ID: 338140
Cookbook: browseurl.jbs
Time: 17:52:02
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

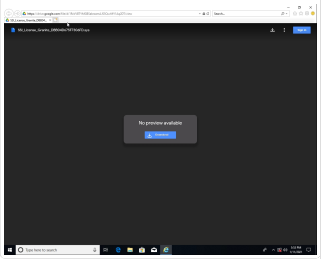
Analysis Report https://drive.google.com/file/d/1RxVVB…

Overview

General Information

Sample URL:	http://https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp=drive_web
Analysis ID:	338140

Most interesting Screenshot:



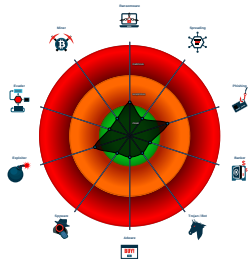
Detection

Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Allocates a big amount of memory (p…
- Found iframes
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6968 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7020 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6968 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

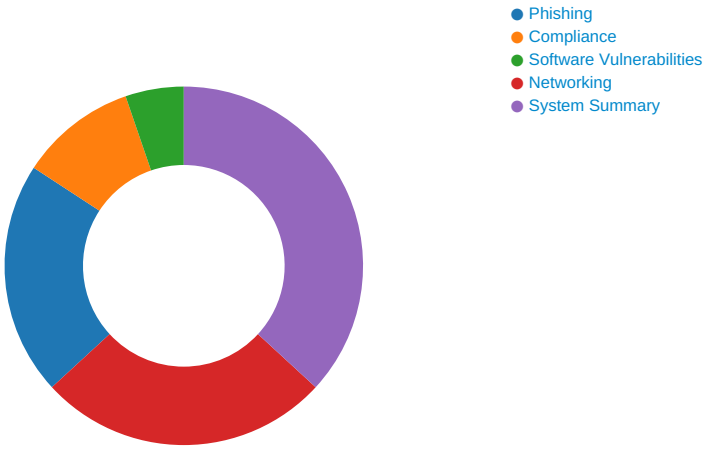
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



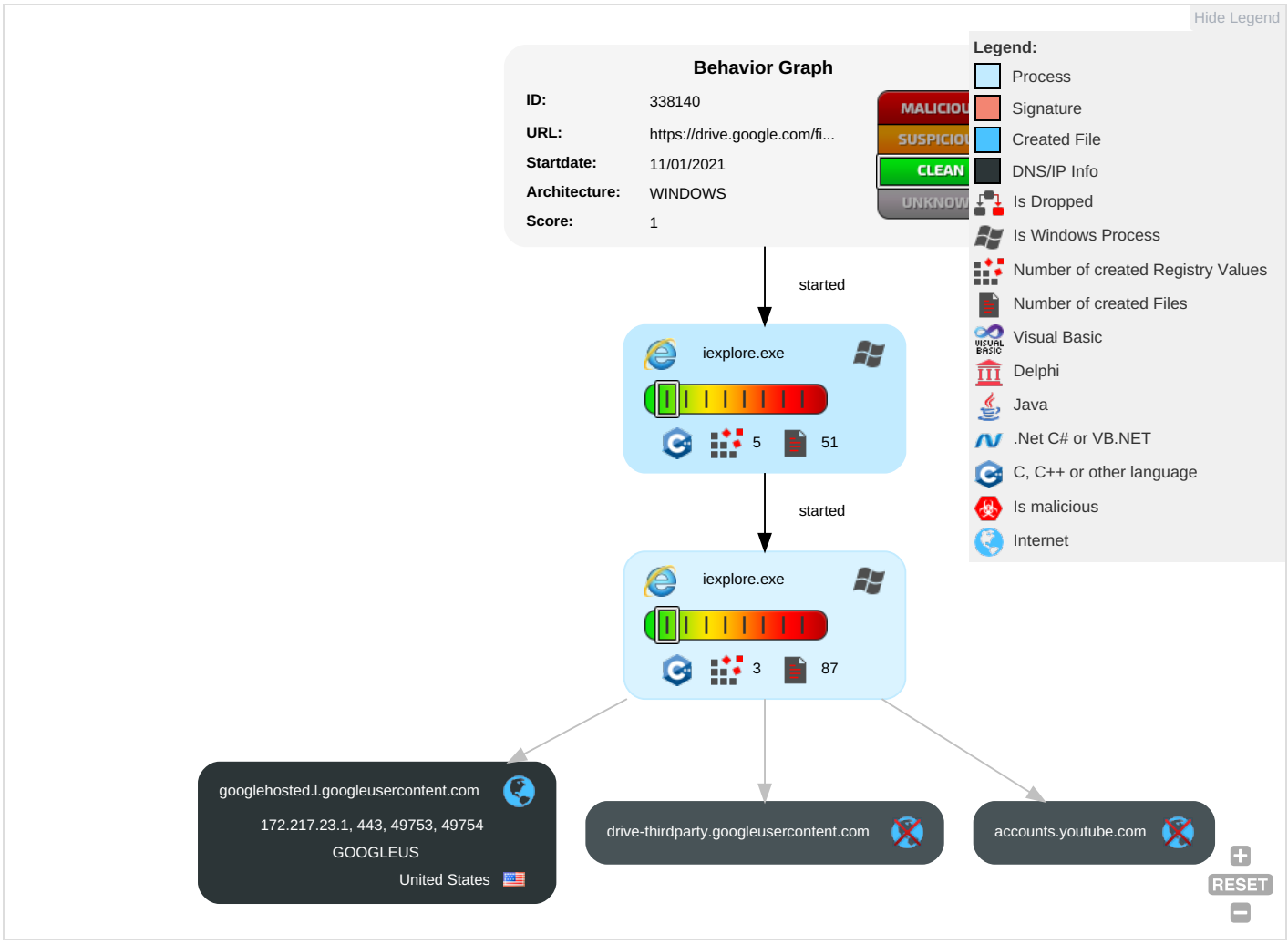
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

