	192.168.2.3	1.1.1.1
May 27, 2022 14:31:10.732525110 CEST	53	57267	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 14:31:05.883194923 CEST	192.168.2.3	1.1.1.1	0x57b5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:05.884046078 CEST	192.168.2.3	1.1.1.1	0xecb1	Standard query (0)	document--1111011111.company.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:05.884350061 CEST	192.168.2.3	1.1.1.1	0x901b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.577806950 CEST	192.168.2.3	1.1.1.1	0xa45f	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.268548012 CEST	192.168.2.3	1.1.1.1	0x7c1e	Standard query (0)	www.company.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.551073074 CEST	192.168.2.3	1.1.1.1	0x4edf	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.782273054 CEST	192.168.2.3	1.1.1.1	0xd4fd	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:09.287587881 CEST	192.168.2.3	1.1.1.1	0xf43	Standard query (0)	www.weebly.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:10.628652096 CEST	192.168.2.3	1.1.1.1	0xf66d	Standard query (0)	www.weebly.com	A (IP address)	IN (0x0001)
May 27, 2022 14:31:10.704484940 CEST	192.168.2.3	1.1.1.1	0x29c8	Standard query (0)	document--1111011111.company.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 14:31:05.900770903 CEST	1.1.1.1	192.168.2.3	0x57b5	No error (0)	accounts.google.com		142.250.185.141	A (IP address)	IN (0x0001)
May 27, 2022 14:31:05.901628971 CEST	1.1.1.1	192.168.2.3	0x901b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:05.901628971 CEST	1.1.1.1	192.168.2.3	0x901b	No error (0)	clients.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)
May 27, 2022 14:31:05.911932945 CEST	1.1.1.1	192.168.2.3	0xecb1	No error (0)	document--1111011111.company.com		199.34.228.55	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.596599102 CEST	1.1.1.1	192.168.2.3	0xa45f	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:06.596599102 CEST	1.1.1.1	192.168.2.3	0xa45f	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.596599102 CEST	1.1.1.1	192.168.2.3	0xa45f	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.596599102 CEST	1.1.1.1	192.168.2.3	0xa45f	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.596599102 CEST	1.1.1.1	192.168.2.3	0xa45f	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
May 27, 2022 14:31:06.860903025 CEST	1.1.1.1	192.168.2.3	0x7a3d	No error (0)	gstaticadssl.l.google.com		142.250.185.99	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.307064056 CEST	1.1.1.1	192.168.2.3	0x7c1e	No error (0)	www.company.com	company.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:07.307064056 CEST	1.1.1.1	192.168.2.3	0x7c1e	No error (0)	company.com		35.71.162.193	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.307064056 CEST	1.1.1.1	192.168.2.3	0x7c1e	No error (0)	company.com		52.223.45.27	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.542534113 CEST	1.1.1.1	192.168.2.3	0x40fe	No error (0)	www-google-analytics.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.568718910 CEST	1.1.1.1	192.168.2.3	0x4edf	No error (0)	www.google.com		142.251.37.100	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.814630032 CEST	1.1.1.1	192.168.2.3	0xd4fd	No error (0)	ec.editmysite.com	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:07.814630032 CEST	1.1.1.1	192.168.2.3	0xd4fd	No error (0)	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		52.25.131.159	A (IP address)	IN (0x0001)
May 27, 2022 14:31:07.814630032 CEST	1.1.1.1	192.168.2.3	0xd4fd	No error (0)	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		52.41.81.16	A (IP address)	IN (0x0001)
May 27, 2022 14:31:09.305732965 CEST	1.1.1.1	192.168.2.3	0xf43	No error (0)	www.weebly.com	weebly.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:09.305732965 CEST	1.1.1.1	192.168.2.3	0xf43	No error (0)	weebly.com		74.115.50.110	A (IP address)	IN (0x0001)
May 27, 2022 14:31:09.305732965 CEST	1.1.1.1	192.168.2.3	0xf43	No error (0)	weebly.com		74.115.50.109	A (IP address)	IN (0x0001)
May 27, 2022 14:31:10.648143053 CEST	1.1.1.1	192.168.2.3	0xf66d	No error (0)	www.weebly.com	weebly.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 14:31:10.648143053 CEST	1.1.1.1	192.168.2.3	0xf66d	No error (0)	weebly.com		74.115.50.109	A (IP address)	IN (0x0001)
May 27, 2022 14:31:10.648143053 CEST	1.1.1.1	192.168.2.3	0xf66d	No error (0)	weebly.com		74.115.50.110	A (IP address)	IN (0x0001)
May 27, 2022 14:31:10.732525110 CEST	1.1.1.1	192.168.2.3	0x29c8	No error (0)	document--1111011111.company.com		199.34.228.55	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- document--1111011111.company.com
  - www.google.com
  - cdn2.editmysite.com
  - ec.editmysite.com
  - www.weebly.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	57477	142.250.185.141	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	54599	142.251.37.100	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49266	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.252418041 CEST	1087	OUT	GET /files/theme/fonts/627fbb5a-3bae-4cd9-b617-2f923e29d55e.woff2?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.424474955 CEST	1205	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff2 Content-Length: 18761 Connection: keep-alive Last-Modified: Fri, 30 Aug 2019 08:25:04 GMT x-rgw-object-type: Normal ETag: "88f6742055e6eecac07f296cbd45214b" x-amz-request-id: tx000000000000000b987de-0061a70616-a9f4046-sfo1 X-Storage-Bucket: z663f X-Storage-Object: 663f4c799beff8f8dfa2ac950ce27ed4fcf8acc11ac5ec04f2bc6574a304730e X-Host: blu40.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 32 00 01 00 00 00 00 49 48 00 10 00 00 00 00 bf d0 00 00 48 e9 00 02 19 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b bd 54 06 60 16 8b 60 00 81 4c 08 83 64 09 92 50 11 08 0a 81 d9 60 81 b4 64 01 36 02 24 03 86 78 0b 86 7c 00 04 20 05 ae 07 07 20 0c 84 2f 1b c7 a8 15 6c 5b d6 b2 db 81 16 fd fc ef 1e 56 b0 5b d8 c0 79 0c 1e b8 ea ce 15 d3 6d c6 21 a8 9b 95 08 39 eb ed a3 64 ff 7f 83 28 43 54 76 02 bc bb 80 b6 20 64 b6 ce 2a 54 7b 3d 6b ff 6e 18 0e ce b9 80 09 90 00 1b 00 f0 b5 e0 05 68 00 c0 d3 ef 00 71 61 8c df 63 06 00 e0 31 06 e0 30 30 7e 53 68 80 84 cb 6a 82 49 96 32 cb 03 30 00 f1 b2 10 00 24 80 15 ea df 65 84 aa 41 83 62 7c 01 12 20 01 92 84 00 be 00 00 00 2b 6c 5c 03 84 59 8a 8e 9e 50 f4 fb 65 3d f3 36 f8 77 c3 ac 80 84 64 12 06 55 22 4c 84 4b 45 d8 28 7b 2c d4 69 20 7b fa a2 67 80 9f 5b 3f 36 a2 37 58 e5 5b 05 ab a0 d6 c4 a2 d8 46 4e 60 84 01 18 80 70 46 92 46 05 77 62 e4 3f 31 12 03 ab ee 04 1b 4f bf 9e 8a 91 e8 29 3e af 2e 95 42 e8 0b 3a d5 22 3f 95 5d c6 b3 e5 80 0b 47 7d cf 2a ca ad f3 0e a6 cc 45 50 60 98 3b 8c df 9d ee 3a 01 4d c0 73 b7 4e 44 87 6d 7e 1f 9f c4 81 26 f0 28 5a 95 f5 ef 7a 3f ac 09 53 ce 7d 4f 14 09 cb 2e 0b bb 90 15 cc a0 f2 10 e3 3d ef c3 8f b9 4e 6d ec 0a e7 06 de 8c 33 16 fd 65 8b ea 4a ab d2 8f 01 dd d6 53 98 7a 60 01 05 16 79 18 7a 9e 27 01 75 ff ab d3 24 c3 c1 ff f6 11 8d 37 02 ce 00 24 e9 27 56 b0 4e ab b6 6e df 21 d9 6b bc 16 80 6f 02 c0 8d 02 7c a2 4d 0d eb 0f ae 7b 55 55 48 99 89 7e b7 6f bc 66 68 89 b8 01 8b aa d6 30 dd 56 da 17 6c e9 8a 7d d7 bd 39 bd ce 10 09 49 48 28 42 01 41 29 f2 b7 6d fe 6d 6c 90 e6 01 77 24 b9 7e a4 a1 08 d2 0a 87 f1 ef dd ca f6 73 71 6d d3 a6 da a2 8c 69 d7 3f d8 08 70 c6 fe 08 70 ee 5c 5c 57 b9 cc 10 13 87 28 44 97 28 17 dd 4b bc 13 ef 44 db 14 9d 49 d1 a4 68 d3 96 a2 f0 bd bf f7 f7 fa 64 42 fc 36 1a 85 77 fb 1e ea ca d0 da 10 84 79 a0 70 3c 74 b5 12 84 44 7e 59 7d 69 ea 4b 3b 31 9b 10 e6 49 be 73 e4 95 5e c7 1c 80 79 e8 e4 a4 63 6d c0 0b 38 39 b3 1f 5a 56 ff ff 4d 4d 5b 60 25 d1 29 84 a2 4e b1 72 d1 b9 68 5d bd fb ff 9f c1 bf 33 e0 70 3e c2 ee 7c 70 03 86 d8 80 d9 5d cb 18 52 81 50 1c 80 b4 0f 48 2a 72 75 7c c8 75 0c 95 ac ca ee 08 e5 5c ba 29 5d ca 9d 8e 4b 97 ee 4a 51 ff 71 61 9c 8a c8 02 e1 8e f5 ab d0 b7 3b 78 f3 67 ff d2 06 c3 52 e6 f8 4f 47 3d 72 af 02 e9 f6 b6 85 50 d0 dd f0 3f 2f 11 d6 fd 64 0d ce fb 95 d2 fb 49 11 91 20 21 88 38 29 6f f2 88 9a c9 98 bd c7 5b 7c 88 48 91 d0 77 11 09 21 94 12 c4 e5 30 5b 68 6f fb 8f a0 ba a9 12 12 8e 31 b5 37 ab 33 4d fb 49 47 3a 35 2e 50 c6 31 4e 40 Data Ascii: wOF2IHHT``LdP`d6$x\|  /l[V[ym!9d(CTv d*T{=knhqac100~ShjI20$eAb| +l\YPe=6wdU"LKE({,i {g[?67X[FN`pFFw b?1O}>.B:"?]G}*EP`;:MsNDm~&(Zz?S}O.=Nm3eJSz`yz'u7'VNn!ko|M{UUH~ofh0Vl}9IH(BA)mmlw$~sqmi?pp\\W(D(KD IhdB6wyp<tD~Y}iK;1Is^ycm89ZVMM[`%)Nrh]3p>|p]RPH*ru|u\)]KJQqa;xgROG=rP?/dI !8)o[|Hw!0[ho173MIG:5.P1N@
May 27, 2022 14:31:07.885855913 CEST	1379	OUT	GET /files/theme/fonts/fa19948e-5e38-4909-b31e-41acd170d6f2.woff?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.1653687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.057981968 CEST	1456	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff Content-Length: 24664 Connection: keep-alive Last-Modified: Wed, 11 Dec 2019 02:22:43 GMT ETag: "921592aa07f703ed55036aed49590184" x-amz-request-id: tx00000000000000002c3a3-00615f8e31-1ff7556-las X-Storage-Bucket: z304f X-Storage-Object: 304fdd345e780b7dbb6c6e6bc39d24e906e40ac2a618bc78ff81abc769f9b4ae X-Host: blu46.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 46 00 01 00 00 00 00 60 57 00 10 00 00 00 00 cc 2c 00 01 00 00 00 00 59 6c 00 00 06 eb 00 00 0d 7f 00 00 00 00 00 00 00 00 47 50 4f 53 00 00 01 6c 00 00 06 c3 00 00 1e bc fe b3 03 03 4f 53 2f 32 00 00 08 30 00 00 00 57 00 00 00 60 65 96 fd c3 56 44 4d 58 00 00 08 88 00 00 03 78 00 00 05 e0 6e 58 75 d4 63 6d 61 70 00 00 0c 00 00 00 00 98 00 00 00 cc 90 e6 b0 e3 63 76 74 20 00 00 0c 98 00 00 00 4b 00 00 01 e4 06 18 05 69 66 70 67 6d 00 00 0c e4 00 00 05 2b 00 00 09 50 a1 cc 85 0f 67 61 73 70 00 00 12 10 00 00 00 08 00 00 00 08 ff ff 00 04 67 6c 79 66 00 00 12 18 00 00 38 79 00 00 78 d8 90 20 03 06 68 65 61 64 00 00 4a 94 00 00 00 36 00 00 00 36 f3 a6 d3 c2 68 68 65 61 00 00 4a cc 00 00 00 1f 00 00 00 24 07 68 07 bb 68 6d 74 78 00 00 4a ec 00 00 01 fc 00 00 03 78 cc f6 37 96 6c 6f 63 61 00 00 4c e8 00 00 02 5a 00 00 03 7c 00 31 2c bc 6d 61 78 70 00 00 4f 44 00 00 00 20 00 00 00 20 02 6e 01 01 6e 61 6d 65 00 00 4f 64 00 00 08 27 00 00 17 81 64 76 02 a6 70 6f 73 74 00 00 57 8c 00 00 00 13 00 00 00 20 ff 9f 00 32 70 72 65 70 00 00 57 a0 00 00 01 ca 00 00 02 2f e3 0f 5b e5 78 9c c5 59 59 6c 54 55 18 fe ba d2 96 a1 d3 76 28 14 4a b1 b4 43 4b 5b ba 30 85 d2 42 25 62 ca 22 9b b1 ec 82 06 c1 e5 41 c1 c6 18 9f e4 01 5e 1c 8d be 98 3e 10 4c 80 18 53 91 20 89 95 87 09 26 20 52 04 79 b0 c3 62 63 a0 26 a6 4f 93 98 34 26 4e 4c ec cb f1 3b ff 3d b7 33 d3 59 19 da e1 7e b9 e7 de 39 cb bf 7d ff 3d 4b 8b 2c 00 45 78 1d 97 90 f5 ce 6b ef 1f 43 01 6a 90 b7 7e e3 d6 6a 34 f6 6c d8 5d 0d cf 8e 6d 3d d5 58 d3 fb e2 f6 6a 3c bf ab 97 f5 5b 00 a5 a0 c7 59 cf 2c f3 cc 36 cf 1c f3 cc 35 cf 3c e4 bf fd c6 7b c7 50 27 e5 72 29 3d 52 76 4a b9 4e ca 1e 8a 13 99 09 4b 2d b5 90 cf 6c da 5c 66 e9 44 89 79 de e3 b3 45 6b 65 cb 1e f4 e1 03 7c c8 fb 24 3e c5 e7 c4 29 9c c1 57 f4 f 2 32 ae 60 88 e5 19 f6 2e 83 13 f5 68 80 07 ed 58 8d 4e 74 61 0d ba 71 1c c3 f0 e3 2e e5 dd c7 03 3c 42 3e 8e 2a 3f 86 9 5 0f 7e de f7 d4 45 dc e7 fd 90 75 59 f0 aa 11 29 bd 52 fa 69 87 7e bf a1 c6 e4 f7 9f 52 0e 49 79 95 a5 53 8d b2 87 53 0d f0 f7 80 fc d6 e5 7e 15 9c ac f5 4a ad 17 d9 15 5e ed c9 82 6d 95 6e 74 d0 2a 50 62 37 32 7c 3d 0d 9d a2 77 94 9a 33 7b b5 65 58 9f b9 d4 98 f2 ab 80 1a 57 81 8c ea 1c 52 23 d4 3a 94 51 9d a3 f4 32 f3 7e ea d8 8e f2 ab cb 80 b6 a7 f2 ad 64 3e 6f 1d 96 9f ca c7 cc 1d d5 39 c4 18 07 39 83 cd e0 c5 f9 d0 ba ca 2c 70 a6 84 b1 61 8c 99 3c 89 8c d8 30 93 3a fa cd cb d3 f4 d3 d6 e9 e7 d7 a3 d9 b5 ef 20 57 b7 e9 ba 2a c2 72 28 90 99 1c b2 2e ce 06 43 8c 65 d0 78 34 a1 26 a2 7b 18 df f5 3d a8 7e 8d ee 11 21 6d 5c f7 4f aa 55 64 58 fe c9 98 a0 35 4a d7 d8 f7 54 1b e2 ca 8a d1 3f a2 dd cc ea cc 93 Data Ascii: wOFF`W,YlGPOSlOS/20W`eVDMXxnXucmapcvt Kifpgm+Pgaspglyf8yx headJ66hheaJ$hhmtxJx7locaLZ\|1, maxpOD nnameOd'dvpostW 2prepW/[xYYlTUv(JCK[0B%b"A^>LS & Rybc&O4&NL;=3Y~9}=K,ExkCj~j4l]m=Xj<[Y,65<{P 'r)=RvJNK-l\fDyEke\|$>)W2`.hXNtaq.<B>*?~EuY)Ri~RIySS~J^mnt*Pb72|=w3{eXWR#:Q2~d>o99,pa<0: W*r(.Cex4&{= ~!m\OUdX5JT?
May 27, 2022 14:31:08.575661898 CEST	1969	OUT	GET /files/theme/fonts/6de0ce4d-9278-467b-b96f-c1f5f0a4c375.ttf?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515. 107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.16 53687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.747270107 CEST	1971	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:08 GMT Content-Type: font/ttf Content-Length: 52269 Connection: keep-alive Last-Modified: Wed, 11 Dec 2019 02:22:44 GMT x-rgw-object-type: Normal ETag: "86cbf50e12da0b519ced148acd8ba2b4" x-amz-request-id: tx000000000000000b60ec5-0061a70324-a9f4046-sfo1 X-Storage-Bucket: z7118 X-Storage-Object: 7118fcc9995d78a79c6a13eca290b043acd29399680aae376df5e95bc537fbd3 X-Host: blu38.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 00 01 00 00 00 10 01 00 00 04 00 00 47 50 4f 53 fe b3 03 03 00 00 01 0c 00 00 1e bc 4f 53 2f 32 65 96 fd c3 00 00 1f c8 00 00 00 60 56 44 4d 58 6e 58 75 d4 00 00 20 28 00 00 05 e0 63 6d 61 70 90 e6 b0 e3 00 00 26 08 00 00 00 cc 63 76 74 20 06 18 05 69 00 00 26 d4 00 00 01 e4 66 70 67 6d a1 cc 85 0f 00 00 28 b8 00 00 09 50 67 61 73 70 ff ff 00 04 00 00 32 08 00 00 00 08 67 6c 79 66 90 20 03 06 00 00 32 10 00 00 78 d8 68 65 61 64 f3 a6 d3 c2 00 00 aa e8 00 00 00 36 68 68 65 61 07 68 07 bb 00 00 ab 20 00 00 00 24 68 6d 74 78 cc f6 37 96 00 00 ab 44 00 00 03 78 6c 6f 63 61 00 3 1 2c bc 00 00 ae bc 00 00 03 7c 6d 61 78 70 02 6e 01 01 00 00 b2 38 00 00 00 20 6e 61 6d 65 64 76 02 a6 00 00 b2 58 00 00 17 81 70 6f 73 74 ff 9f 00 32 00 00 c9 dc 00 00 00 20 70 72 65 70 e3 0f 5b e5 00 00 c9 fc 00 00 02 2f 00 01 00 00 00 0a 00 64 00 ae 00 01 6c 61 74 6e 00 08 00 22 00 05 41 46 4b 20 00 2a 44 45 55 20 00 32 4e 4c 44 20 00 3a 52 4f 4d 20 00 42 54 52 4b 20 00 4a 00 00 ff ff 00 01 00 00 00 00 ff ff 00 01 00 01 00 00 ff ff 00 01 00 02 00 00 ff ff 00 01 00 03 00 00 ff ff 00 01 00 04 00 00 ff ff 00 01 00 05 00 06 6b 65 72 6e 00 26 6b 65 72 6e 00 2c 6b 65 72 6e 00 32 6b 65 72 6e 00 3 8 6b 65 72 6e 00 3e 6b 65 72 6e 00 44 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 01 00 04 00 09 00 00 00 02 00 0a 00 12 00 01 00 02 00 00 00 10 00 01 00 02 00 00 00 d2 00 01 00 2e 00 04 00 00 00 12 00 56 00 70 00 76 00 7c 00 76 00 82 00 8c 00 92 00 92 00 98 00 9e 00 a4 00 ae 00 b4 00 ba 00 c4 00 b4 00 9e 00 01 00 12 00 0f 00 27 00 29 00 32 00 33 00 37 00 38 00 39 00 3a 00 3c 00 7d 00 cf 00 d0 00 d1 00 d2 00 d3 00 d4 00 db 00 06 00 6d ff d0 00 cf ff b8 00 d0 ff b8 00 d2 ff ac 00 d3 ff ac 00 da ff d0 00 01 00 88 ff d6 00 01 00 88 ff 88 00 01 00 88 ff d0 00 02 00 88 ff 88 00 c3 ff e2 00 01 00 88 ff e0 00 01 00 88 ff c4 00 01 00 88 ff be 00 01 00 0f ff dc 00 02 00 0f ff a6 00 88 ff a6 00 01 00 0f ff a6 00 01 00 59 ff f4 00 02 00 0f ff a6 00 88 ff 88 00 01 00 0f ff 88 00 02 18 88 00 04 00 00 19 4c 1b 24 00 36 00 3a 00 00 ff e2 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff e2 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: GPOSOS/2e`VDMXnXu (cmap&cvt i&fpgm(Pgasp2glyf 2xhead6hheah $hmtx7Dxloca1,|maxpn8 namedvX post2 prep[/dlatn"AFK *DEU 2NLD :ROM BTRK Jkern&kern,kern2kern8kern>kernD.Vpv|v')23789:<}mYL$6:<<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	64601	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.252933025 CEST	1088	OUT	GET /files/theme/fonts/2cd55546-ec00-4af9-aeca-4a3cd186da53.woff2?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.423345089 CEST	1193	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff2 Content-Length: 16561 Connection: keep-alive Last-Modified: Fri, 30 Aug 2019 08:25:03 GMT ETag: "27958408325380d903e67d87768563b8" x-amz-request-id: tx00000000000000009274c06-005eaa58ef-10e2649-las X-Storage-Bucket: z83f8 X-Storage-Object: 83f8b8932766826c1dd3a228b48f4072586ca09f781d64e2950d9f0e235c00a0 X-Host: blu46.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 32 00 01 00 00 00 00 40 b0 00 10 00 00 00 00 9a 08 00 00 40 4c 00 02 19 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b bd 32 3f 4c 49 4e 4f 12 06 60 00 81 4c 08 83 62 09 95 22 11 08 0a 81 b2 08 81 94 7f 01 36 02 24 03 86 78 0b 86 7c 00 04 20 05 93 14 07 20 0c 84 4c 1b ec 86 15 6c 9b 56 b3 db 01 71 d3 4e ef 4c 01 37 46 6e b7 83 a2 20 fd ab 8b 0e d8 ee 56 a5 62 63 ac 91 fd ff 05 b2 31 1c 68 f5 0b 44 0b a6 52 51 6a da 10 46 a9 3d 06 ae 73 d7 15 14 38 01 80 65 2b a6 12 20 86 08 81 6b 29 c2 0b cd 09 e0 23 71 02 d7 dd 23 bf 71 40 ad 45 03 58 00 00 37 f 0 02 14 e0 13 0b 00 00 f6 86 19 00 d0 00 11 30 5f 81 09 18 b7 88 d1 1f 00 aa b2 c4 80 f8 01 8f f5 00 4a 60 81 6d c3 1e 8a 46 47 cf f9 72 da 3b 20 e0 19 8d 34 02 5b 92 81 14 db 1b 19 12 f6 c6 ca 6e b3 ff ef 07 a2 53 cb 27 00 72 6b b9 f9 2e f1 ed 03 41 53 38 d3 ad c7 f4 f5 70 e9 f3 00 bf b6 fa 61 88 1e 06 26 a2 98 4a 1e cc bc 09 a6 0a 98 00 25 4a 49 83 b2 51 41 6c 5c bd d5 5d b0 7a f7 ec ff ad c0 5d bd 13 5d d7 a8 03 03 3b b6 91 a0 1a 43 f7 ee 83 58 64 49 04 0e 55 ab 44 27 c2 15 8d a8 90 f5 8d 8a 2b 3b 62 9b 33 6d c3 4f 90 60 5a e3 c9 d1 1e 24 ad a1 4c ca 4d 18 3f 37 ff 15 66 03 7a 56 72 63 b3 1e a1 e9 61 8f bf 2c a5 03 17 54 f0 bf 6b 3b 34 13 52 84 d2 56 91 d7 97 96 2e 2d 61 96 cc 7e 42 4f f5 73 88 bd 9c 95 31 7b af 62 7c f7 d1 15 ea c6 9f 30 b4 21 0d 6d 17 32 40 9a bb ff 32 a7 49 c1 99 5d fb 08 e8 55 00 90 a5 24 0e b0 db fa 18 ec 6f f2 2d 01 1d c2 bb e7 7f ea 4a 3b 48 95 67 15 f8 3a 85 1d 46 9f 15 5a 22 69 37 85 3c e3 9b f1 ba bd 2e 50 a2 f6 aa 32 f0 74 d5 5e 17 e6 a2 4a 05 58 38 8c f0 bd ed 7d c5 ab d1 13 5f 66 c0 4d 98 29 9a b7 ae 47 e3 9e 7a 53 b1 4b 63 69 9d e2 18 1a b0 c0 0e 10 f8 00 26 2c 87 6b aa ab 36 ab 59 da 3f 48 d2 2b 67 63 e7 02 97 14 70 a0 40 cd 28 95 97 f5 ff df d4 b4 c5 68 97 ab 90 a2 53 28 4a ca b9 64 57 be fb ff 0c f0 ef cc 20 7c 80 20 e7 03 a4 17 43 2a 70 b8 2b 19 b3 e1 88 50 04 40 7a 05 92 bb 56 08 b9 73 48 25 b1 eb 40 48 b9 b3 73 d3 ba 55 eb e3 be f1 ff ed f7 ab ce 47 df 07 4f 1c 42 b2 44 88 44 6f fd e2 33 e8 fc 87 a8 a4 3f e0 c9 3d 12 f1 86 0f e6 f3 f1 4d 62 da 54 4a d8 12 36 6d de 1a 89 0b ff bf 16 bf 3c a1 b6 f3 af 8f 81 c3 65 31 98 c4 56 96 75 8a a2 bb 61 e4 4c 61 dd 27 ab 78 cf 5f 4a 91 22 12 42 08 41 82 78 5f 4c 0e ab 9b da 7b 7e a4 aa 16 25 95 70 0d 67 0d 15 b1 d3 18 81 64 21 8b d8 f5 c5 fb 77 89 33 1b 05 da ff bf e3 5c 9e 02 68 60 49 d6 0a 77 25 bb e5 4b 96 8b 0d 7e 3f 54 fa a5 98 8b b9 b8 8d db 74 cd e1 f3 a1 53 c1 2d f7 ad 00 82 00 4d 95 5d 62 1e dc 6a 69 82 24 a1 8b 3f 70 d4 49 85 f0 0f 5b 0a 6f 97 64 67 5d e6 25 dd 45 af bb 8c 97 03 47 27 0e 90 d5 ff ca da fd fc b8 Data Ascii: wOF2@@L2?LINO`Lb"6$x\|  LlVqNL7Fn Vbc1hDRQjF=s8e+ k)#q#q@EX70_J`mFGr; 4[nS'rk.AS8pa&J%JlQ Al\]z]];CXdIUD'+;b3mO`Z$LM?7fzVrca,Tk;4RV.-a~BOs1{b|0!m2@2l]U$o-J;Hg:FZ"i7<.P2t^JX8}_fM)GzSKci&,k6Y? H+gcp@(hS(JdW \| C*p+P@zVsH%@HsUGOBDDo3?=MbTJ6m<e1VuaLa'x_J"BAx_L{~%pgd!w3\h`lw%K~?TtS-M]bji$? pI[odg]%EG'
May 27, 2022 14:31:07.671128035 CEST	1347	OUT	POST /ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails] HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Content-Length: 83 Accept: application/json, text/javascript, */*; q=0.01 X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Content-Type: application/json; charset=UTF-8 Origin: http://document--1111011111.company.com Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en Data Raw: 7b 22 6a 73 6f 6e 72 70 63 22 3a 22 32 2e 30 22 2c 22 6d 65 74 68 6f 64 22 3a 22 43 75 73 74 6f 6d 65 72 41 63 63 6f 75 6e 74 73 3a 3a 67 65 74 41 63 63 6f 75 6e 74 44 65 74 61 69 6c 73 22 2c 22 70 61 72 61 6d 73 22 3a 5b 5d 2c 22 69 64 22 3a 30 7d Data Ascii: {"jsonrpc":"2.0","method":"CustomerAccounts::getAccountDetails","params":[],"id":0}
May 27, 2022 14:31:08.053121090 CEST	1454	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 12:31:07 GMT Server: Apache Vary: X-W-SSL,User-Agent X-Host: grn91.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 348 Keep-Alive: timeout=10, max=53 Connection: Keep-Alive Content-Type: application/json Data Raw: 7b 22 6a 73 6f 6e 72 70 63 22 3a 22 32 2e 30 22 2c 22 69 64 22 3a 30 2c 22 6d 65 74 68 6f 64 22 3a 22 43 75 73 74 6f 6d 65 72 41 63 63 6f 75 6e 74 73 3a 3a 67 65 74 41 63 63 6f 75 6e 74 44 65 74 61 69 6c 73 22 2c 22 72 65 73 75 6c 74 22 3a 7b 22 73 75 63 63 65 73 73 22 3a 66 61 6c 73 65 2c 22 6d 65 73 73 61 67 65 22 3a 22 43 75 73 74 6f 6d 65 72 20 61 63 63 6f 75 6e 74 73 20 72 65 73 74 72 69 63 74 65 64 20 6f 72 20 6e 6f 74 20 65 6e 61 62 6c 65 64 2e 22 2c 22 65 76 65 6e 74 22 3a 22 22 2c 22 64 61 74 61 22 3a 7b 22 63 6f 64 65 22 3a 22 64 6f 6e 74 53 68 6f 77 22 2c 22 6d 65 73 73 61 67 65 22 3a 22 43 75 73 74 6f 6d 65 72 20 61 63 63 6f 75 6e 74 73 20 72 65 73 74 72 69 63 74 65 64 20 6f 72 20 6e 6f 74 20 65 6e 61 62 6c 65 64 2e 22 2c 22 6d 65 73 73 61 67 65 5f 74 6c 22 3a 22 43 75 73 74 6f 6d 65 72 20 61 63 63 6f 75 6e 74 73 20 72 65 73 74 72 69 63 74 65 64 20 6f 72 20 6e 6f 74 20 65 6e 61 62 6c 65 64 2e 22 7d 2c 22 74 6f 74 61 6c 22 3a 6e 75 6c 6c 2c 22 68 74 74 70 5f 72 65 73 70 6f 6e 73 65 5f 63 6f 64 65 22 3a 34 30 31 7d 7d Data Ascii: {"jsonrpc":"2.0","id":0,"method":"CustomerAccounts::getAccountDetails","result":{"success":false,"message":" Customer accounts restricted or not enabled.","event":"","data":{"code":"dontShow","message":"Customer accounts restricted or not enabled.","message_tl":"Customer accounts restricted or not enabled."},"total":null,"http_response_code":401}}