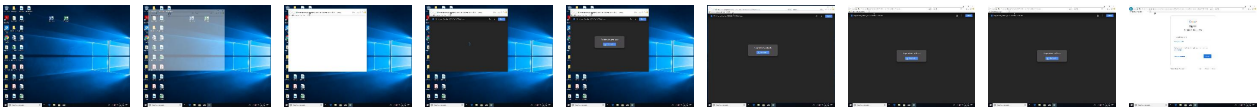
Behavior Graph

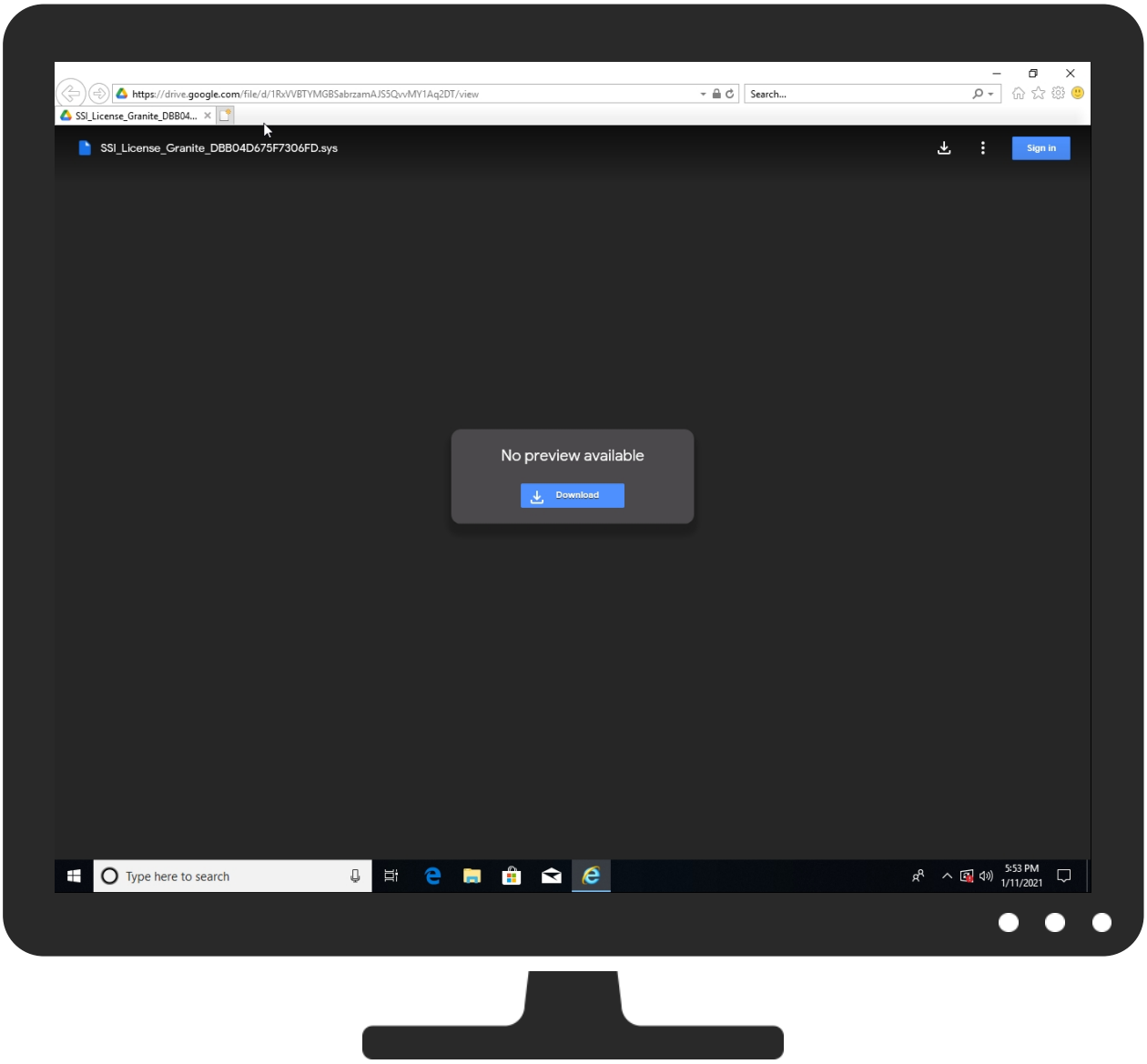


Screenshots

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://https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp=drive_web	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.broofa.com	0%	URL Reputation	safe	
http://www.broofa.com	0%	URL Reputation	safe	
http://www.broofa.com	0%	URL Reputation	safe	
http://https://accounts.googl	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://accounts.googl	0%	URL Reputation	safe	
http://https://accounts.googl	0%	URL Reputation	safe	
http://https://accounts.googlom/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/viewsp=drive_webe.com/ServiceLogin	0%	Avira URL Cloud	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products	0%	Avira URL Cloud	safe	
http://www.bohemiancoding.com/sketch/ns	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch/ns	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch/ns	0%	URL Reputation	safe	

Domains and IPs

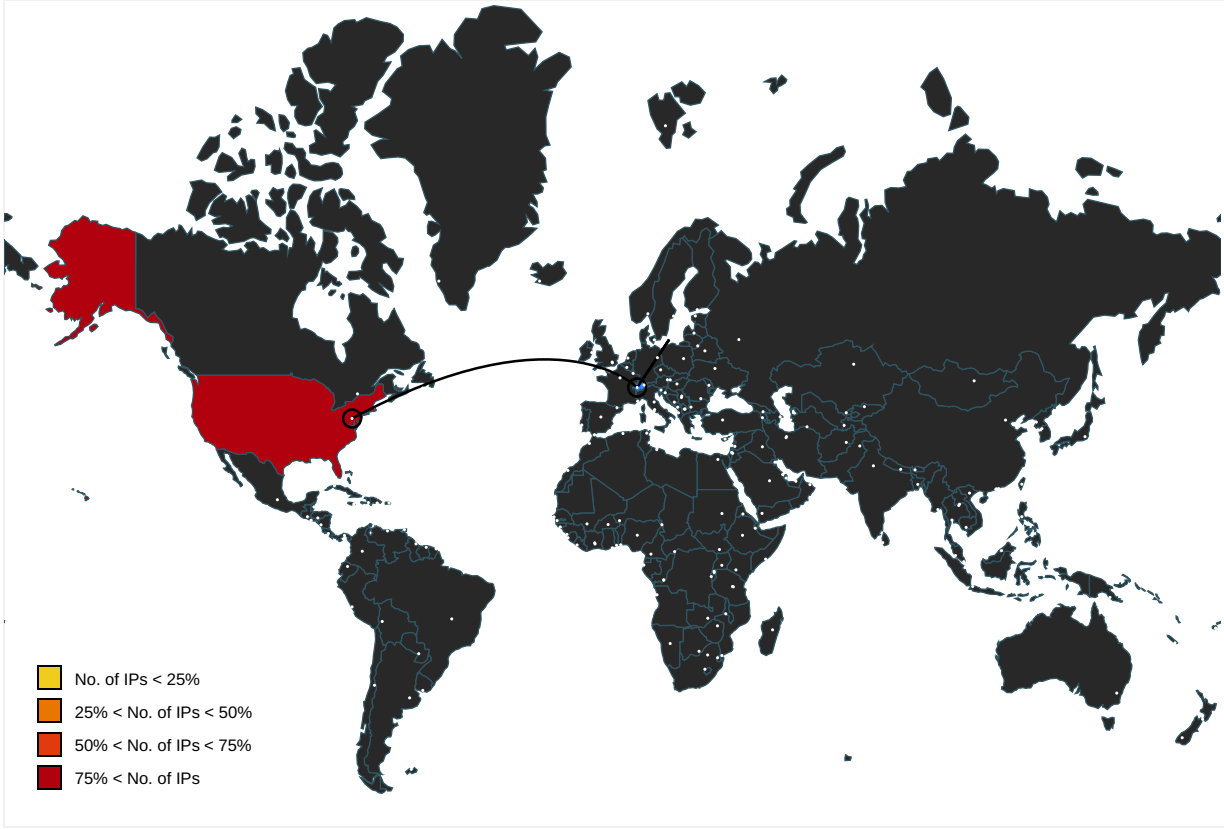
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
accounts.youtube.com	unknown	unknown	false		high
drive-thirdparty.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	m=v[1].js.2.dr, m=_b,_tp[1].js.2.dr	false		high
http://www.broofa.com	m=v[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://accounts.googl	{705C3408-542D-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://accounts.googlom/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/viewsp=drive_webe.com/ServiceLogin	{705C3408-542D-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.bohemiancoding.com/sketch	v-sprite33[1].svg.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://developers.googleblog.com/2018/03/discontinuing-support-for-json-rpc-and.html	cb=gapi[1].js.2.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/	m=v[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/a/default-user	2295042476-docos_binary_i18n__en_gb[1].js.2.dr	false		high
http://https://www.google.co.uk/intl/en-GB/about/products	view[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.bohemiancoding.com/sketch/ns	v-sprite33[1].svg.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://g.co/recover	ServiceLogin[1].htm.2.dr	false		high
http://https://accounts.youtube.com/accounts/CheckConnection?pmpo	ServiceLogin[1].htm.2.dr	false		high
http://creativecommons.org/ns#	v-sprite33[1].svg.2.dr	false		high
http://https://www.youtube.com	m=v[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.1	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338140
Start date:	11.01.2021
Start time:	17:52:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp=drive_web
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/54@2/1

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://accounts.google.com/ServiceLogin?service=wise&passive=1209600&continue=https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp%3Ddrive_web&followup=https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp%3Ddrive_web&ec=GAZAGQ
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 88.221.62.148, 172.217.23.14, 172.217.20.227, 172.217.20.234, 172.217.23.67, 216.58.207.142, 172.217.20.238, 172.217.23.35, 104.42.151.234, 172.217.22.234, 172.217.23.42, 216.58.207.164, 172.217.22.205, 172.217.22.206, 172.217.22.238, 52.255.188.83, 51.104.144.132, 92.122.213.194, 92.122.213.247, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, blobcomments-pa.clients6.google.com, docs.google.com, ssl.gstatic.com, arc.msn.com.nsatc.net, ogs.google.com, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, drive.google.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, fonts.googleapis.com, plus.l.google.com, accounts.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcoleus17.cloudapp.net, www3.l.google.com, play.google.com, content.googleapis.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, apis.google.com, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: https://drive.google.com/file/d/1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT/view?usp=drive_web