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.127785921 CEST	1839	OUT	GET /files/theme/fonts/46cf1067-688d-4aab-b0f7-bd942af6efd8.ttf?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.1653687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*
May 27, 2022 14:31:08.300400972 CEST	1905	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:08 GMT Content-Type: font/ttf Content-Length: 39185 Connection: keep-alive Last-Modified: Wed, 11 Dec 2019 02:22:44 GMT x-rgw-object-type: Normal ETag: "98f6dacde86ebbaac7cc62b34a6e54cf" x-amz-request-id: tx000000000000000d26573-0061a7031d-a9f3e81-sfo1 X-Storage-Bucket: z6503 X-Storage-Object: 65032d5699bf3d4deb4313aa4d1bb8375053ac7e93dfb4bf631ce9261da20c2b X-Host: grn67.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 00 01 00 00 00 10 01 00 00 04 00 00 47 50 4f 53 ec ec 14 b3 00 00 01 0c 00 00 1e b2 4c 49 4e 4f 93 af c8 c2 00 00 1f c0 00 00 00 12 4f 53 2f 32 65 f1 01 d7 00 00 1f d4 00 00 00 60 63 6d 61 70 90 e6 b0 e3 00 00 20 34 00 00 00 cc 63 76 74 20 07 7a 07 d7 00 00 21 00 00 00 01 e2 66 70 67 6d 63 0e 9d d9 00 00 22 e4 00 00 0a a2 67 61 73 70 ff ff 00 04 00 00 2d 88 00 00 00 08 67 6c 79 66 b3 67 b4 92 00 00 2d 90 00 00 58 10 68 65 61 64 f4 0f af ac 00 00 85 a0 00 00 00 36 68 68 65 61 07 59 07 8a 00 00 85 d8 00 00 00 24 68 6d 74 78 d7 00 2c e7 00 00 85 fc 00 00 03 78 6c 6f 63 61 00 27 77 bc 00 00 89 74 00 00 03 7c 6d 61 78 70 03 33 0b 90 00 00 8c f0 00 00 00 20 6e 61 6d 65 3c 21 96 46 00 00 8d 10 00 00 09 94 70 6f 73 74 ff 9f 00 32 00 00 96 a4 00 00 00 20 70 72 65 70 66 9a cf 76 00 00 96 c4 00 00 02 4c 00 01 00 00 00 0a 00 64 00 ae 00 01 6c 61 74 6e 00 08 00 22 00 05 41 46 4b 20 00 2a 44 45 55 20 00 32 4e 4c 44 20 00 3a 52 4f 4d 20 00 42 54 52 4b 20 00 4a 00 00 ff ff 00 01 00 00 00 00 ff ff 00 01 00 01 00 00 ff ff 00 01 00 02 00 00 ff ff 00 01 00 03 00 00 ff ff 00 01 00 04 00 00 ff ff 00 01 00 05 00 06 6b 65 72 6e 00 26 6b 65 72 6e 00 2c 6b 65 72 6e 00 32 6b 65 72 6e 00 38 6b 65 72 6e 00 3e 6b 65 72 6e 00 44 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 01 00 04 00 09 00 00 00 02 00 0a 00 12 00 01 00 02 00 00 00 10 00 01 00 02 00 00 00 c8 00 01 00 2e 00 04 00 00 00 12 00 56 00 70 00 76 00 7c 00 76 00 76 00 82 00 88 00 88 00 8e 00 94 00 9a 00 a4 00 aa 00 b0 00 ba 00 aa 00 94 00 01 00 12 00 0f 00 27 00 29 00 32 00 33 00 37 00 38 00 39 00 3a 00 3c 00 7d 00 cf 00 d0 00 d1 00 d2 00 d3 00 d4 00 db 00 06 00 6d ff d0 00 cf ff b8 00 d0 ff b8 00 d2 ff b8 00 d3 ff b8 00 da ff d0 00 01 00 88 ff d6 00 01 00 88 ff 88 00 01 00 88 ff d0 00 01 00 88 ff e2 00 01 00 88 ff c4 00 01 00 88 ff be 00 01 00 0f ff dc 00 02 00 0f ff a6 00 88 ff a6 00 01 00 0f ff a6 00 01 00 59 ff f4 00 02 00 0f ff a6 00 88 ff 88 00 01 00 0f ff 88 00 02 18 88 00 04 00 00 19 4c 1b 24 00 36 00 3a 00 00 ff e2 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff e2 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: GPOSLINOOS/2e`cmap 4cvt z!fpgmc"gasp-glyfg-Xhead6hheaY$hmtx,xloca'wt|maxp3 name<!Fpost2 prepfvLdlatn"AFK *DEU 2NLD :ROM BTRK Jkern&kern,kern2kern8kern>kernD.Vpv|vv')23789:<}mYL$6:<<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	50986	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.433981895 CEST	1217	OUT	GET /files/theme/fonts/2e3f5cb9-101f-46cf-a7b3-dfaa58261e03.woff2?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.604341984 CEST	1314	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff2 Content-Length: 18637 Connection: keep-alive Last-Modified: Fri, 30 Aug 2019 08:25:04 GMT x-rgw-object-type: Normal ETag: "b3aa7e2126c418e820b06924717c2ce9" x-amz-request-id: tx000000000000000c79046-0061a707ba-a9f1ce7-sfo1 X-Storage-Bucket: zcace X-Storage-Object: cace42567eefa76edc8b069bb9cdf9fda7486243911fa88188efb2efca387a4a X-Host: grn78.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 32 00 01 00 00 00 00 48 cc 00 10 00 00 00 00 c2 a4 00 00 48 6d 00 02 19 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b bd 3c 06 60 16 8b 60 00 81 4c 08 83 64 09 92 50 11 08 0a 81 de 50 81 ba 34 01 36 02 24 03 86 78 0b 86 7c 00 04 20 05 af 01 07 20 0c 84 2f 1b f9 ab 25 ca b6 5d a5 f4 66 55 41 2c 8c 9f a2 0a b6 cd a4 db ed c8 f6 9b 2b 4e 96 28 b7 4f c1 ed c0 a8 eb ff 97 ca fe ff 23 c4 31 b6 03 9a 59 02 a2 0a ad d5 4c 19 ab 76 1e 43 71 94 f3 ce 65 66 07 bb 1b d0 0b 5e 01 54 40 05 38 5d 40 05 54 12 3c 62 25 53 96 9c ba 04 9a 40 13 94 40 22 a4 f6 03 40 03 b8 5f 36 04 00 00 b6 53 6b ea f7 52 50 a2 51 17 8d 01 00 70 03 00 81 d0 28 00 00 7c c7 05 01 e0 5e 66 b8 01 0b c0 f8 01 5e 16 c8 00 d7 0b 14 f8 05 00 00 00 00 ac b0 71 0d 62 96 d4 1e 3d 45 43 1e ea c7 d2 b7 ff 8e ff 5d 98 55 54 84 63 05 68 6c 62 5c b8 2e b2 ce 75 aa cb e3 23 6c 59 ef 00 cd ad 41 8f 58 dd ad 6e db ed d6 4d 0c 59 34 2b 46 a4 44 19 8d 2f 60 00 16 02 da 18 d1 8f 62 a1 ef a3 2f 58 d1 1f a9 be cc 9b d3 2f d9 92 2c 83 4c b2 65 e0 c4 61 b7 4d 53 97 92 a6 3f 19 20 3c cd 6d 0f 17 00 f4 ee 68 20 4b c0 c7 1e f7 ed e5 b2 19 7a ea 0f b6 77 1f 9b 84 e3 12 cb a3 24 c1 c0 a9 de ff ea 4c c9 0e bc f7 7f 5c 76 92 bb 5b 09 a7 e2 32 d6 92 29 ec b0 cb 20 ad c9 7a 80 54 c6 91 7d 52 e7 2b 39 25 70 3e 90 0a f2 a9 ec 32 c6 96 0b 2e 84 7a 67 15 e5 7f fe 17 28 ce 48 fa 30 cd cf 7f 4a 3a 01 c0 dc ad 13 d1 ff ea 16 33 e7 f6 47 f0 16 b1 2d 98 24 ad 8f f7 82 59 ed 17 1d a7 db 46 1d 38 5d 1f 39 8d af 50 5e 62 d3 0e 45 a3 3e 8d fe ed dd 1f e0 ae 3c e0 76 3e d0 ae 92 8f 1e 26 c6 1b 70 53 e1 25 55 b3 5b cc cf 4e 8e 6f 7b 2b 0a 35 82 47 54 48 05 f1 7d a7 24 21 a3 03 89 75 fb f8 01 54 42 15 fb c7 51 cf b6 f2 24 39 69 d2 85 5a 38 8c fe ff 2f cb a4 dd 0a 09 39 a7 41 8e 00 4a f2 1e ee 84 0c 90 01 fc f7 ff 5f d5 ff 56 75 a8 d7 dd d2 d6 9f d8 a5 74 a6 14 bb 94 27 ac 4e 75 f5 ec 9e 09 1b 46 72 08 01 65 14 a7 25 a7 0d 11 ed 1e ee 04 98 a9 8d 7c 8c 8c cd e0 02 68 f8 ff ff fb ff f1 19 0b 68 03 06 78 dd d6 3d 7d e7 58 f4 b2 dd e7 67 67 44 d7 0a 2c c5 c2 30 c0 fc de 69 49 53 2a 65 a5 41 ea 3f 2a de 39 d9 b7 4f d7 7d 49 47 a5 02 28 59 63 79 8b 2f ad a3 a0 10 02 6d 96 63 09 0c f5 1f 17 c9 57 27 b2 40 b8 13 ea 57 a1 6f c9 ff 3f f7 6a 33 44 b5 09 b7 33 37 e1 98 84 dd 84 bf 29 be 24 85 40 21 29 e6 8f f0 ff 62 7e 89 3e 37 e9 96 0e 58 31 b9 94 33 ce 88 53 57 b9 b1 27 50 55 03 f4 44 42 d8 41 66 ab c4 8b 59 28 74 9c 56 4b 25 6b ee 81 6c f6 be 97 50 90 c7 98 0e db 3b 21 9a 35 e7 94 00 dd 89 55 ae 1d 98 dc 5d bf 09 e9 90 0e e9 90 9a 60 8c 50 55 21 84 30 Data Ascii: wOF2HHm<``LdPP46$x\| /%]fUA,+N(O#1YLvCqef^T@8]@T<b%S@@"@_6SkRPQp(\|^f^qb=EC]UTc hlb\.u#lYAXnMY4+FD/`b/X/,LeaMS? <mh Kzw$L\v[2) zT}R+9%p>2.zg(H0J:3G-$YF8]9P^bE><v>&pS%U[No{+5GTH}$!u TBQ$9iZ8/9AJ_Vut'NuFre%\|hhx=}XggD,0iIS*eA?*9O}IG(Ycy/mcW'@Wo?j3D37)$@!)b~>7X13SW'PUDBAfY(t VK%klP;!5U]`PU!0
May 27, 2022 14:31:07.867021084 CEST	1378	OUT	GET /files/theme/fonts/f26faddb-86cc-4477-a253-1e1287684336.woff?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.1653687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.037210941 CEST	1387	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff Content-Length: 24866 Connection: keep-alive Last-Modified: Wed, 11 Dec 2019 02:22:43 GMT x-rgw-object-type: Normal ETag: "0f12c575e08f164252dbddaf87f03c35" x-amz-request-id: tx000000000000000cb1182-0061a70896-a9f6a62-sfo1 X-Storage-Bucket: ze0bc X-Storage-Object: e0bc8743cf211c699ebb439c59780abf7b40b543b28bd198f6f355bb109a7424 X-Host: grn64.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 46 00 01 00 00 00 00 61 21 00 10 00 00 00 00 c9 2c 00 01 00 00 00 00 5a 38 00 00 06 e9 00 00 0d 78 00 00 00 00 00 00 00 00 47 50 4f 53 00 00 01 6c 00 00 06 ed 00 00 1e d4 00 a8 07 d1 4f 53 2f 32 00 00 08 5c 00 00 00 58 00 00 00 60 66 5b 02 eb 56 44 4d 58 00 00 08 b4 00 00 03 85 00 00 05 e0 6f 0e 76 94 63 6d 61 70 00 00 0c 3c 00 00 00 98 00 00 00 cc 90 e6 b0 e3 63 76 74 20 00 00 0c d4 00 00 00 55 00 00 01 e4 07 cc 08 a4 66 70 67 6d 00 00 0d 2c 00 00 05 2b 00 00 09 50 a1 cc 85 0f 67 61 73 70 00 00 12 58 00 00 00 08 00 00 00 08 ff ff 00 04 67 6c 79 66 00 00 12 60 00 00 39 0b 00 00 76 3c 5a 77 39 c4 68 65 61 64 00 00 4b 6c 00 00 00 36 00 00 00 36 f3 b9 d4 b9 68 68 65 61 00 00 4b a4 00 00 00 20 00 00 00 24 07 81 07 b4 68 6d 74 78 00 00 4b c4 00 00 02 12 00 00 03 78 de 7c 27 99 6c 6f 63 61 00 00 4d d8 00 00 02 56 00 00 03 7c 00 30 08 30 6d 61 78 70 00 00 50 30 00 00 00 20 00 00 00 20 02 6e 00 f1 6e 61 6d 65 00 00 50 50 00 00 08 06 00 00 17 07 3e 89 4d 67 70 6f 73 74 00 00 58 58 00 00 00 13 00 00 00 20 ff 9f 00 32 70 72 65 70 00 00 58 6c 00 00 01 ca 00 00 02 2f e3 0f 5b e5 78 9c c5 59 5b 6c 54 45 18 fe b6 37 da d2 76 db 2e 0b 85 52 2c 6d 69 69 4b 2f 6c 4b 69 01 89 98 72 91 4b 8d 85 0a 08 1a 04 2f 0f 0a 12 e3 a3 3c c0 8b ab 89 3e 98 3e 18 4c 84 68 ac 95 20 c1 6a c8 06 0d 88 94 8b c6 d8 52 6a 63 60 4d cc 86 40 63 4d a3 a1 21 91 97 f1 9b ff 9c b3 dd ed 5e ba bd 2d f3 65 66 ce ce fc 67 fe cb f7 9f 99 73 5a d8 00 a4 e3 25 9c 81 ed f5 17 df 3a 84 54 14 21 79 dd 86 2d 85 a8 68 5e df 56 08 57 cb d6 e6 42 ac 6a 7d 7a 5b 21 9e dc d1 ca f1 cd 80 52 d0 f7 19 bd cd ec 13 cc 3e d1 ec 93 cc 3e 19 29 af bd fc e6 21 94 4a bb 4c 5a 97 b4 8d d2 ae 95 b6 99 cb c9 9a 51 5b bd 6a 1a fb 04 da 9c 6b e8 44 b6 d9 ff c5 be 5e 6b 85 13 fb f1 36 8e c1 cd 7a 0c 1f a0 9d 38 8e 93 38 85 b3 38 87 ef 71 15 bf a0 0f 5e b6 e7 78 8f 13 76 94 a1 1c 2e d4 61 25 1a d1 84 55 58 8d 35 68 41 1b 8e a0 07 bd b8 41 e9 9b e8 c7 6d a4 e0 a0 ea 45 8f f2 a0 97 b5 8f f5 26 eb 2d 8e d9 e0 56 03 d2 ba a5 35 46 fe 94 b6 9b ed 65 35 4c 2b dd ea 02 af 06 f9 bb 9b bf 6d e8 54 23 6c ed ca cb 39 bb ea e0 7c 87 fc d6 ed 6e ce 59 a3 6e 19 75 23 21 cf ad 3d 9c bf 35 bf 04 0d b4 13 ca 47 4b e3 5c 1e 85 4e d1 eb a5 e6 f8 96 da 38 eb 33 8b f2 a9 5e 35 a8 86 99 29 f1 d4 d9 ad 06 a8 b5 3b ae 3a bd f4 32 fe 7e ea d8 7a f9 d4 c5 41 db 23 79 56 e2 9f b7 19 86 9f ca c3 cc f5 ea 1c 62 8c 47 b8 83 cd 60 e1 7e 68 94 5c 03 dc 29 61 da e0 63 26 fb 11 17 1b 66 52 47 bb 79 f1 28 fd b4 74 f6 f2 e9 d1 ec 5a 75 84 27 dd 74 95 bc 80 1c 1a 8c 4f 0e 19 85 bb 41 37 63 Data Ascii: wOFFa!,Z8xGPOSlOS/2\X`f[VDMXovcmap<cvt Ufpgm,+PgaspXglyf`9v<Zw9headKl66hheaK $hmtxKx|'lo caMV|00maxpP0 nnamePP>MgpostXX 2prepXl/[xY[lTE7v.R,miiK/lKirK/<>>Lh jRjc`M@cM!^-efgsZ%:T!y-h^VWBj}z [!R>>)!JLZQ[jkD^k6z888q^xv.a%UX5hAAmE&-V5Fe5L+mT#!9|nYnu#!=5GK\N83^5);:2~zA#yVbG`~h\)ac&fRGy(tZu'tOA7c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	54849	52.25.131.159	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.058433056 CEST	1461	OUT	OPTIONS /com.snowplowanalytics.snowplow/tp2 HTTP/1.1 Host: ec.editmysite.com Connection: keep-alive Accept: */* Access-Control-Request-Method: POST Access-Control-Request-Headers: content-type Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Sec-Fetch-Mode: cors Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:08.247374058 CEST	1904	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 12:31:08 GMT Content-Length: 0 Connection: keep-alive Server: nginx Access-Control-Allow-Origin: http://document--1111011111.company.com Access-Control-Allow-Credentials: true Access-Control-Allow-Headers: Content-Type, SP-Anonymous Access-Control-Max-Age: 5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	55759	52.25.131.159	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.456121922 CEST	1953	OUT	POST /com.snowplowanalytics.snowplow/tp2 HTTP/1.1 Host: ec.editmysite.com Connection: keep-alive Content-Length: 1957 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Content-Type: application/json; charset=UTF-8 Accept: */* Origin: http://document--1111011111.company.com Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:08.644964933 CEST	1970	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 12:31:08 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 2 Connection: keep-alive Server: nginx Set-Cookie: sp=6f09e634-3f7a-4428-a215-09325d168236; Expires=Sat, 27 May 2023 12:31:08 GMT; Domain=; Path=/; Secure; SameSite=None P3P: policyref="/w3c/p3p.xml", CP="NOI DSP COR NID PSA OUR IND COM NAV STA" Access-Control-Allow-Origin: http://document--1111011111.company.com Access-Control-Allow-Credentials: true Data Raw: 6f 6b Data Ascii: ok