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\accounts.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.4435199657021
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1ryRtFwsoIcDAqFf3ssGR8qSRlwKb:JFK1rFK1rUFxmAq93ssGi6Zb
MD5:	FB76C79F7C5E2C93430AFD793DFFEB45
SHA1:	66425EA2712882A32A6B7DE6C6D6A8DFA813D14D
SHA-256:	C96D1BFD93EF702966117E9879412CD9BBBFFC34904CF0F88B2128D68F498EA8
SHA-512:	04886CD98D2D9598F066E9A2D8B6589B6060ECC6FA0126AF22E87AAC1610F5C44287BA074F8FA18E8CEDFA011E804CE7F437F34A3397038F06320A8DBBD87C9
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="promo" value="{}" ltime="1098234480" htime="30861370" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{705C3406-542D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.85164873982753
Encrypted:	false
SSDEEP:	192:rgZxZ22y9WQtYifeVrzMSjBcJD4sfRVSjX:rQXNyU0FPOI3G
MD5:	9542730A3A3A16CA8DBEDC0DF5F293D2
SHA1:	DFD22E79A327EED4BBBE8E8B49BC7628FC8BA011
SHA-256:	F02259A6519F2C57B90C231B7876DE575A129576F8CCB018E5B6EEE951306DAD
SHA-512:	6CDD9B4F22CC63CA231C786FC0C8FCC326E20827AD2006C2E9E83630ED51061A393F6F9ED198C790EF16A1808AAEE469C2A07BAAAB43EB98E8272DE1A92CE D0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{705C3408-542D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	48436
Entropy (8bit):	2.4628549311257553
Encrypted:	false
SSDEEP:	384:rfv9NKhAgR7maAkMFEjEXJtfLfdfFfQfGfH9GZHxc8shHxqshHxqMLSjrv:SO7dlWM8
MD5:	0667DDADFA6170CEEA28DC4BD84D008E
SHA1:	0708C9B39405182B6E04C5F7B6441AFB3CF95E4A
SHA-256:	83D5EFC02D3B6EE3A9D368A6EE1082707BF65E72241B1C6461AE4FA364C3EDBA
SHA-512:	877702950BE65D38051E529B619E52CF2E512D924AB62B94A49B4D3CCA9204E634A89436BBE530E0C33D8AAB4DD01A6BECCC6169D6D99F11A5ACA155862A45 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{705C3408-542D-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7742C457-542D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565649228365321
Encrypted:	false
SSDEEP:	48:Iw6GcprXGwpa5G4pQNGrapbSlrGQpK/G7HpRKsTGIpG:r+ZBQb6tBSlFAOTK4A
MD5:	FF28B3A19A7FE6E9C45D11601CB60600
SHA1:	ADA178249FE03FE32AB443F394B75D58CEFC8A6A
SHA-256:	4AF68E89CA48EF779C51F86FEA4D31BD4637602A88FE7F727E50C77D501274D1
SHA-512:	413BD134F765E059ED5643EEC9571415C342AA4191EAFDAC22118548AE5D1A0187C7B2E972E71F12BF2A40FB5B6E9C8F00B3940C207CAB594E9C8AF10D4438EA
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	4.569088558171749
Encrypted:	false
SSDEEP:	96:G4mwP4L6ZaiRvIJct+UP47v+rcqlBPG9O:204LKaiRvI6tFPqWceBPGs
MD5:	A0889ADBF73438EC56AFB7CAC3594290
SHA1:	3FCA0CFC164FA0330C02B64B3032562C40D3FBC2
SHA-256:	BF96DF9B4CC2DA671EA31170BB57E6AD602B92C7831BC891A053DCF85EA0C1BC
SHA-512:	9BE5EFAB06FAEF910CFCF182311181B583AE54BCEF603CE27A6B9976C724D5C4F5BABF69BE3F23B4CEC183BF1266C81DBE10D1472F0EF7C7EAA1725F1CB1A0AC
Malicious:	false
Reputation:	low
Preview:	H.h.t.t.p.s.:././.s.s.l...g.s.t.a.t.i.c...c.o.m./.i.m.a.g.e.s./.b.r.a.n.d.i.n.g./.p.r.o.d.u.c.t./.1.x./.d.r.i.v.e._.2.0.2.0.q.4._.3.2.d.p...p.n.g.?....PNG.....IHDR... ... .szz.....IDATx.b .....+.....m..dW.@..tm.Y.....m.....m.m..L.|.....{..b...t.....=H..qt..V..X..<jQc...p...fdU.\2.....9T...Jz!9...L.)&.....n....`~.T.\.\.$.....qQ.....LFOx.....^&,"bB..Lh9$_.6<...A...Q.T&y.,'...p...W`.2.?X(.o.4.J?.2...@.4...*..X..c.....[UZJ...MN.].z..f..DFe.J.....!r...0X.....).....^*..!....u..c..R4.GH....Y....E....Q.....+!..)...e".....,.Ge.r.T..