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	57143	74.115.50.110	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:09.483129025 CEST	2029	OUT	GET /uploads/reseller/assets/356764895-favicon.ico HTTP/1.1 Host: www.weebly.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:09.655073881 CEST	2029	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 12:31:09 GMT Content-Type: text/html Content-Length: 3739 Connection: keep-alive ETag: "61c39c46-e9b" X-Host: grn63.sf2p.intern.weebly.net X-W-DC: SFO

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	60839	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:10.910954952 CEST	2035	OUT	GET /uploads/1/4/1/8/141840186/1screenshot-2021-04-26-at-19-59-20-orig-orig-orig_orig.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: document--1111011111.company.com

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:11.080173969 CEST	2042	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:10 GMT Content-Type: image/png Content-Length: 46476 Connection: keep-alive Last-Modified: Mon, 10 May 2021 13:49:51 GMT x-rgw-object-type: Normal ETag: "86023205c6da4584ac9ad959a7504d4c" x-amz-request-id: tx00000000000000281f026-00628523cc-b9fbc7f-sfo1 X-Storage-Bucket: ze542 X-Storage-Object: e542893276ee236968914d1271b54a4afd7df253d4bfb04ff8e5fcda5817e397 X-Host: grn63.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 4f 00 00 00 66 08 06 00 00 00 13 75 aa 79 00 00 b5 53 49 44 41 54 78 da ec 5d 0d 93 e4 a8 0d cd ff ff 9f 49 25 b9 ab 4b d2 36 08 77 cf ac d3 b0 e8 1e 96 60 64 af d7 db b3 7b a2 ea 15 fa 78 c8 18 bb 7b 2c 03 3d 7f 5b bd 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 59 3c 79 f2 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 17 4f 9e bc 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 93 27 2f 5e bc 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e4 c9 8b 17 2f 5e bc 78 f1 e2 c5 8b 17 2f 5e 3c 79 f2 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 97 9f 2d 79 5a 52 5a 1d af 00 95 fa be 3c 71 5f d6 07 c0 7a 83 fb 90 73 07 a4 1f b2 a1 c3 ae fc 1a fa 98 fa d8 67 fa 88 da 38 07 33 8e 2d 9b 63 7a ff aa 2f e3 3e 68 d8 fd d4 9c 7b 01 ae f3 1d b6 0c 96 a5 ce 7d 7c 64 1d 72 06 cb b2 ad e6 54 b0 2c 21 38 6f 03 3e ec 90 33 7a f2 db bd 91 0b 1e b5 16 76 f8 35 67 e8 7f 68 bc 3d d6 47 d7 fe 36 92 b9 ce 6d cb d8 2e f9 73 3a c0 a2 60 73 c1 3b ce 5d 24 2f 31 c7 88 cf bc 34 6e 83 98 0d 8c 63 5c e1 e7 be 94 6b fa f6 b8 06 0f db 7f 3c e6 7d 80 87 02 da 30 04 bf 1f 87 6b 7c 0e 75 1b f6 01 b0 fd 50 5d db 0c 3f e4 93 c7 3c ee b7 fb 68 fb af d7 ad 3e bc b2 cf 47 af f5 67 bf 17 5e 7f ed ed 63 be fe fe b5 c7 d1 e6 9f ef 13 e4 d3 f7 c2 bd 2f 7f f9 f2 be 4d 9e e6 db ff d6 79 da 62 12 ba f2 df 7a ba cd 9f 58 3f 19 cf e6 d8 31 d1 17 f8 2 7 2b de ed c0 f1 8d f3 0c f3 6d 8d 61 5e 13 85 95 32 62 c1 53 8f 4f 3d d6 fa a9 67 c4 af a0 c0 72 e1 d5 ba 22 f3 e3 c8 3f d6 61 8b 19 42 e7 3e 15 7c cc e7 be 07 e8 3d 7f 12 e7 40 76 1f 01 dd c7 02 12 f1 48 c7 de da c3 cc 31 04 9f 6d 73 91 59 8f 51 f1 21 97 9a 65 d9 87 5a 17 5d f0 43 b7 6f e0 07 19 53 f0 03 db f9 5e 61 39 83 d6 58 64 ca 50 1c d8 21 a7 a6 6d 2a 89 7d d5 53 7c ca c5 56 f4 65 29 72 b5 47 c8 a5 ae 6d 33 98 2f 6c dc 3e d7 0b c1 76 af bc fb 52 50 ec f7 82 2a 2f 89 65 24 16 59 ae ba c6 f2 44 e5 dc a5 1d 72 fb 02 03 fe 22 e7 e4 b4 9c 5b 08 d3 1a e6 27 42 c6 ad d6 53 f9 fc c6 e2 83 1f 32 eb cc 07 57 61 2a 1c 85 79 be 15 ff 3c 95 ba 41 cb 9f 8b 3e 67 5e 45 68 f9 a1 ad 4b cc 12 8f db 04 cd c7 31 80 0d 27 ca 5a f5 b1 e8 5b de c4 7c f4 e3 a3 78 7c cc 44 b1 bd 7e 78 e1 b0 34 d7 ad a3 3f 7a fe 04 1b e2 f1 cb 2b d6 c1 67 c0 0f 5d f7 41 bc 10 3b 0c dc f7 4b ae ab 3d eb 83 36 db cf 16 b7 15 48 84 cf 31 7f 5f 40 17 48 52 d6 d0 31 6c 90 e5 37 fb 68 ea da 66 c4 80 7c 0c e8 63 f8 38 46 b4 63 80 73 cd 38 da f1 ed 71 a4 73 e3 78 fe 5a 9f b8 5f Data Ascii: PNGIHDROfuySIDATx]I%K6w`d{x{,=[x/^xY<y/^xOx/^x'/^x/^x/^x/^<y/^x-yZRZ<q_zsg83-cz/>h{}|drT,!8o>3zv5g h=G6m.s:`s;]$/14nc\k<}0k\|uP]?<h>Gg^c/MybzX?1'+ma^2bSO=gr"?aB>\|=@vH1msYQ!eZ]CoS^a9XdP!m*}S\|Ve)rGm3/l> vRP*/e$YDr"['BS2Wa*y<A>g^EhK1'Z[|x|D~x4?z+g]A;K=6H1_@HR1l7hf|c8Fcs8qsxZ_
May 27, 2022 14:31:11.413713932 CEST	2128	OUT	GET /uploads/1/4/1/8/141840186/3pdp-orig-orig_orig.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: document--1111011111.company.com
May 27, 2022 14:31:11.585231066 CEST	2146	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:11 GMT Content-Type: image/png Content-Length: 15272 Connection: keep-alive Last-Modified: Thu, 10 Feb 2022 08:37:12 GMT x-rgw-object-type: Normal ETag: "72afce6a160fc291147021b6aac153c1" x-amz-request-id: tx00000000000000286f5ff-00628523cc-b9fbc64-sfo1 X-Storage-Bucket: z3e53 X-Storage-Object: 3e53901bb513d98511cdc10c3e14aa61e71d88728f1bfdc614c0caed4e10602c X-Host: blu78.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 a5 00 00 00 3e 08 06 00 00 00 d3 68 bd 5b 00 00 3b 6f 49 44 41 54 78 da ec dd 5b 6c 14 55 00 c6 71 5e f0 82 fa 66 e2 8b 09 46 01 25 6a e2 05 2f 54 28 2a 8f 3e 41 02 c1 48 8c 0f 90 80 80 42 34 a9 21 4d c0 87 86 06 62 28 ad 05 4a 4b 42 4a 8c bd f8 24 a0 d1 a5 5b a1 dc 0c c1 5e 82 35 05 5a da 52 48 ba 6d 22 ad bd c0 ee 9c f9 3c 67 ca a9 8d 68 45 9a 6e ab fd ff 92 2f 33 b3 b3 81 d9 79 98 ec d7 73 66 76 5a 18 4a 84 10 42 08 21 84 10 42 c8 18 72 d7 28 a5 84 10 42 08 21 84 10 42 26 ae 94 0a 00 00 00 00 80 31 a1 94 02 00 00 00 00 28 a5 00 00 00 00 00 50 4a 01 00 00 80 71 13 86 21 19 11 80 52 0a 00 00 00 a4 a9 8c 06 41 a0 54 2a a5 64 32 49 86 e2 ce 47 74 5e 8c 31 02 28 a5 00 00 00 c0 38 30 c6 50 ba ee ec 3c 31 7a 0a 4a 29 00 00 00 90 86 d1 52 f2 47 28 ec 98 8c a5 34 94 8c 91 82 e0 9f 63 6c 42 63 13 2a b4 4b 13 06 77 16 05 0a c5 5f 61 00 00 00 30 fe f7 8f 7a 9d 9d 9d 6a 6c 6c 54 6d 6d ad ea eb eb d5 d0 d0 e0 96 53 2e fe 73 d7 d5 d5 45 b9 7c f9 b2 06 07 07 75 0b f7 9b 62 92 8d 94 86 a3 e6 5f a3 87 4e 1d c6 18 a6 ca 00 00 80 09 fd 2e e2 f5 f7 f7 47 45 ac a2 a2 42 fb f6 ed 53 71 71 b1 4a 4a 4a a6 7c f6 ef df 1f 9d 8f 0 3 07 0e 28 16 8b a9 a3 a3 c3 97 51 4a 29 98 be 0b 00 00 00 8c 45 10 04 c3 e5 ea dc b9 73 2a 2a 2a d2 b6 6d db b4 6b d7 2e 5f c6 dc 6b 2e 6e 7d ca c4 7f 6e 5f ce dd 72 c7 8e 1d ca c9 c9 d1 e1 c3 87 95 48 24 74 0b 83 0b 98 c0 52 1a a4 a4 be 1e e9 7a b7 4d 97 d4 d3 fd d7 71 fb dc 7b fa 7a 15 24 07 34 98 ba ae df 92 09 f5 0d a7 4b 7d 37 6f 25 19 c5 ee ef 8c de 33 90 fa 55 29 73 53 00 00 00 c0 78 fd e4 8b 9f b2 5b 5a 5a aa dc dc 5c 1d 3a 74 28 9a be db da da aa 0b 17 2e a8 a9 a9 49 17 2f 5e 9c 92 71 9f df e5 ca 95 2b 3a 73 e6 8c 0a 0b 0b a3 c2 5e 53 53 13 dd 67 ea 8b 3d 90 be 52 1a 86 1a 96 b8 a6 f0 d8 d7 0a 2b 76 2b fc 32 5f aa dc 6b d7 6d ca f7 d8 e5 9e a1 ed 72 b7 ef 73 a9 cc ae 1f 3f a2 eb 1d 75 aa 4b 7c a3 58 fb 5e 55 b5 16 2a de b6 47 f1 f6 22 bb b4 db 36 f1 b6 a2 68 3b d6 ba 5b 47 6d ce 5e fb 4a 5d fd cd f2 42 85 cc ed 1d c3 85 d7 18 e3 e3 b6 27 f4 58 fc 05 ac a7 a7 47 5d 5d 5d 6e c9 05 0d 00 00 a4 8d 31 c6 7f f7 70 e5 2a 2a a1 79 79 79 ca cf cf 57 4b 4b 8b 70 bb de de de 68 94 74 fb f6 ed aa ac ac d4 c0 c0 c0 f0 f9 03 d2 53 4a 5d 91 30 81 86 35 fe a4 30 e7 7d 9 9 15 cf cb 2c 99 ab 70 c5 8b 76 7d 9e cc 32 bb bd fc 05 85 6f cf b3 cb e7 64 96 3e 2b 2d 7b 59 61 ee 46 b5 9f fd 42 a5 bf 7c a2 cd a7 33 95 7d fc 15 6d 39 91 a1 ad a7 17 69 cb c9 85 36 0b b4 f5 54 a6 3e 3d b5 48 9b 6b 32 94 5d f3 9a 8a 6b df 53 53 77 7c c4 21 18 4a e9 18 Data Ascii: PNGIHDR>h[;oIDATx[lUq^fF%j/T(*>AHB4!Mb(JKBJ$[^5ZRHm"<ghEn/3ysfvZJB!Br(B!B&1(PJq!RAT*d2IG t^1(80P<1zJ)RG(4clBc*Kw_a0zjlTmmS.sE\|ub_N.GEBSqqJJJ\|(QJ)Es***mk._k.n}n_rH$tRzMq{z$4K}7o%3U)sSx[ZZ\: t(.I/^q+:s^SSg=R+v+2_kmrs?uK|X^U*G"6h;[Gm^J]B'XG]]]n1p**yyyWKKphtSJ]050},pv}2od>+-{YaFB|3}m9i6T>=Hk2]kSSw|!J

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	60840	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:10.911092997 CEST	2036	OUT	GET /uploads/1/4/1/8/141840186/editor/2screenshot-2021-04-26-at-19-59-12-orig-orig.png?1652460803 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: document--1111011111.company.com
May 27, 2022 14:31:11.083208084 CEST	2054	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:10 GMT Content-Type: image/png Content-Length: 47588 Connection: keep-alive Last-Modified: Fri, 13 May 2022 16:54:01 GMT x-rgw-object-type: Normal ETag: "e9f5fab58c91223b66dbc7d8a8d064f2" x-amz-request-id: tx00000000000000734d4f7-00628b73bf-b9fbc77-sfo1 X-Storage-Bucket: z3b1f X-Storage-Object: 3b1f7691ebb9f6305b70a17a304ed4f6f84d9153ccf6ba7dafcf6e613ab19816 X-Host: grn64.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 f5 00 00 01 0c 08 06 00 00 00 dd d5 2f c0 00 00 00 01 6f 72 4e 54 01 cf a2 77 9a 00 00 80 00 49 44 41 54 78 da ec fd f9 73 1c 49 96 e7 09 7e 54 d5 cc dd e1 8e fb 22 40 f0 be 19 f7 9d 11 99 19 79 54 1e 95 9d 59 95 d5 d7 4c cf c8 c8 8a 8c ac c8 8a ec 0f fb d7 ec 6f 2b bb 23 3d bb db 3b 3b 3d dd 5b 53 5d 9d d9 9d 95 95 57 45 64 46 c6 7d 91 41 32 78 13 bc 71 df 80 bb 99 ea db 1f d4 cc dc 1c 04 49 90 04 0f 80 f6 15 41 10 e1 70 37 57 33 35 d3 a7 ef bd ef fb 3e 25 22 42 81 02 05 0a 14 28 50 60 d3 43 3f ee 01 14 28 50 a0 40 81 02 05 36 06 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 05 0a 14 28 50 a0 c0 16 41 61 d4 0b 14 28 50 a0 40 81 2d 82 c2 a8 17 28 50 a0 40 81 02 5b 04 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 05 0a 14 28 50 a0 c0 16 41 61 d4 0b 14 28 50 a0 40 81 2d 82 c2 a8 17 28 50 a0 40 81 02 5b 04 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 8f 03 f2 b8 07 50 a0 40 81 02 05 b6 22 82 c7 3d 80 a7 06 22 ab fe 05 14 e9 7f 3c 94 ba c7 83 16 28 50 a0 40 81 02 4d 14 46 fd a1 42 bc f1 4e 0d b9 d6 6b 1b 6e e7 9a ef 47 15 c6 bd 40 81 02 05 0a dc 17 94 88 14 c1 e0 87 01 11 40 12 03 ad 9a af 2d 2f c2 e2 22 04 01 54 db a1 54 ba d5 88 4b 6a e4 0b 03 5f a0 40 81 02 05 d6 8f c2 a8 6f 18 a4 99 2b 5f 6d 88 57 96 90 a9 09 e4 c6 55 b8 f0 35 ee f2 05 a4 52 c3 ec 39 88 1a da 8e f4 f4 a1 bb fb bc 91 0f c3 35 0e 9d 9b a2 c2 c8 17 28 50 a0 40 81 db a0 30 ea 0f 0c 69 e6 c7 85 a6 d1 b5 31 cc cf 22 57 2e 61 cf 9d c2 5d f8 1a 77 ed 32 6e f2 26 6e 7e 0e 82 00 dd d5 83 ee ea 41 f5 0e a0 87 b6 63 b6 ef 46 6d df 0d 43 23 a8 8e 2e 30 81 0f d9 67 5f b5 6a aa 0a 03 5f a0 40 81 02 05 72 28 8c fa fd 40 92 b0 7a fa 6f 0a e7 a0 be 02 37 ae 60 47 cf e1 ce 9e f2 06 fd c6 15 dc e2 3c 12 45 a0 35 a2 35 88 a0 9c f5 ff 9a 00 55 2e a1 da 3b d1 03 c3 e8 91 3d e8 1d 7b d0 43 3b d0 43 23 d0 37 00 a5 0a 18 93 1f 44 6b 64 60 f5 58 0a 14 28 50 a0 c0 53 87 c2 a8 af 1b 6b 90 de 52 34 ea c8 e4 38 72 f5 22 72 e9 2c f6 fc d7 c4 17 cf e1 26 c7 90 46 1d 51 0a a5 74 52 40 b8 ca 00 a7 b9 77 91 ec d8 ca 04 a8 5a 27 7a 60 1b c1 c8 6e f4 c8 6e d4 d0 08 6a 70 18 d5 37 08 1d dd 3e 17 df 32 bc e4 38 a8 1c a1 be 30 Data Ascii: PNGIHDR/orNTwIDATxsl~T"@yTYLo+#=;;=[S]WEdF}A2xqIAp7W35>%"B(P`C?(P@6Q/P@^@IF@"(z(EP(P`0(PAa(P@-(P@[Q/P@^@IF@"(z(EP(P`0(PAa(P@-(P@[Q/P@^@IF@"(z(EP(P`0P@"="<(P@MFBNknG@@-/"TTKj_@o+_mWU5R95(P@0i1"W.a]w2n&n~AcFmC#.0g_j_@r(@zo7`G<E55U.;={C;C#7Dkd`X(PSkR48r"r,&FQtR@wZ'z`nnjp7>280

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	53183	52.25.131.159	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	52791	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.196275949 CEST	96	OUT	GET / HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.395495892 CEST	170	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 12:31:06 GMT Server: Apache Set-Cookie: is_mobile=0; path=/; domain=document--1111011111.company.com Vary: X-W-SSL,Accept-Encoding,User-Agent Set-Cookie: language=en; expires=Fri, 10-Jun-2022 12:31:06 GMT; Max-Age=1209600; path=/ Cache-Control: private ETag: W/"9c914c4469a59d58104fecad7951b405-gzip" Content-Encoding: gzip X-Host: blu105.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 5871 Keep-Alive: timeout=10, max=72 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed 3c fd 77 db 46 8e 3f 5b ef ed ff 30 65 bb a5 dc 88 a2 64 4b fe d0 57 cf 71 dc 6e fa da c4 1b 3b d7 db 8b b3 7a 23 72 24 31 a6 48 86 a4 2c eb 5c fd ef 07 60 86 5f 12 e5 8f a6 e9 de de 8b db 48 e4 0c 80 c1 60 00 0c 06 04 d5 fb ea c5 eb d3 cb 7f 9c 9f b1 69 3c 73 07 95 1e 7e 31 97 7b 93 be 26 3c 6d 50 d9 e9 4d 05 b7 e1 7b a7 17 3b b1 2b 06 cf a1 f3 9a 5d e2 35 33 d8 df fc 99 e8 99 b2 a7 37 13 31 67 41 e8 07 22 8c 97 7d cd 9f 74 22 27 16 43 8f cf 84 c6 2c df 8b 85 17 f7 b5 1c 01 8d 99 30 e4 26 5a 2c 3b 9f 82 62 8b c8 0a 9d 20 76 7c ef 69 88 ce 8c 4f f2 63 4d e3 38 e8 98 a6 ed 5b f3 19 34 18 46 13 fe 1a f8 d1 ac 5b fe 2c e0 de 12 bf cd 79 e0 fa dc 8e cc a6 d9 82 7f 47 66 b3 d5 3c 6a 35 9a 47 07 66 13 38 11 c2 8b a6 7e 6c ec 35 f6 9a 46 a3 65 ec 1d 18 3c 36 9a c7 46 fb 18 da 0c 3f 74 26 d9 c7 10 3f ea 81 37 f9 f3 78 14 b6 13 fb a1 b9 f7 00 ab cd bd 8c 4b 64 f0 fb e6 41 7b af 75 d0 38 6a ec ff 79 bc ee 07 76 f0 04 61 cd 43 f7 77 0c 4f d4 2a 3d d7 01 7d 09 85 db d7 1c 0b 35 29 5e 06 02 ae 71 4e 26 8d 39 0d c5 b8 af 99 e6 62 b1 a8 2f 84 18 b9 45 ee 43 11 09 d7 15 a1 c9 a3 48 c4 91 b9 df 3e 38 3c 68 1d 1d b7 8d 31 bf 41 92 75 f8 90 63 55 14 f3 c8 a1 21 3e ce 9d 9b be 76 2a d9 36 2e 61 d8 dc 24 62 71 1b 9b 68 99 5d 66 4d 79 08 94 fb f3 78 6c 1c 11 21 c6 24 1d 34 b3 be 76 e3 88 45 e0 87 71 0e 7b e1 d8 f1 b4 6f 0b 18 5f 18 74 53 63 8e e7 c4 0e 77 8d c8 e2 ae e8 37 eb 0d c9 d3 ce 0e 1a 3a 09 c1 b1 01 13 ed d7 18 f1 48 18 51 bc 44 1b 22 d1 d0 75 34 15 22 4e 04 44 0c 5a 51 94 c9 c7 b2 bd bd 3a 6a d9 6c 89 44 48 48 00 60 e2 4d 54 87 ab ef 47 73 c7 b5 2f 1d 60 1a 94 0a d6 f9 e0 e8 48 29 55 b6 08 9f 32 92 ef da e6 98 7b d6 72 e4 df d2 80 9f 67 98 c8 b7 50 90 b8 b6 b9 79 c5 eb f3 9a 01 2a 87 91 c8 de 6a a0 b0 1f 84 25 9d d5 93 59 19 3b 00 61 ce b8 e3 0d 09 3a 99 1c 18 66 f3 a0 d1 02 3c f4 77 c9 ea c5 53 31 13 06 e1 a7 23 11 21 dd 34 c7 a0 22 51 7d e2 fb 13 57 f0 c0 89 92 49 7d 3f e6 33 c7 5d f6 7f c1 7e 11 86 3c ee b4 1a 8d da 61 a3 f1 6d 34 1f a1 fa b9 3c 76 bc 1a 7d 1a c0 9f 4e cc eb 19 f3 ba 64 5e 4f 98 d7 a5 79 11 c0 7a d7 Data Ascii: <wF?[0edKWqn;z#r$1H,\`_H`i<s~1{&<mPM{;+]5371gA"}t"'C,0&Z,;b v\|iOcM8[4F[,yGf<j5Gf8~l5Fe<6F?t&?7xKdA{u8jyvaCwO*=}5)^qN&9b/ECH>8<h1AucU!>v*6.a$bqh]fMyxl!$4vEq{o_tScw7:HQD"u4"NDZQ:jlDHH`MTGs/`H)U2{rgPy*j%Y;a:f<wS1#!4"Q}WI}?3]~<am4<v}Nd^Oyz
May 27, 2022 14:31:06.590301037 CEST	194	OUT	GET /files/main_style.css?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en
May 27, 2022 14:31:06.760210037 CEST	585	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:06 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Access-Control-Allow-Headers: Origin, Authorization, Content-Type Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS Access-Control-Allow-Origin: * X-Host: gm45.sf2p.intern.weebly.net Content-Encoding: gzip Data Raw: 31 63 65 38 0d 0a 1f 8b 08 00 00 00 00 00 00 03 e5 3d 6b 93 e4 b6 8d df fd 2b fa b2 b5 35 3b 57 ad 3e bd 1f b3 15 e7 1c db 97 6c 95 af 72 65 bb ce 1f 92 7c a0 24 6a 5a b7 dd ad 8e a4 de d9 b1 2b ff fd 40 ea 45 52 24 45 75 cf da 7b 75 71 cd 66 46 02 41 10 04 01 10 04 a1 cb 61 bb a9 e0 e7 50 6e 37 7b 07 7e 5c f8 f1 e0 c7 87 9f 00 7e c2 ed e6 5c e3 ed a6 a8 ea e3 76 93 56 f9 33 3c 6c 8f d0 24 2f 3f ec ce a8 46 8f 35 3a ef e1 d5 a1 ca de ff e3 52 b5 04 b8 c4 87 bc c1 ed 76 53 9e ce 97 76 f3 cb e6 88 ea c7 f2 f4 b0 b1 df 6e ce 28 cf cb d3 23 fd fd 9f 5f 5c ae 27 e0 7c 75 a7 9b dd 53 53 b6 d8 22 38 2d da ae 6b f3 d7 f6 f9 8c 7f 7f d7 e2 8f ed dd df b7 0b 50 f8 88 ca 83 1c 8c 20 40 35 46 b2 77 0d 3e e0 ac 5d 42 5e a3 bc ac 96 69 c8 f6 38 7b 9f 56 1f 19 c8 ac 3a 5a e7 ba ca 2f 59 6b 55 e7 b6 ac 4e d6 63 5d 5d ce 8d 6e 88 66 8d c4 11 ab 5b cd 18 a0 06 15 f8 61 46 89 c8 1e b3 56 13 b7 40 38 ac 27 9c be 2f 5b 0b fe b6 9a 3d ca ab a7 87 cd a9 3a e1 b7 1b eb 58 fd 2c 79 2c 01 ec 51 a0 f3 19 c3 42 38 65 98 43 31 7f 3c 7f 42 18 25 60 95 8a e7 0a 86 0e a0 30 c6 1a 37 e5 cf 98 41 fc ef 45 75 6a ad 02 65 18 de f6 bf 1f cb c3 f3 c3 e6 ee 8f 65 0d ab e7 19 df bd dd 34 75 f6 b0 b9 d4 87 37 77 ed 1e 1f f1 bf 11 c0 e6 df 9c 28 0b 82 d4 8d 2c 9c a0 d4 f2 bd 2c b7 d2 c4 8f ad dc 4f 8a 24 f2 63 3b 0f e3 1d ae da 3f bc 2a 71 51 7e fc 83 13 06 ae 1f 3a a1 ed df dd 7f 0a 9c 54 23 a0 f6 cd 1d bc bf bb df ce 91 bb d8 2b 82 2c 4d 2c c7 76 0a cb 0f b3 c2 42 51 ea 59 79 81 50 10 bb a1 83 6d 6f f7 54 15 85 2b c7 4b 5f 49 31 17 c8 49 80 4c 6c 05 d8 8b 2d 3f b1 13 2b f5 1c 6c f9 0e ca 72 27 02 aa 0b 97 62 56 23 96 e2 0d 73 6c 67 d8 cf ad c4 8d 00 6f 18 a5 c0 8e b0 b0 32 a7 08 0a 1b f9 99 17 05 bb b6 55 a0 6d eb 0b 26 82 2e 45 9d 14 b9 8f 91 9d 59 a9 93 20 cb 4f 5d c7 82 47 85 e5 45 b6 1f 44 76 94 e7 51 bc 6b 3e 3c be 32 01 94 f7 0f ad c9 4c 53 b1 7a c2 e5 e3 be 7d d8 38 b6 dd 3f 69 da e7 03 15 45 00 3e dc 2c 8c 71 ea 27 71 e6 25 d0 24 05 be 47 31 cc 40 1a 3b 64 42 a2 2c c1 59 9e e7 de 5a 61 bc 05 e7 a2 30 3a 59 98 39 31 60 73 bd 2c b1 fc 3c 44 16 b2 9d d8 8a 82 24 77 b2 24 c7 b9 13 5c 29 8c 20 6e 41 90 05 16 8a 63 98 b0 04 c1 1a 4a 5d 18 85 97 06 59 86 7c 27 f2 9c 6b 84 d1 43 41 e8 64 b1 67 f9 76 ee 5b 7e 1c c6 56 ec 06 81 85 63 3f 08 70 6a db 49 e6 5f 29 8c 5e 12 86 45 1c 84 56 92 c3 a2 84 85 14 59 31 f9 27 f2 6d bb 70 d2 28 0f 9d 84 0a a3 09 e0 0d c2 58 b6 e8 50 66 37 0b 23 4e 9c 30 72 41 13 78 a9 47 a8 74 3c 98 5b 1f 26 d8 8b 7d 2f f1 31 ce 7d 77 Data Ascii: 1ce8=k+5;W>lre|$jZ+@ER$Eu{uqfFAaPn7{~\~\vV3<l$/?F5:RvSvn(#_\'\|uSS"8-kP @5Fw>]B^i8{V:Z/YkUNc]]nf[aFV@8'/[=:X,y,QB8eC1<B%`07AEujee4u7w(,,O$c;?*qQ~:T#+,M,vBQYyPmoT+K_I1ILl-?+lr'bV#slgo2Um&.EYO]GEDvQk><2LSz}8?iE>,q'q%$G1@;dB,YZa0:Y91`s,<Dw\) nAcJ]Y|'kCAdgv[~Vc?pjI_)^EVY1'mp(XPf7#N0rAxGt<[&}/1}w

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.914134026 CEST	897	OUT	GET /files/theme/plugins.js?1565969634 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en
May 27, 2022 14:31:07.088587999 CEST	1065	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:06 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Tue, 26 Oct 2021 13:57:33 GMT x-rgw-object-type: Normal ETag: W/"2b8d85f1ea01d2c3e8b962eac8d76a5c" x-amz-request-id: tx000000000000000b88c06-0061a70540-a9f4046-sfo1 X-Storage-Bucket: zb635 X-Storage-Object: b6353ca52760aba4e7547ae9861db68158dc2af0f4febece55e5c775ee4449f5 X-Host: blu72.sf2p.intern.weebly.net Content-Encoding: gzip Data Raw: 33 64 36 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ed 7d 6b 77 1b c7 b1 e0 77 fd 8a d1 87 35 00 1b 02 45 c5 ce 71 c0 d0 0e 4d 41 36 73 c5 c7 11 29 47 bc 5c 1e 69 08 0c c9 b1 00 0c 32 33 20 89 98 fc ef 5b 8f 7e 54 3f 06 00 25 39 37 7b 76 9d 73 22 62 fa 55 5d 5d 5d 5d 55 5d 5d f5 64 e3 eb a7 c9 2f e9 64 92 95 bd bf 1f 27 cf 92 9b 17 bd e7 bd 6f e1 8f 17 cf 37 bf 7d f6 fc 2f cf 5e 7c ff 24 f9 3a b9 ae eb 59 7f 63 e3 9a 6a fe 56 f5 ae f2 fa 7a 7e d1 cb 8b 0d 28 c5 0a bb c5 6c 51 e6 57 d7 75 d2 1e 76 a8 71 f2 f7 a2 cc 3f 26 27 e9 f4 2a 1b 8f b2 72 0b ab bd ce 87 d9 b4 ca 46 c9 7c 0a 9f 92 fa 3a 4b f6 f7 4e 92 31 7f 4e be de 78 d2 be 9c 4f 87 75 5e 4c db b7 f9 74 54 dc 76 93 51 31 9c 4f b2 69 dd 4d b2 bb 59 51 d6 07 e9 24 eb 52 07 97 f9 34 1b 75 92 df 9f 24 49 6b 0e cd ab ba cc 87 75 6b eb c9 93 9b b4 4c 7e 1d 1c bc 3c 7c f3 fe e8 cd e0 d5 de bb c1 71 b2 9d 9c b5 5a dd a4 75 9b 5d 7c cc 6b fc 6b 52 fc 0b ff d9 3f a6 1f 15 fe 7f d1 3a df a2 d6 27 83 e3 93 f7 83 d7 83 fd c1 c1 09 34 d5 40 f4 86 65 96 d6 d9 60 9c e1 af 76 6b 94 df b4 3a 6a c0 93 d3 a3 c1 fb 57 6f 0f 76 4f f6 0e 0f a0 4d 4b 4f 45 43 54 16 00 35 14 ec a7 f5 75 8f 7e f0 58 e9 45 a5 bf c2 9f fc 6d 5a dc c2 b7 97 30 56 0f fe 84 0e 36 be 26 44 57 59 9d a4 49 9d 4f b2 62 5e 27 b7 b0 0e f0 f3 2a bf c9 a6 49 35 2c 66 19 d6 f9 db 2c 2d d3 49 f2 fb 2b 35 fe 43 72 39 95 df 0f e6 93 8b ac 7c d0 bd c8 a2 c3 8b df b2 61 fd 90 0c 8b 69 9d dd 71 51 99 d5 f3 72 5a 25 bf 4f b9 dd 13 5c 27 3d 37 04 e8 84 fb d9 e5 36 ed cb 69 57 77 dd d5 1d f1 2a 25 09 f7 25 1a b5 2f 60 99 5f 4d a9 91 ae 6b 9a 03 66 1f cc cc f3 4b a2 97 b4 bc a2 95 48 f2 2a 49 a7 f0 b3 4c 17 dd e4 36 4b 6e 53 f8 58 17 40 25 d9 70 5e 67 54 f9 72 9a 00 88 59 3a bc 4e a0 49 b9 50 fd e4 80 c3 1c 6a eb f6 d8 7c 04 eb 54 9b 4e 46 05 62 f9 3a 9f 5e f5 b0 0d fc 55 e1 80 73 a4 dd 8b 45 92 8e c7 d4 ff 24 ab af 8b 51 05 7f a7 d0 db 70 98 cd 70 75 2a 68 36 06 48 61 b1 b9 7b 0d 73 4f a2 fa eb fb 1d 2c 7c c0 52 f9 fd 18 a8 78 7a e5 af 99 5e 98 33 85 a4 73 77 69 7e 2a 8a 71 96 4e bd b5 c9 a7 37 c5 c7 8c 86 d9 29 af da 30 50 37 91 88 56 8b 02 18 Data Ascii: 3d69}kww5EqMA6s)G\i23 [~T?%97{vs"bU]]]U]]d/d'o7}/^|$:YcjVz~(lQWuvq?&'*rF\|:KN1NxOu^LtTvQ 1OiMYQ$R4u$IkukL~<\|qZu]\|kkR?:'4@e`vk:jWovOMKOECT5u~XEmZ0V6&DWYIOb^'*I5,f,-I+5Cr9\|aiqQrZ%O\ '=76iWw*%%/`_MkfKH*IL6KnSX@%p^gTrY:NIPj\|TNFb:^UsE$Qppu*h6Ha{sO,|Rxz^3swi~*qN7)0P7V
May 27, 2022 14:31:07.100222111 CEST	1084	OUT	GET /uploads/1/4/1/8/141840186/1screenshot-2021-04-26-at-19-59-20-orig-orig-orig_orig.png HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.270840883 CEST	1103	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: image/png Content-Length: 46476 Connection: keep-alive Last-Modified: Mon, 10 May 2021 13:49:51 GMT x-rgw-object-type: Normal ETag: "86023205c6da4584ac9ad959a7504d4c" x-amz-request-id: tx00000000000000002137be1-006284e178-b9fbc77-sfo1 X-Storage-Bucket: ze542 X-Storage-Object: e542893276ee236968914d1271b54a4afd7df253d4bfb04ff8e5fcda5817e397 X-Host: blu44.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 4f 00 00 00 66 08 06 00 00 00 13 75 aa 79 00 00 b5 53 49 44 41 54 78 da ec 5d 0d 93 e4 a8 0d cd ff ff 9f 49 25 b9 ab 4b d2 36 08 77 cf ac d3 b0 e8 1e 96 60 64 af d7 db b3 7b a2 ea 15 fa 78 c8 18 bb 7b 2c 03 3d 7f 5b bd 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 59 3c 79 f2 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 17 4f 9e bc 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 93 27 2f 5e bc 78 f1 e2 c5 8b 17 2f 5e bc 78 f1 e4 c9 8b 17 2f 5e bc 78 f1 e2 c5 8b 17 2f 5e 3c 79 f2 e2 c5 8b 17 2f 5e bc 78 f1 e2 c5 8b 97 9f 2d 79 5a 52 5a 1d af 00 95 fa be 3c 71 5f d6 07 c0 7a 83 fb 90 73 07 a4 1f b2 a1 c3 ae fc 1a fa 98 fa d8 67 fa 88 da 38 07 33 8e 2d 9b 63 7a ff aa 2f e3 3e 68 d8 fd d4 9c 7b 01 ae f3 1d b6 0c 96 a5 ce 7d 7c 64 1d 72 06 cb b2 ad e6 54 b0 2c 21 38 6f 03 3e ec 90 33 7a f2 db bd 91 0b 1e b5 16 76 f8 35 67 e8 7f 68 bc 3d d6 47 d7 fe 36 92 b9 ce 6d cb d8 2e f9 73 3a c0 a2 60 73 c1 3b ce 5d 24 2f 31 c7 88 cf bc 34 6e 83 98 0d 8c 63 5c e1 e7 be 94 6b fa f6 b8 06 0f db 7f 3c e6 7d 80 87 02 da 30 04 bf 1f 87 6b 7c 0e 75 1b f6 01 b0 fd 50 5d db 0c 3f e4 93 c7 3c ee b7 fb 68 fb af d7 ad 3e bc b2 cf 47 af f5 67 bf 17 5e 7f ed ed 63 be fe fe b5 c7 d1 e6 9f ef 13 e4 d3 f7 c2 bd 2f 7f f9 f2 be 4d 9e e6 db ff d6 79 da 62 12 ba f2 df 7a ba cd 9f 58 3f 19 cf e6 d8 31 d1 17 f8 27 2b de ed c0 f1 8d f3 0c f3 6d 8d 61 5e 13 85 95 32 62 c1 53 8f 4f 3d d6 fa a9 67 c4 af a0 c0 72 e1 d5 ba 22 f3 e3 c8 3f d6 61 8b 19 42 e7 3e 15 7c cc e7 be 07 e8 3d 7f 12 e7 40 76 1f 01 dd c7 02 12 f1 48 c7 de da c3 cc 31 04 9f 6d 73 91 59 8f 51 f1 21 97 9a 65 d9 87 5a 17 5d f0 43 b7 6f e0 07 19 53 f0 03 db f9 5e 61 39 83 d6 58 64 ca 50 1c d8 21 a7 a6 6d 2a 89 7d d5 53 7c ca c5 56 f4 65 29 72 b5 47 c8 a5 ae 6d 33 98 2f 6c dc 3e d7 0b c1 76 af bc fb 52 50 ec f7 82 2a 2f 89 65 24 16 59 ae ba c6 f2 44 e5 dc a5 1d 72 fb 02 03 fe 22 e7 e4 b4 9c 5b 08 d3 1a e6 27 42 c6 ad d6 53 f9 fc c6 e2 83 1f 32 eb cc 07 57 61 2a 1c 85 79 be 15 ff 3c 95 ba 41 cb 9f 8b 3e 67 5e 45 68 f9 a1 ad 4b cc 12 8f db 04 cd c7 31 80 0d 27 ca 5a f5 b1 e8 5b de c4 7c f4 e3 a3 78 7c cc 44 b1 bd 7e 78 e1 b0 34 d7 ad a3 3f 7a fe 04 1b e2 f1 cb 2b d6 c1 67 c0 0f 5d f7 41 bc 10 3b 0c dc f7 4b ae ab 3d eb 83 36 db cf 16 b7 15 48 84 cf 31 7f 5f 40 17 48 52 d6 d0 31 6c 90 e5 37 fb 68 ea da 66 c4 80 7c 0c e8 63 f8 38 46 b4 63 80 73 cd 38 da f1 ed 71 a4 73 e3 78 fe 5a 9f b8 5f cf f5 f1 f8 b5 b6 8f 71 5d 1f 71 ad 5f dd 47 eb 5e 1a c3 fe Data Ascii: PNGIHDROfuySIDATx]I%K6w`d{x{,=[x/^xY<y/^xOx/^x'/^x/^x/^x/^<y/^x-yZRZ<q_zsg83-cz/>h{}|drT,!8o>3zv5g h=G6m.s:`s;]$/14nc\k<}0k\|uP]?<h>Gg^c/MybzX?1'+ma^2bSO=gr"?aB>\|=@vH1msYQ!eZ]CoS^a9XdP!m*}S\|Ve)rGm3/l> vRP*/e$YDr"['BS2Wa*y<A>g^EhK1'Z[|x|D~x4?z+g]A;K=6H1_@HR1l7hf|c8Fcs8qsxZ_q]q_G^

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	54965	151.101.1.46	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.644011974 CEST	231	OUT	GET /css/sites.css?buildTime=1651866883 HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.659873009 CEST	235	IN	HTTP/1.1 200 OK Server: nginx Content-Type: text/css Last-Modified: Thu, 19 May 2022 17:44:26 GMT ETag: W/"628681fa-347ac" Expires: Fri, 03 Jun 2022 19:57:18 GMT Cache-Control: max-age=1209600 X-Host: grn89.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 29746 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:06 GMT Age: 578029 Connection: keep-alive X-Served-By: cache-sjc10034-SJC, cache-mxp6924-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 75 X-Timer: S1653654667.651470,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ec bd 8b 92 e3 b8 91 28 fa 2b 3c 55 d1 31 5d b3 a2 9a e2 43 8f 52 78 8e 3d 63 cf ae 23 76 6d c7 f1 9e bd 27 ee b1 a3 83 92 a8 2a ba 29 51 4b 4a f5 b0 a2 fe fd e2 49 26 5e 24 48 51 35 33 77 ba 35 3d 2d 91 40 22 91 48 20 13 89 44 e6 6f bf 24 af db 22 de 25 a5 53 1e d2 fd d9 fb 70 3e 16 f1 be dc e6 c5 ee be c8 8f f1 31 f9 e8 6d 92 87 bb b7 89 a7 7b 17 4c e9 db b7 4f df fe 0f e7 7f 25 db 2c 79 71 9e 26 e3 68 ec 39 ae f3 78 3c 1e ca fb 4f 9f 1e d2 e3 e3 69 35 5e e7 bb 4f 59 92 fc 23 2f 36 f1 fe 53 41 0b 7f fb 69 fc 50 a4 9b f3 26 2d 0f 59 fc 7a 9f ee b3 74 9f b8 ab 2c 5f 7f 59 f2 87 ee ae 74 71 e9 55 fe 52 3d c3 bf 97 df 8a d5 96 ff cc f3 dd fd 64 c9 cb bb cf 45 7c b8 c7 ff 5b 4a 3f 0f f1 66 93 ee 1f ee bd e5 2e 2e 1e d2 3d fa 72 c8 cb f4 98 e6 fb fb 22 c9 e2 63 fa 94 2c 9f d3 cd f1 f1 1e 77 1c 95 42 b5 eb 9f 59 72 3c 26 85 5b 1e e2 35 86 e2 7a e3 60 92 ec 9c ff 91 ee 0e 79 71 8c f7 c7 e5 b7 52 91 3d 22 5a 9c c1 12 cf 88 0e 10 42 18 88 10 b2 b4 3c ba e5 f1 35 4b dc e3 eb 21 41 10 f6 c9 1b 21 d6 fd 2a 41 63 90 8c e8 8f 78 8b da 39 6b 9b 13 db e0 cf 1e d3 63 42 1e 26 fc 91 d8 3b da 88 f3 ad d0 0c fa 79 79 43 0c 32 1d 71 3e 48 f7 13 67 e2 c4 a7 63 be 14 7e 71 2c ce 68 d0 dd 32 fd 27 06 bc 42 ad a0 b6 d1 93 66 1c f5 55 fe ef 3a 8b cb f2 db df dc e0 b2 9f 3f af f3 cc bd f9 fb 95 18 6f 93 16 c9 9a 70 13 6a e6 b4 db 2f f5 4f 2f 1a b5 46 86 7d 4a 8a 63 ba 8e 33 37 ce d2 87 fd fd 31 af 79 7e e2 1d 18 fd 10 11 92 2c 3b ab 80 78 ef 28 35 da 46 8a 92 e9 94 65 e5 ba 48 92 bd 03 60 8f d0 42 91 1f e1 93 b3 cc 68 74 24 26 3e 78 b1 fc 96 7e 5f 2c c6 0b b1 d4 84 95 5a 4c c6 53 f4 67 56 17 45 8b 0e 79 20 14 f7 58 f1 79 30 0e f0 9f aa 38 7a e0 93 07 b0 f8 82 95 9e 45 55 b9 59 28 61 30 67 65 a6 53 09 01 f4 40 45 60 c6 4a 47 73 a9 7d f4 40 6d 7f ca 4b d7 14 08 65 0a 44 ac 4c 28 13 20 d4 11 20 64 a5 03 b9 ff 81 ae ff 01 2b ed d7 fd f7 e5 fe 57 c3 24 f7 7f a2 eb 3f 1f 2e b9 fb 55 ef 7f bb 4b 36 69 ec 7c dc a5 7b b6 02 39 e1 1c f1 e7 dd 19 40 79 29 2d d9 03 17 ec c6 21 b8 46 37 26 41 35 6c f8 04 15 eb c6 2a a8 42 37 6e 41 15 6c 18 06 15 eb c6 33 a8 42 37 b6 41 15 6c 38 07 15 eb c6 3c 78 6c da f8 47 cb 40 5e b2 13 f8 a7 dc 59 f2 0f 2e d8 8d 7f 70 8d 6e fc 83 6a d8 f0 0f 2a d6 8d 7f Data Ascii: (+<U1]CRx=c#vm'*)QKJI&^$HQ53w5=-@"H Do$"%Sp>1m{LO%,yq&h9x<Oi5^OY#/6SAiP&-Yzt,_YtqUR=dE|[J?f..=r"c,wBYr<&[5z`yqR="ZB<5K!A!*Acx9kcB&;yyC2q>Hgc~q,h2'BfU:?opj/O/F}Jc371y~,;x(5FeH`Bht$&>x~_,ZLSgVEy Xy08zEUY(a0geS@E`JGs}@mKeDL(d+W$?.UK6i|{9@y)-!F7&A5l*B7nAl3B7Al8<xlG@^Y.pnj*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	54918	151.101.1.46	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.644438982 CEST	231	OUT	GET /css/old/fancybox.css?1651866883 HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:06.660440922 CEST	251	IN	HTTP/1.1 200 OK Server: nginx Content-Type: text/css Last-Modified: Thu, 19 May 2022 17:44:32 GMT ETag: "62868200-f47" Expires: Fri, 03 Jun 2022 19:57:23 GMT Cache-Control: max-age=1209600 X-Host: blu108.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 1218 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:06 GMT Age: 578024 Connection: keep-alive X-Served-By: cache-sjc10044-SJC, cache-mxp6920-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1960 X-Timer: S1653654667.651967,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: *

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	59531	151.101.1.46	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.644629955 CEST	232	OUT	GET /css/social-icons.css?buildtime=1651866883 HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:06.660593033 CEST	253	IN	HTTP/1.1 200 OK Server: nginx Content-Type: text/css Last-Modified: Thu, 19 May 2022 17:44:26 GMT ETag: W/"628681fa-3319" Expires: Fri, 03 Jun 2022 19:57:20 GMT Cache-Control: max-age=1209600 X-Host: blu86.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 1640 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:06 GMT Age: 578026 Connection: keep-alive X-Served-By: cache-sjc10031-SJC, cache-mxp6937-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1479 X-Timer: S1653654667.652356,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 5a cb 72 ea 38 10 dd cf 57 64 c8 e6 a6 2a 24 d8 10 02 a6 a6 66 fe 61 b6 b3 91 6d 01 2a 6c 8b b1 45 08 37 95 7f 1f c9 f2 83 47 4b 6a 1b d7 5d 4d 56 29 bb cf e9 a3 3e 46 ef bf d6 3c 13 e3 35 89 e8 57 f5 5f ca 92 53 30 3a 16 3c 62 24 19 ad 8a 3c 0a 0e 79 f2 e3 f5 35 8a 33 ff 85 c6 4c a4 a7 82 09 fa 12 f1 f4 55 61 8a d7 e3 df 65 f0 6b 05 7a a1 5c fc 29 8a 3f bc f9 9b bf 5c f8 fe 7c be 98 2f 9e 06 63 7a 64 74 cd 3e 9f 1e d6 3c 4f 89 f8 31 a2 69 48 e3 98 c6 63 be a7 99 38 ed e9 e8 e9 b9 6b 9e 23 5f af 6f 25 37 29 d4 eb 1e ac 42 d8 48 45 7e a0 3d e5 16 1f 9b db b2 54 2f db 04 32 6a f4 b4 2a 6d 3d 52 b6 d9 8a 20 53 6f 12 fd a8 10 a7 84 56 4f be 5f 8e 2a e3 58 33 8c e3 9c 85 61 28 df 86 54 72 d1 af 48 c6 cb d2 06 a3 7f e8 7c 12 8d ea 68 a9 6f bc cf 79 7c 88 44 47 64 15 1d f1 84 e7 0f 9d 72 af 4a 4c f0 b8 9e bc bf 93 c9 15 5f f1 ef 81 e4 d4 40 f8 0c c5 c2 a1 5f 21 89 76 9b 9c 1f b2 78 dc 3b 5f 40 d6 82 e6 1d b2 6a 80 b1 c1 e5 df 95 80 94 b0 04 2c d4 d4 66 12 02 65 31 c8 82 ae b5 4e e7 d3 70 4a 31 c5 52 64 88 12 a9 30 c0 94 6e 79 d0 86 b4 c1 a6 06 82 66 a8 4e 34 e4 7c 07 16 67 62 33 04 89 b4 98 e2 60 68 8c 09 df 96 cb 05 a6 60 35 21 a2 5c 75 28 64 50 e7 7c 68 93 2e 01 a6 06 c3 46 25 2c da e5 e3 84 ae 05 58 af d8 ea 15 1a 6c b3 cb 49 52 37 60 32 99 4f e3 08 55 c1 96 13 53 be 36 1a f0 ad 57 56 bc 75 d7 18 53 e3 6d ee e5 e5 80 06 15 8f 22 ec c3 a0 dd fe d9 58 da 36 4c 26 8b 59 87 52 96 a4 f8 2a 96 e1 d0 80 d5 2b 6f 57 0f cf 40 e6 02 18 4d 04 4b b7 70 db e7 c0 39 8d 33 e0 fb fe e6 d0 e5 1a e0 97 d6 d1 20 c8 9a 85 dd 9a 7d 72 28 c0 02 cd 6c c6 20 50 16 5b 2c e8 5a 6b 1c cf c2 e9 12 53 28 45 86 28 90 0a 03 0c e9 96 07 6d 47 1b 6c 6a 20 68 06 cb 0a 41 36 39 49 c1 ea bc db 1c c1 42 2d b6 b8 28 9a 69 c5 fa dd 5f 86 98 9a 35 8c 88 92 35 b1 d0 c4 a2 7b 46 b4 55 57 08 53 a3 41 bf 12 96 ed e4 0a 2e 03 0b e6 db ec 42 22 2d 6e 39 18 1a b3 16 0b 12 a2 26 cd 35 21 a2 66 75 28 64 55 e7 7c 68 a7 2e 01 a6 06 c3 bd 1c 93 b1 39 2d e0 e1 7b 69 ed ea 90 50 5b 7f e7 a0 a8 a5 47 91 ef f9 ef a8 ce a8 66 c4 f4 45 75 2c e0 56 8f 8c f8 3e f0 12 61 6a 34 e8 57 5e c0 03 c4 9b cd 29 37 c8 e2 91 19 dc 08 f5 e7 6f be 8f a9 95 e4 42 d4 47 46 41 13 b9 2e 59 d0 5e 34 b1 c6 c6 41 2e 88 43 1a 26 e0 Data Ascii: Zr8Wd*$fam*lE7GKj]MV)>F<5W_S0:<b$<y53LUaekz\)?|/czdt><O1iHc8k#_o%7)BHE~=T/2j*m=R SoVO_*X3a(TrH|hoy|DGdrJL_@_!vx;_@j,fe1NpJ1Rd0nyfN4|gb3`h`5!\u(dP|h.F%,XIIR7`2OUS6WVuSm"X6L&YR*+oW@MKp93 }r(l P[,ZkS(E(mGlj hA69IB-(i_55{FUWSA.B"-n9&5!fu(dU|h.9-{iP[GfEu,V>aj4W^)7oBGFA.Y^4A.C&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	58024	151.101.1.46	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.645133018 CEST	232	OUT	GET /js/lang/en/stl.js?buildTime=1651866883& HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.661313057 CEST	265	IN	HTTP/1.1 200 OK Server: nginx Content-Type: application/javascript Last-Modified: Thu, 19 May 2022 17:43:17 GMT ETag: "628681b5-2c075" Expires: Fri, 03 Jun 2022 19:57:18 GMT Cache-Control: max-age=1209600 X-Host: grn87.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 32604 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:06 GMT Age: 578028 Connection: keep-alive X-Served-By: cache-sjc10043-SJC, cache-mxp6932-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 22 X-Timer: S1653654667.652116,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 1f 8b 08 00 00 00 00 00 00 03 cc bd db 76 1b 49 92 20 f8 dc fd 15 51 d5 d5 25 e5 94 88 14 25 e5 4d 95 95 35 bc 49 a2 44 52 4c 82 94 5a 39 9a c1 71 00 0e 20 c4 40 04 32 2e a4 90 6a 9d d3 2f fb 05 bb 2f f3 38 67 1f f6 cc 43 bf cd 1f e4 9f f4 97 ac dd dc c3 03 f0 40 04 40 68 67 cf 51 26 23 02 e6 e6 e6 ee e6 e6 66 e6 e6 e6 ff 78 1b c6 c3 e4 b6 d3 7b 1b fc 2d 90 e7 b7 5a f7 a3 f9 d2 fb bf fe 6b f0 e9 f3 5f ff b1 f7 b6 33 d6 79 37 cc f5 89 8a c7 85 1a eb ab 8b 13 00 1e 15 f1 20 0f 93 f8 7e 04 9f bf fa f4 8f ff 90 ea bc 48 e3 e0 de d7 5f ab 2c d3 79 b6 93 e5 6a 1c c6 e3 ce 2d e1 eb c4 3a ff fa 43 f6 35 82 7f fd cf f8 ff 7f fe 3a cb a3 ce 87 ec ef fd 22 8c 86 97 e1 54 ff 6d f7 d1 e3 27 7f be d7 49 f5 2c 52 03 7d ff 1e c3 dd 7b 10 50 25 7f fd c7 cf 48 4e 1e 85 7f b3 b5 67 5f 7d 92 8a b3 bf d2 af 99 50 0a 24 de d3 f1 3d 6a c0 28 8f fe 86 3f c1 9f fb b6 e4 57 01 10 7d a3 d2 60 e4 b6 26 a3 cf f4 3d 87 ef 79 94 fd 97 ec bf 62 5f 64 7f 95 cf 0a 3e ef a5 a9 9a 77 66 69 92 27 f9 7c a6 3b 59 14 0e 74 67 a0 a2 e8 be 4a c7 c5 54 c7 79 f6 20 d8 fd 0a cb 8c 92 34 b8 8f 05 43 28 f8 f0 af f0 e7 c7 40 75 22 1d 8f f3 09 bc fd e5 2f 5c e3 3f 50 75 9d 6c 16 85 f9 fd 7b 9f 3e dd fb 4b f8 97 7b 9f 3f df fb aa f3 21 09 e3 fb ea bf 84 ff 95 d0 7d 86 ff e0 9f 34 3a 0f fe 0e 85 4c 7f 7d fd df de bf cf fe d3 fd ce 5f fe fe 15 3e fc e9 eb 07 c1 bd 3f ed de fb 2a 78 4a e4 7f 7e f0 8f ff 00 0d 82 7a 5e 76 5f 9f 75 66 2a cd a0 8f 3f bd ff 63 3e d1 53 dd 19 ea 5c 85 51 f6 fe 8f 4f df ff f1 d0 3c 3f 30 bf 66 45 1f 1a ab 22 fa b9 6b 5f ec ef 83 89 1e 5c 27 45 4e bf 1f d8 17 fb 7b aa d5 f0 2c b9 a5 9f 2f e0 39 a0 17 fb 73 5f 0d ae 2f 93 fd 28 19 13 c4 3e bc 06 79 12 f0 87 92 88 89 4a 35 53 c0 4f 0f 4a e2 b3 41 1a ce 70 0c a5 01 ce bb 85 fa 35 9f d3 af 3f e3 5f fc aa a7 d0 73 b9 ce 3a 3a d2 34 6a 9d 41 92 5c 87 7a 27 99 e5 3b d0 80 ce 30 cc 06 91 02 de 4c a9 e0 e5 24 cc 82 5b dd 47 2e 0b 8a 4c 67 c1 54 a5 d7 3a 07 3e 0f 54 3c 0c f2 14 08 c7 97 5c 0f 26 71 02 d4 87 80 3c 78 3d 23 08 40 18 24 a3 20 27 24 61 14 05 50 4b 30 4f 0a f3 03 f0 4f c0 f5 03 f7 e8 8f 03 0d 3f 23 fb e4 93 24 d3 41 ac f5 50 0f b1 57 d2 02 46 7e a2 0d 21 1d e8 4b 20 27 9f a8 3c c8 92 a9 0e 80 31 87 c5 20 47 e2 e6 41 9c Data Ascii: vI Q%%M5IDRLZ9q @2.j//8gC@@hgQ&#fx{-Zk_3y7 ~H_.yj-:C5:"Tm'I,R}{P%HNg_}P$=j(?W}`&=yb_d>wf i'|;YtgJTy 4C(@u"/\?Pul{>K{?!}4:L}_>?*xJ~z^v_uf*?c>S\QO<?0fE"k_\'EN{,/9s_/(>yJ5SOJAp5?_s::4jA\z';0L$[G.LgT:>T< \&q<x=#@$ '$aPK0OO?#$APWF~!K '<1 GA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	56565	151.101.1.46	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.645284891 CEST	233	OUT	GET /js/site/main.js?buildTime=1651866883 HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:06.661016941 CEST	259	IN	HTTP/1.1 200 OK Server: nginx Content-Type: application/javascript Last-Modified: Mon, 23 May 2022 16:19:09 GMT ETag: "628bb3fd-74804" Expires: Tue, 07 Jun 2022 10:01:47 GMT Cache-Control: max-age=1209600 X-Host: blu85.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 146400 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:06 GMT Age: 268159 Connection: keep-alive X-Served-By: cache-sjc10042-SJC, cache-mxp6962-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 605 X-Timer: S1653654667.652785,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: *

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.037585020 CEST	898	OUT	GET /js/site/main-customer-accounts-site.js?buildTime=1651866883 HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 14:31:07.053304911 CEST	900	IN	HTTP/1.1 200 OK Server: nginx Content-Type: application/javascript Last-Modified: Thu, 19 May 2022 17:44:49 GMT ETag: "62868211-8250f" Expires: Fri, 03 Jun 2022 19:57:19 GMT Cache-Control: max-age=1209600 X-Host: blu94.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 158975 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:07 GMT Age: 578028 Connection: keep-alive X-Served-By: cache-sjc10033-SJC, cache-mxp6962-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 5 X-Timer: S1653654667.045205,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 1f 8b 08 00 00 00 00 00 03 e4 bd 7b 77 db 46 f2 28 f8 ff 7e 0a 09 e3 91 01 13 a2 44 d9 71 62 d0 08 af fc 4a 3c 63 c5 1e 4b 1e 27 a1 18 2e 44 36 25 d8 14 c0 00 a0 65 45 e4 7e f6 ad 47 3f 01 50 b6 e7 37 77 cf 3d 67 f3 10 81 46 3f aa bb ab eb d5 d5 d5 fe 6c 99 4d aa 34 cf 7c 11 dc 7c 4a 8a ad 2a be 59 f7 55 e2 56 e6 17 c1 4d 3a f3 ab 61 31 0a 0a 51 2d 8b 6c 0b 9f bb e2 f3 22 2f aa b2 8f 45 d2 18 93 e2 1b 99 16 dd ac c3 74 1a 15 e1 3c 4f a6 62 1a cd 92 79 29 d6 7d 81 c5 26 c9 7c ee a7 aa 74 98 86 e6 39 0b fa 69 97 8b c4 55 b1 14 7d d9 9c ce b1 ce ba 97 b1 e8 67 dd 49 5c c1 df 45 ec 5d 54 d5 a2 8c f6 f6 26 d3 ec a0 2b a6 69 75 79 5d a6 95 e8 4e f2 cb bd 0f e5 9e e7 e6 f2 3a 57 69 36 cd af ba 87 c7 c7 cf 4f 8e c7 4f 0e 8f 9f 77 3c ca b8 5a 41 4e d5 60 e6 ef 07 eb c0 1f 9a 91 09 2b 80 ee 46 28 40 e2 cc bf 7f d0 0b d6 61 3d 07 0e 46 d1 df f6 8b 58 7f a1 d1 93 ed be 17 e2 6c 7e bd 1d c7 cb 6c 2a 66 69 26 a6 3b 3b ce a7 ee 87 7f 2d 45 e1 e4 08 6e 24 54 6d 19 d7 ee 37 99 c8 83 0c 00 01 50 22 08 0b b7 41 df 74 a3 08 36 f5 21 4c a9 17 c3 cc ef 05 a3 30 8d 6d 24 71 00 89 e5 db f8 bd 79 5a ad 00 83 f4 5b 77 59 cd 63 e7 6d b5 6a a9 0e 3e cd 92 74 2e a6 27 f3 32 6e 49 5b ad 86 a3 7e 4b 7a 77 b1 2c 2f a0 1e 35 79 c2 6e 7a e6 34 3d fb 52 d3 2f aa 96 b6 31 b1 b5 71 fc 50 6b dd f3 fe 07 1d 7f d7 d6 fa bb 4d ad bf fb 52 eb a5 d3 7a f9 a5 d6 8f db 5a 3f de d4 fa f1 17 5b 17 d5 d3 3c ff 98 8a b8 15 bf e2 4c 5c 6d 3d 4b 2a 58 e4 98 f5 24 bd 14 7e d1 3d 97 4f 41 27 bb 77 f0 e0 de c3 7d fc af 27 ee 07 92 ca 78 80 b8 69 21 ca d8 eb 14 dd 2a 7f 77 f2 f4 b8 2a d2 ec dc 0f fa d3 7c b2 bc 14 59 05 4b 9f 5a 15 1d 0f 72 55 1d af bf e5 75 52 1b b2 c9 5c 24 45 03 36 7b 40 34 ec 00 b2 e7 85 bb b0 d2 ad f2 e7 2d 3d 53 94 93 5a 25 60 b3 b8 06 51 b7 5c cc d3 ca f7 fa 5e d0 9f e5 85 cf c3 b0 df 2f 1e 67 dd b9 c8 ce ab 8b 7e d1 e9 70 45 69 9c 01 ad ec 5f 5d c0 50 03 b1 9c 5c 24 c5 61 05 44 29 8e bd 2d 2f 48 e3 b4 5b 2e cf 4a ee 7a 0f a8 e6 0c 32 01 7c e2 f3 6b 20 d4 90 6b 3f d0 a4 d3 64 ac 64 33 40 71 f9 21 58 b7 4d 1c d3 10 20 b3 26 e9 ed f3 a7 87 6f 4e 9e fe 7c 38 7e f3 ee c9 ab 97 4f c7 ff 7c fe 9b 44 95 a1 d7 f6 d1 1b c5 de c3 57 b3 07 af 1f bd 3b 3e c4 7f 5e 1f 27 8f 26 2f 1e 1c Data Ascii: {wF(~DqbJ<cK'.D6%eE~G?P7w=gF?lM4|J*YUVM:a1Q-l"/Et<Oby)}&|t9iU}gl\E]T&+iuy]N:Wi6OOw<ZAN`+F(@a=FXl~l*fi&;;-En$Tm7P"At6!L0m$qyZ[wYcmj>t.'2nI[~Kzw,/5ynz4=R/1qPkMRzZ?[<L\m=K*X$~=OA'w}'xi!*w*|YKZrUuR\$E6{@4-=SZ%`Q\^/g~pEi_]P\$aD)-/H[.Jz2|k k?dd3@q!XM &oN|8~O|DW;>^'&/
May 27, 2022 14:31:07.525486946 CEST	1247	OUT	GET /js/wsnbn/snowday262.js HTTP/1.1 Host: cdn2.editmysite.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.541167021 CEST	1249	IN	HTTP/1.1 200 OK Server: nginx Content-Type: application/javascript Last-Modified: Wed, 25 May 2022 14:22:37 GMT ETag: "628e3bad-124fe" Expires: Thu, 09 Jun 2022 08:38:41 GMT Cache-Control: max-age=1209600 X-Host: blu11.sf2p.intern.weebly.net Content-Encoding: gzip Via: 1.1 varnish, 1.1 varnish Content-Length: 25752 Accept-Ranges: bytes Date: Fri, 27 May 2022 12:31:07 GMT Age: 100346 Connection: keep-alive X-Served-By: cache-sjc10069-SJC, cache-mxp6962-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1953 X-Timer: S1653654668.533048,VS0,VE0 Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 1f 8b 08 00 00 00 00 00 03 c4 7d 6b 7b da c8 92 f0 e7 33 bf c2 d6 d9 f5 48 43 1b 03 be 06 ac 78 6d 27 76 ee c9 24 76 9c 84 30 7e 1a 10 20 0c 08 24 71 b3 61 7f fb 5b 55 7d 51 4b e0 24 73 ce ee be e7 64 8c d4 97 ea ee ea ba 75 a9 db 6e 8d 07 8d d8 0f 06 1b 9e 5d 67 6d d6 74 1e 74 4a c3 1e b0 ae f3 e0 b7 ec cd 76 75 50 13 4f 75 7a 9a f0 70 c3 77 e3 f9 d0 0b 5a 1b a1 37 1a fb a1 e7 ba 96 aa 6a 6d 6d c9 c4 0a d6 e9 6e 6d f9 ce 43 e8 c5 e3 70 b0 e1 03 d4 cd 82 b3 84 0c ae 13 b9 4c 44 b8 7d 77 e0 4d 37 9e 87 61 10 da d6 39 1f 0c 82 78 a3 e5 0f 9a 1b fd a0 39 ee 79 1b bf 5b b9 41 ce fa dd 72 2a 71 27 0c a6 1b fd 7c 23 68 7a ae f5 f6 fd b3 eb 37 cf 6f df bd bf ba bd 78 7f fd ee 99 c5 fa 04 af e3 62 ef dd 07 6f 36 0c c2 38 2a 3f 2c 97 15 1c 45 b5 50 cb 37 78 af 67 77 f2 32 8b a9 fe db 3d 31 c4 c0 a5 82 c5 5a b5 57 ab c8 ae 36 ec e0 24 28 f7 9c 25 eb b0 a4 a6 c7 04 f6 96 b2 14 36 a9 32 a9 17 fc 97 b0 d5 82 31 63 e9 96 5b a8 b4 8e 9b f9 9e 37 68 c7 9d 4a 2b 97 73 1e 1a 76 b3 da aa e9 16 1a 4b c7 7e 28 96 ab ba cf 12 06 13 68 62 b2 71 31 90 57 9f de bf a3 a9 c0 07 e7 01 ff ba 80 07 5b 57 16 c5 da bd a0 ce 7b ee 85 4a b5 64 5b 71 c7 8f 2c c7 76 18 55 14 a5 f2 8f c0 d4 e4 d3 b2 07 7a 7e 07 c7 c5 c2 89 55 80 99 2b 0f 70 e6 25 2e 9e f1 d8 cb 0f c3 20 0e 30 21 1f 07 08 64 d3 44 8d f3 b0 b6 8c ab 3b 7e e7 cd 13 d2 8a 2e fc 81 1f 7b 36 f6 37 3f e1 bd b1 f7 be 65 3b ce 09 bd b7 bd f8 fa ea fc 62 dc eb 7d f5 78 68 3b 39 6b db ca b5 6c 23 ef 6d 30 88 3b 90 51 5c 93 87 dd 00 50 39 eb 2a 93 f1 22 18 87 11 e5 94 b3 e0 fc c1 38 f6 d6 e7 7d f2 1a c1 a0 29 f2 be 59 e5 01 f4 ea b7 65 e5 53 1c fa 83 f6 ea 68 df 8d fb 75 2f 5c 4d 3f 0b 82 9e c7 07 bf 88 9e 34 56 96 44 96 8d 99 bb 53 fd 3e 2e c0 ff f0 2f 6f c2 df 83 42 61 9b 7e f6 e0 ef 61 a1 f5 7d 5c 3c ac ef d1 df fd ef e3 52 a1 d0 d8 a6 9f 16 fe 2d 1d d1 4b 89 5e 0e 0a f4 72 00 2f 2d af 85 7f 5b 2d 4c 82 9f 56 6d a7 cd bc a8 c1 87 bc de f3 b0 d1 ef df ad ef 33 6c 6a 56 6c 7d 9f 1d b6 e0 e1 49 eb ff a0 13 6d 3e 64 c0 4e bc 41 cc fa 5e cc dd 07 eb 7b 1d e6 e7 3b fc 65 d6 f7 98 1e 63 7c 1c d0 e3 00 1f 5b f4 d8 c2 c7 90 1e 43 8b fd 6e fd 5e fe 1d 06 f1 3b 24 7e a7 44 f8 59 b2 d0 1b 56 f4 1a 18 8d 03 20 9b 88 a6 d5 79 Data Ascii: }k{3HCxm'v$v0~ $qa[U}QK$sdun]gmttJvuPOuzpwZ7jmmnmCpLD}wM7a9x9y[Ar*q'|#hz7oxbo68*?,EP7xgw 2=1ZW6$(%621c[7hJ+svK~(hbq1W[W{Jd[q,vUz~U+p%. 0!dD;~.{67?e;b}xh;9kl#m0;Q\P9*"8})YeShu/\M?4VDS>./oBa~a}\ <R-K^r/-[-LVm3ljVl}Im>dNA^{;ec\|[Cn^;$~DYV y

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	54558	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:06.916435957 CEST	897	OUT	GET /files/theme/custom.js?1565969634 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.093554974 CEST	1083	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Thu, 14 Oct 2021 18:47:17 GMT x-rgw-object-type: Normal ETag: W/"48e887857aec23f184b0aa49c18d2445" x-amz-request-id: tx000000000000000d1c66f-0061a70293-a9f3e81-sfo1 X-Storage-Bucket: z0567 X-Storage-Object: 0567021bc3973d113c6b0b6e68d0e9a8b53f38a7f60716c83214a133cc00139a X-Host: blu78.sf2p.intern.weebly.net Content-Encoding: gzip Data Raw: 37 31 38 0d 0a 1f 8b 08 00 00 00 00 00 00 03 e5 58 5b 6f db 36 14 7e cf af e0 dc 60 92 51 5b 71 b7 15 28 9a 3a 40 d7 a5 6b b0 76 d8 90 02 7b 28 8a 81 96 68 8b 2b 25 0a 14 e5 0b d6 fc f7 9d 43 52 12 25 4b 4e da 61 4f 0b 10 d8 16 c5 73 f9 ce 77 2e e4 5f bf 57 4c 1d c2 75 95 c7 9a cb 3c 3c 9f 92 bf cf ce 08 fc 5d 5c 90 d7 7c cf 12 92 d3 ad 79 70 1e ad f3 28 4e 59 fc e9 0d a3 09 53 bf c9 92 e3 1e 9e 6f c8 92 34 12 ca 58 49 21 ae c5 8c d8 6f af 04 2d 4b 94 4a dc df 96 2a 72 9e 31 d8 73 1e ea 94 97 d3 cb b3 66 8d af 49 f8 0d 2c 46 82 e5 1b 9d fa db 08 51 4c 57 2a bf 6c 9e dc f9 fb c2 f3 46 f3 34 b2 df de cb 22 9c 92 2b f2 74 d1 95 43 50 7d 44 93 c4 98 16 fa 66 7a c2 09 13 25 3b 25 78 b9 5c 92 41 c9 8a 65 72 cb 4e 0a 37 df ee 8c e3 80 f3 3b b9 e2 82 91 92 27 6c 45 55 79 e6 b0 66 fb 82 e6 09 5d 09 76 6b 57 7c 98 ed 22 4b 3a f0 b6 d0 22 b0 0e 57 34 09 36 04 b1 e0 f1 a7 60 d6 8a 68 6d 07 2f 0d ea 29 2d ad d9 5d e9 be 93 1d e8 ba af d5 fe 39 e8 ba 7b 7c 50 46 b6 59 50 cc ef 3b 87 cc 4d ae 99 da 52 41 84 94 45 8d 0b 77 0f df c2 33 1f 92 58 e6 89 61 e4 8c d0 d8 7e 26 95 a2 f6 9b e0 19 d7 3e 4e b1 ac 50 0e 08 58 5c 36 0f 51 8d 79 56 32 5d eb 6e 93 63 da e2 45 c2 7a ff d5 d2 ca 26 9f 3f 7b 29 72 b3 be 16 2c 63 b9 be de f3 52 97 ad 6d 1d 30 63 c1 a8 6a f4 58 e5 e3 30 52 67 45 cb 23 67 c3 e3 c7 3d 0c 5b c7 3b 68 be 42 cb d0 78 66 6d 23 cc 18 77 46 c6 0d ef 64 36 6c 8b b5 54 b5 07 36 1f 21 8b 9b 05 97 b6 8d 4e 84 74 c5 55 52 b2 03 7b 25 73 8d b9 60 e0 b5 02 78 ce f5 f3 56 be 2c b4 57 28 cc 5e 5a f6 c8 0c a6 86 c1 4a 26 87 60 3a 52 8b c2 1d cf 13 b9 9b 91 80 ae d7 7c 1f b4 e5 05 10 78 99 24 00 3a b0 8e 95 44 cb 1a 87 d2 bd 80 ea a2 3f 6b 76 b3 32 6c f7 9a 0c 69 34 37 79 12 ec 40 2f 9b 33 88 ad 54 c1 94 7c fb 2d da f7 c8 3e 85 c2 39 8f a9 d2 73 1a 4c 07 0a da c8 8b a9 ce 44 78 6a 6d 0a b9 54 08 1a b3 f0 e2 43 38 fd 78 b1 01 57 83 a9 97 46 ee 0b 50 f8 3d cf 98 ac f4 00 83 6b 67 0d 86 af 40 fe 8d 66 59 e9 73 cb 81 a1 35 8d d3 eb 2d a2 e4 af 9a ba f8 40 47 ff 33 57 6b be 3b 15 d1 8a e6 39 53 f3 9d a2 05 89 20 e3 34 e5 f0 1b 99 02 a1 9a 14 10 58 e0 c7 5c cb 62 32 b3 ef 3b 6a ce 53 43 22 78 11 c0 62 ea 0d e3 9b 54 43 79 7c 4c 26 c5 7e d2 22 3b 23 4f 9e 2e 16 ee f7 dd cc 02 ed f1 e5 f9 50 6d 1d e3 b1 63 e3 1a 34 43 22 58 56 22 27 01 05 50 2c e4 46 c2 87 f5 c8 77 d2 31 b0 29 c1 01 0a 98 f3 7c 84 e7 b5 44 8e e1 25 3b ae 53 52 56 ab ba a5 5b d8 2c fa 90 08 d5 3c 61 6b 5a 09 0d 0a d6 Data Ascii: 718X[o6~`Q[q(:@kv{(h+%CR%KNaOsw._WLu<<]|yp(NYSo4XI!o-KJ*r1sfI,FQLW*lF4"+tCP}Dfz%;%x\Aer N7;'lEUyf]vkW|"K:"W46`hm/)-]9{|PFYP;MRAEw3Xa~&>NPX\6QyV2]ncEz&?{)r,cRm0cjX0RgE#g=[;hBxfm#wFd6lT6!NtU R{%s`xV,W(^ZJ&`:R|x$:D?kv2li47y@/3T|->9sLDxjmTC8xWFP=kg@fYs5-@G3Wk;9S 4X\b2;jSC"xbTCy|L&~";#O.Pmc4C" XV'"P,Fw1)|D%;SRV[,<akZ
May 27, 2022 14:31:07.150634050 CEST	1085	OUT	GET /uploads/1/4/1/8/141840186/editor/2screenshot-2021-04-26-at-19-59-12-orig-orig.png?1652460803 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.327341080 CEST	1165	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: image/png Content-Length: 47588 Connection: keep-alive Last-Modified: Fri, 13 May 2022 16:54:01 GMT x-rgw-object-type: Normal ETag: "e9f5fab58c91223b66dbc7d8a8d064f2" x-amz-request-id: tx000000000000005faddd7-006289556d-b9fbc63-sfo1 X-Storage-Bucket: z3b1f X-Storage-Object: 3b1f7691ebb9f6305b70a17a304ed4f6f84d9153ccf6ba7dafcf6e613ab19816 X-Host: blu78.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 f5 00 00 01 0c 08 06 00 00 00 dd d5 2f c0 00 00 00 01 6f 72 4e 54 01 cf a2 77 9a 00 00 80 00 49 44 41 54 78 da ec fd f9 73 1c 49 96 e7 09 7e 54 d5 cc dd e1 8e fb 22 40 f0 be 19 f7 9d 11 99 19 79 54 1e 95 9d 59 95 d5 d7 4c cf c8 c8 8a 8c ac c8 8a ec 0f fb d7 ec 6f 2b bb 23 3d bb db 3b 3b 3d dd 5b 53 5d 9d d9 9d 95 95 57 45 64 46 c6 7d 91 41 32 78 13 bc 71 df 80 bb 99 ea db 1f d4 cc dc 1c 04 49 90 04 0f 80 f6 15 41 10 e1 70 37 57 33 35 d3 a7 ef bd ef fb 3e 25 22 42 81 02 05 0a 14 28 50 60 d3 43 3f ee 01 14 28 50 a0 40 81 02 05 36 06 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 05 0a 14 28 50 a0 c0 16 41 61 d4 0b 14 28 50 a0 40 81 2d 82 c2 a8 17 28 50 a0 40 81 02 5b 04 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 05 0a 14 28 50 a0 c0 16 41 61 d4 0b 14 28 50 a0 40 81 2d 82 c2 a8 17 28 50 a0 40 81 02 5b 04 85 51 2f 50 a0 40 81 02 05 b6 08 0a a3 5e a0 40 81 02 05 0a 6c 11 14 46 bd 40 81 02 05 0a 14 d8 22 28 8c 7a 81 02 05 0a 14 28 b0 45 50 18 f5 02 05 0a 14 28 50 60 8b a0 30 ea 8f 03 f2 b8 07 50 a0 40 81 02 05 b6 22 82 c7 3d 80 a7 06 22 ab fe 05 14 e9 7f 3c 94 ba c7 83 16 28 50 a0 40 81 02 4d 14 46 fd a1 42 bc f1 4e 0d b9 d6 6b 1b 6e e7 9a ef 47 15 c6 bd 40 81 02 05 0a dc 17 94 88 14 c1 e0 87 01 11 40 12 03 ad 9a af 2d 2f c2 e2 22 04 01 54 db a1 54 ba d5 88 4b 6a e4 0b 03 5f a0 40 81 02 05 d6 8f c2 a8 6f 18 a4 99 2b 5f 6d 88 57 96 90 a9 09 e4 c6 55 b8 f0 35 ee f2 05 a4 52 c3 ec 39 88 1a da 8e f4 f4 a1 bb fb bc 91 0f c3 35 0e 9d 9b a2 c2 c8 17 28 50 a0 40 81 db a0 30 ea 0f 0c 69 e6 c7 85 a6 d1 b5 31 cc cf 22 57 2e 61 cf 9d c2 5d f8 1a 77 ed 32 6e f2 26 6e 7e 0e 82 00 dd d5 83 ee ea 41 f5 0e a0 87 b6 63 b6 ef 46 6d df 0d 43 23 a8 8e 2e 30 81 0f d9 67 5f b5 6a aa 0a 03 5f a0 40 81 02 05 72 28 8c fa fd 40 92 b0 7a fa 6f 0a e7 a0 be 02 37 ae 60 47 cf e1 ce 9e f2 06 fd c6 15 dc e2 3c 12 45 a0 35 a2 35 88 a0 9c f5 ff 9a 00 55 2e a1 da 3b d1 03 c3 e8 91 3d e8 1d 7b d0 43 3b d0 43 23 d0 37 00 a5 0a 18 93 1f 44 6b 64 60 f5 58 0a 14 28 50 a0 c0 53 87 c2 a8 af 1b 6b 90 de 52 34 ea c8 e4 38 72 f5 22 72 e9 2c f6 fc d7 c4 17 cf e1 26 c7 90 46 1d 51 0a a5 74 52 40 b8 ca 00 a7 b9 77 91 ec d8 ca 04 a8 5a 27 7a 60 1b c1 c8 6e f4 c8 6e d4 d0 08 6a 70 18 d5 37 08 1d dd 3e 17 df 32 bc e4 38 a8 1c a1 be 30 Data Ascii: PNGIHDR/orNTwIDATxsl~T"@yTYLo+#=;;=[S]WEdF}A2xqIAp7W35>%"B(P`C?(P@6Q/P@^@lF@"(z(EP(P`0(PAa(P@-(P@[Q/P@^@lF@"(z(EP(P`0(PAa(P@-(P@[Q/P@^@lF@"(z(EP(P`0P@"="<(P@MFBNknG@@-/"TTKj_@o+_mWU5R95(P@0i1"W.a]w2n&n~AcFmC#.0g_j_@r(@zo7`G<E55U.;={C;C#7Dkd`X(PSkR48r"r,&FQtR@wZ'z`nnjp7>280
May 27, 2022 14:31:07.874495983 CEST	1379	OUT	GET /files/theme/fonts/1e9892c0-6927-4412-9874-1b82801ba47a.woff?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.1653687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:08.047967911 CEST	1432	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: font/woff Content-Length: 20710 Connection: keep-alive Last-Modified: Wed, 11 Dec 2019 02:22:43 GMT ETag: "9df5efadcd24b83511f3c339178210d8" x-amz-request-id: tx000000000000000092316f9-005eaa5727-10e2649-las X-Storage-Bucket: z0d88 X-Storage-Object: 0d887fc553f2b9a6488c8bbdeb38d0e70e2da58d5bb34161d32f683af096fdb8 X-Host: grn45.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 77 4f 46 46 00 01 00 00 00 00 50 e5 00 10 00 00 00 00 99 10 00 01 00 00 00 00 4d 58 00 00 03 8d 00 00 07 c8 00 00 00 00 00 00 00 00 47 50 4f 53 00 00 01 6c 00 00 06 b6 00 00 1e b2 ec ec 14 b3 4c 49 4e 4f 00 00 08 24 00 00 00 12 00 00 00 12 93 af c8 c2 4f 53 2f 32 00 00 08 38 00 00 00 58 00 00 00 60 65 f1 01 d7 63 6d 61 70 00 00 08 90 00 00 00 98 00 00 00 cc 90 e6 b0 e3 63 76 74 20 00 00 09 28 00 00 00 4e 00 00 01 e2 07 7a 07 d7 66 70 67 6d 00 00 09 78 00 00 05 ed 00 00 0a a2 63 0e 9d d9 67 61 73 70 00 00 0f 68 00 00 00 08 00 00 00 08 ff ff 00 04 67 6c 79 66 00 00 0f 70 00 00 33 2a 00 00 58 10 b3 67 b4 92 68 65 61 64 00 00 42 9c 00 00 00 36 00 00 00 36 f4 0f af ac 68 68 65 61 00 00 42 d4 00 00 00 1f 00 00 00 24 07 59 07 8a 68 6d 74 78 00 00 42 f4 00 00 02 05 00 00 03 78 d7 00 2c e7 6c 6f 63 61 00 00 44 fc 00 00 02 45 00 00 03 7c 00 27 77 bc 6d 61 78 70 00 00 47 44 00 00 00 20 00 00 00 20 03 33 0b 90 6e 61 6d 65 00 00 47 64 00 00 03 f9 00 00 09 94 3c 21 96 46 70 6f 73 74 00 00 4b 60 00 00 00 13 00 00 00 20 ff 9f 00 32 70 72 65 70 00 00 4b 74 00 00 01 e4 00 00 02 4c 66 9a cf 76 78 9c c5 59 4b 6c 54 55 18 fe fa a4 2d d3 0e ed 50 28 94 e2 50 86 96 96 be 0b a5 85 4a c4 b4 80 bc 8c e5 2d 68 10 7c 2c 14 6c 8c 61 25 0b d8 38 9a e8 c2 74 61 30 11 42 4c 45 82 44 ab 8b 09 26 20 52 04 5d d8 e1 61 63 60 dc cc 6a 56 b3 9a b8 e8 e6 fa 9d ff 9e 3b 8f ce a3 43 99 5e ce 97 73 ee dc 73 ce 3d ff e3 fb cf 2b 83 3c 00 65 78 13 57 91 f7 de 1b 1f 9e 44 09 ea 51 b4 79 cb 0e 37 9a 07 06 f7 b9 d1 b5 7b e7 80 1b 1b 86 5e de e5 c6 8b 7b 87 58 bf 1d 30 0c a8 ef cc 67 9e 7e e6 eb 67 81 7e 16 ea 67 11 8a df 7d eb 83 93 68 90 b2 45 ca 2e 29 7b a5 dc 24 e5 00 87 93 31 33 96 6a d4 52 3e f3 a9 73 95 29 13 0b f4 f3 2e 9f 6d 4a 2a 5b f6 63 18 a7 f0 11 f3 29 9c 85 97 f8 1c 23 38 87 6f 70 19 3f e0 1a cb 11 f6 ae 82 13 8d 68 42 17 ba b1 1e bd e8 c3 06 f4 e3 34 26 e0 c7 3d dc c7 03 3c c4 63 14 e3 84 e1 c7 84 e1 83 9f f9 3e f3 03 e6 47 ac cb 83 d7 98 94 d2 2b a5 59 13 94 72 5c ca eb 2c 9d 46 80 fa 39 8d 51 be 8f ca bb 2a 0f 19 91 68 ad 57 6a bd c8 af f1 2a fd 97 ec ac f5 a0 87 ba 80 63 f5 c3 e6 f4 2c 64 8a dc 00 25 db 9b 3a 6c 96 a7 93 11 34 fc 46 c8 08 1b 21 5b 65 8e 1b 93 94 3a 6e ab cc 00 ad b4 df 4e e5 db 00 67 9d 0d d2 9e c9 5c b1 3f 6e 1d a6 9d 86 8f 91 1b 50 31 44 1f 47 b8 82 cd 61 e2 7a 68 a6 2a 13 5c 29 a1 75 08 32 92 a3 b0 45 87 b9 94 31 a2 7f 3c 4b 3b 2d 99 7e ce 1e c5 ae 95 23 dc d3 72 95 6a e2 62 28 64 4f 0c 99 89 ab c1 38 7d 19 d1 16 4d 19 53 c9 3d b4 ed 2a 8f 19 7f 25 f7 48 18 2d ac fa cf 28 55 c6 30 ed 93 6f 22 e6 57 aa c6 ca d3 75 48 3b 56 8a fe 09 ed 7a 55 57 56 ca 4e aa 59 9b 79 e5 9d 89 5f a5 Data Ascii: wOFFPMXGPOSlLINO$OS/28X`ecmapcvt (Nzfpgmxcgasphglyfp3*XgheadB66hheaB$YhmtxBx,locaDE|'wma xpGD  3nameGd<!FpostK` 2prepKtLfvxYKlTU-P(PJ-h|,la%8ta0BLED& R]ac`jV;C^ss=+<exWDQy7{^{X0g~g~g}hE.){$ 13jR>s).mJ*[c)#8op?hB4&=<c>G+Yr\,F9Q*hWj*c,d%:l4F![e:nNg\?nP1DGazh*\)u2E1<K;-~#rjb(dO8}MS=*%H-(U0o"W uH;VzUWVNYy_
May 27, 2022 14:31:08.062218904 CEST	1471	OUT	GET /files/theme/fonts/63a74598-733c-4d0c-bd91-b01bffcd6e69.ttf?1652461604 HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive Origin: http://document--1111011111.company.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Referer: http://document--1111011111.company.com/files/main_style.css?1652461604 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en; _snow_id.8a80=cdee608d-345c-4729-a8ec-f49d163ae349.1653687067.1.1653687067.1653687067.284b84f9-1721-4504-87d0-8d672f14f019; _snow_ses.8a80=*

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>May 27, 2022 14:31:08.236088037 CEST</td><td>1851</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 May 2022 12:31:08 GMT
Content-Type: font/ttf
Content-Length: 51501
Connection: keep-alive
Last-Modified: Wed, 11 Dec 2019 02:22:43 GMT
x-rgw-object-type: Normal
ETag: "53427fd099b7a52f111705d7c7558f14"
x-amz-request-id: tx000000000000000d17512-0061a7024d-a9f3e81-sfo1
X-Storage-Bucket: z56e2
X-Storage-Object: 56e2dd12548082d7acc7cc3762be313b6d43809588e973cf9338f513159904b5
X-Host: grn78.sf2p.intern.weebly.net
Accept-Ranges: bytes
Data Raw: 00 01 00 00 00 10 01 00 00 04 00 00 47 50 4f 53 00 a8 07 d1 00 00 01 0c 00 00 1e d4 4f 53 2f 32 66 5b 02 eb
00 00 1f e0 00 00 00 60 56 44 4d 58 6f 0e 76 94 00 00 20 40 00 00 05 e0 63 6d 61 70 90 e6 b0 e3 00 00 26 20 00 00 00
cc 63 76 74 20 07 cc 08 a4 00 00 26 ec 00 00 01 e4 66 70 67 6d a1 cc 85 0f 00 00 28 d0 00 00 09 50 67 61 73 70 ff ff 00
04 00 00 32 20 00 00 00 08 67 6c 79 66 5a 77 39 c4 00 00 32 28 00 00 76 3c 68 65 61 64 f3 b9 d4 b9 00 00 a8 64 00 00
00 36 68 68 65 61 07 81 07 b4 00 00 a8 9c 00 00 00 24 68 6d 74 78 de 7c 27 99 00 00 a8 c0 00 00 03 78 6c 6f 63 61 00 3
0 08 30 00 00 ac 38 00 00 03 7c 6d 61 78 70 02 6e 00 f1 00 00 af b4 00 00 00 20 6e 61 6d 65 3e 89 4d 67 00 00 af d4 00
00 17 07 70 6f 73 74 ff 9f 00 32 00 00 c6 dc 00 00 00 20 70 72 65 70 e3 0f 5b e5 00 00 c6 fc 00 00 02 2f 00 01 00 00 00 0
a 00 64 00 ae 00 01 6c 61 74 6e 00 08 00 22 00 05 41 46 4b 20 00 2a 44 45 55 20 00 32 4e 4c 44 20 00 3a 52 4f 4d 20
00 42 54 52 4b 20 00 4a 00 00 ff ff 00 01 00 00 00 00 ff ff 00 01 00 01 00 00 ff ff 00 01 00 02 00 00 ff ff 00 01 00 03 00 00
ff ff 00 01 00 04 00 00 ff ff 00 01 00 05 00 06 6b 65 72 6e 00 26 6b 65 72 6e 00 2c 6b 65 72 6e 00 32 6b 65 72 6e 00 38
6b 65 72 6e 00 3e 6b 65 72 6e 00 44 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00
01 00 00 00 00 00 01 00 00 00 01 00 04 00 09 00 00 00 02 00 0a 00 12 00 01 00 02 00 00 00 10 00 01 00 02 00 00 00 ea
00 01 00 34 00 04 00 00 00 15 00 62 00 7c 00 82 00 88 00 82 00 82 00 8e 00 94 00 94 00 9a 00 a0 00 aa 00 b0 00 b6 00
bc 00 c6 00 cc 00 d2 00 dc 00 cc 00 b6 00 01 00 15 00 0f 00 27 00 29 00 32 00 33 00 37 00 38 00 39 00 3a 00 3b 00 3c
00 4e 00 55 00 7d 00 cf 00 d0 00 d1 00 d2 00 d3 00 d4 00 db 00 06 00 6d ff d0 00 cf ff b8 00 d0 ff b8 00 d2 ff b8 00 d3 ff
b8 00 da ff d0 00 01 00 88 ff d6 00 01 00 88 ff 88 00 01 00 88 ff d0 00 01 00 88 ff e0 00 01 00 88 ff c4 00 01 00 c3 ff ee 00
02 00 88 ff be 00 c3 ff e8 00 01 00 c4 ff ee 00 01 00 a8 ff f4 00 01 00 0f ff dc 00 02 00 0f ff a6 00 88 ff a6 00 01 00 0f ff a6
00 01 00 59 ff f4 00 02 00 0f ff a6 00 88 ff 88 00 01 00 0f ff 88 00 02 18 88 00 04 00 00 19 4c 1b 24 00 36 00 3a 00 00 ff
e2 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: GPOSOS/2f[`VDMXov @cmap& cvt &fpgm(Pgasp2 glyfZw92(v<headd6hhea$hmtx|'xloca008|maxpn nam
e>Mgpost2 prep[/dlatn"AFK *DEU 2NLD :ROM BTRK Jkern&kern,kern2kern8kern>kernD4b|')23789:;<NU}mYL$6:<</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	54490	199.34.228.55	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.215816021 CEST	1086	OUT	GET /uploads/1/4/1/8/141840186/3pdp-orig-orig_orig.png HTTP/1.1 Host: document--1111011111.company.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: is_mobile=0; language=en

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:31:07.385917902 CEST	1180	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 12:31:07 GMT Content-Type: image/png Content-Length: 15272 Connection: keep-alive Last-Modified: Thu, 10 Feb 2022 08:37:12 GMT x-rgw-object-type: Normal ETag: "72afce6a160fc291147021b6aac153c1" x-amz-request-id: tx00000000000000029fff2f-0062853908-b9fbc20-sfo1 X-Storage-Bucket: z3e53 X-Storage-Object: 3e53901bb513d98511cdc10c3e14aa61e71d88728f1bfdc614c0caed4e10602c X-Host: grn67.sf2p.intern.weebly.net Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 a5 00 00 00 3e 08 06 00 00 00 d3 68 bd 5b 00 00 3b 6f 49 44 41 54 78 da ec dd 5b 6c 14 55 00 c6 71 5e f0 82 fa 66 e2 8b 09 46 01 25 6a e2 05 2f 54 28 2a 8f 3e 41 02 c1 48 8c 0f 90 80 80 42 34 a9 21 4d c0 87 86 06 62 28 ad 05 4a 4b 42 4a 8c bd f8 24 a0 d1 a5 5b a1 dc 0c c1 5e 82 35 05 5a da 52 48 ba 6d 22 ad bd c0 ee 9c f9 3c 67 ca a9 8d 68 45 9a 6e ab fd ff 92 2f 33 b3 b3 81 d9 79 98 ec d7 73 66 76 5a 18 4a 84 10 42 08 21 84 10 42 c8 18 72 d7 28 a5 84 10 42 08 21 84 10 42 26 ae 94 0a 00 00 00 00 80 31 a1 94 02 00 00 00 00 28 a5 00 00 00 00 00 50 4a 01 00 00 80 71 13 86 21 19 11 80 52 0a 00 00 00 a4 a9 8c 06 41 a0 54 2a a5 64 32 49 86 e2 ce 47 74 5e 8c 31 02 28 a5 00 00 00 c0 38 30 c6 50 ba ee ec 3c 31 7a 0a 4a 29 00 00 00 90 86 d1 52 f2 47 28 ec 98 8c a5 34 94 8c 91 82 e0 9f 63 6c 42 63 13 2a b4 4b 13 06 77 16 05 0a c5 5f 61 00 00 00 30 fe f7 8f 7a 9d 9d 9d 6a 6c 6c 54 6d 6d ad ea eb eb d5 d0 d0 e0 96 53 2e fe 73 d7 d5 d5 45 b9 7c f9 b2 06 07 07 75 0b f7 9b 62 92 8d 94 86 a3 e6 5f a3 87 4e 1d c6 18 a6 ca 00 00 80 09 fd 2e e2 f5 f7 f7 47 45 ac a2 a2 42 fb f6 ed 53 71 71 b1 4a 4a 4a a6 7c f6 ef df 1f 9d 8f 0 3 07 0e 28 16 8b a9 a3 a3 c3 97 51 4a 29 98 be 0b 00 00 00 8c 45 10 04 c3 e5 ea dc b9 73 2a 2a 2a d2 b6 6d db b4 6b d7 2e 5f c6 dc 6b 2e 6e 7d ca c4 7f 6e 5f ce dd 72 c7 8e 1d ca c9 c9 d1 e1 c3 87 95 48 24 74 0b 83 0b 98 c0 52 1a a4 a4 be 1e e9 7a b7 4d 97 d4 d3 fd d7 71 fb dc 7b fa 7a 15 24 07 34 98 ba ae df 92 09 f5 0d a7 4b 7d 37 6f 25 19 c5 ee ef 8c de 33 90 fa 55 29 73 53 00 00 00 c0 78 fd e4 8b 9f b2 5b 5a 5a aa dc dc 5c 1d 3a 74 28 9a be db da da aa 0b 17 2e a8 a9 a9 49 17 2f 5e 9c 92 71 9f df e5 ca 95 2b 3a 73 e6 8c 0a 0b 0b a3 c2 5e 53 53 13 dd 67 ea 8b 3d 90 be 52 1a 86 1a 96 b8 a6 f0 d8 d7 0a 2b 76 2b fc 32 5f aa dc 6b d7 6d ca f7 d8 e5 9e a1 ed 72 b7 ef 73 a9 cc ae 1f 3f a2 eb 1d 75 aa 4b 7c a3 58 fb 5e 55 b5 16 2a de b6 47 f1 f6 22 bb b4 db 36 f1 b6 a2 68 3b d6 ba 5b 47 6d ce 5e fb 4a 5d fd cd f2 42 85 cc ed 1d c3 85 d7 18 e3 e3 b6 27 f4 58 fc 05 ac a7 a7 47 5d 5d 5d 6e c9 05 0d 00 00 a4 8d 31 c6 7f f7 70 e5 2a 2a a1 79 79 79 ca cf cf 57 4b 4b 8b 70 bb de de de 68 94 74 fb f6 ed aa ac ac d4 c0 c0 c0 f0 f9 03 d2 53 4a 5d 91 30 81 86 35 fe a4 30 e7 7d 9 9 15 cf cb 2c 99 ab 70 c5 8b 76 7d 9e cc 32 bb bd fc 05 85 6f cf b3 cb e7 64 96 3e 2b 2d 7b 59 61 ee 46 b5 9f fd 42 a5 bf 7c a2 cd a7 33 95 7d fc 15 6d 39 91 a1 ad a7 17 69 cb c9 85 36 0b b4 f5 54 a6 3e 3d b5 48 9b 6b 32 94 5d f3 9a 8a 6b df 53 53 77 7c c4 21 18 4a e9 18 Data Ascii: PNGIHDR>h[;oIDATx[lUq^fF%j/T(*>AHB4!Mb(JKBJ$[^5ZRHm"<ghEn/3ysfvZJB!Br(B!B&1(PJq!RAT*d2IG t^1(80P<1zJ)RG(4clBc*Kw_a0zjllTmmS.sE\|ub_N.GEBSqqJJJ\|(QJ)Es***mk._k.n}n_rH$tRzMq{z$4K}7o%3U)sSx[ZZ\: t(.I/^q+:s^SSg=R+v+2_kmrs?uK|X^U*G"6h;[Gm^J]B'XG]]]n1p**yyyWKKphtSJ]050},pv}2od>+-{YaFB|3}m9i6T>=Hk2]kSSw|!J

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	57477	142.250.185.141	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 12:31:06 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515. 107 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+620
2022-05-27 12:31:06 UTC	0	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-05-27 12:31:06 UTC	0	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, 27 May 2022 12:31:06 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-UUYyBCvy5OkbMQpO1oVG3w' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-UUYyBCvy5OkbMQpO1oVG3w' '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 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 12:31:06 UTC	2	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-05-27 12:31:06 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

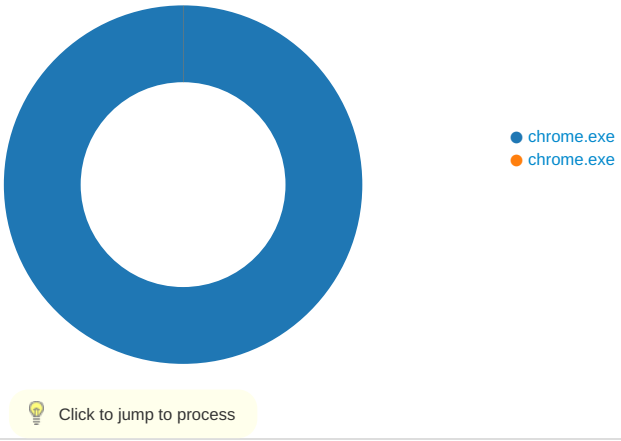
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	54599	142.251.37.100	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 12:31:07 UTC	2	OUT	GET /recaptcha/api.js?_=1653687066398 HTTP/1.1 Host: www.google.com Connection: keep-alive sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: http://document--1111011111.company.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 12:31:07 UTC	2	IN	HTTP/1.1 200 OK Expires: Fri, 27 May 2022 12:31:07 GMT Date: Fri, 27 May 2022 12:31:07 GMT Cache-Control: private, max-age=300 Content-Type: text/javascript; charset=UTF-8 Cross-Origin-Resource-Policy: cross-origin X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' 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"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-05-27 12:31:07 UTC	3	IN	Data Raw: 33 35 32 0d 0a 2f 2a 20 50 4c 45 41 53 45 20 44 4f 20 4e 4f 54 20 43 4f 50 59 20 41 4e 44 20 50 41 53 54 45 20 54 48 49 53 20 43 4f 44 45 2e 20 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 77 3d 77 69 6e 64 6f 77 2c 43 3d 27 5f 5f 67 72 65 63 61 70 74 63 68 61 5f 63 66 67 27 2c 63 66 67 3d 77 5b 43 5d 3d 77 5b 43 5d 7c 7c 7b 7d 2c 4e 3d 27 67 72 65 63 61 70 74 63 68 61 27 3b 76 61 72 20 67 72 3d 77 5b 4e 5d 3d 77 5b 4e 5d 7c 7c 7b 7d 3b 67 72 2e 72 65 61 64 79 3d 67 72 2e 72 65 61 64 79 7c 7c 66 75 6e 63 74 69 6f 6e 28 66 29 7b 28 63 66 67 5b 27 66 6e 73 27 5d 3d 63 66 67 5b 27 66 6e 73 27 5d 7c 7c 5b 5d 29 2e 70 75 73 68 28 66 29 3b 7d 3b 77 5b 27 5f 5f 72 65 63 61 70 74 63 68 61 5f 61 70 69 27 5d 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 Data Ascii: 352/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptch a_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);}; w['__recaptcha_api']='https://www.g
2022-05-27 12:31:07 UTC	3	IN	Data Raw: 61 72 20 65 3d 64 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 27 73 63 72 69 70 74 5b 6e 6f 6e 63 65 5d 27 29 2c 6e 3d 65 26 26 28 65 5b 27 6e 6f 6e 63 65 27 5d 7c 7c 65 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 27 6e 6f 6e 63 65 27 29 29 3b 69 66 28 6e 29 7b 70 6f 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 27 6e 6f 6e 63 65 27 2c 6e 29 3b 7d 76 61 72 20 73 3d 64 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 27 73 63 72 69 70 74 27 29 5b 30 5d 3b 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 70 6f 2c 20 73 29 3b 7d 29 28 29 3b 0d 0a Data Ascii: ar e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonc e',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();
2022-05-27 12:31:07 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **7668**, Parent PID: **4320**

General

Target ID:	1
Start time:	14:30:58
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument http://document--1111011111.company.com/
Imagebase:	0x7ff68c970000
File size:	2438312 bytes
MD5 hash:	74859601FB4BEEA84B40D874CCB56CAB
Has elevated privileges:	true
Has administrator privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: **7404**, Parent PID: **7668**

General

Target ID:	3
Start time:	14:31:01
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1740,10588110985535776619,16488514565616499681,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2108 /prefetch:8
Imagebase:	0x7ff68c970000
File size:	2438312 bytes
MD5 hash:	74859601FB4BEEA84B40D874CCB56CAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly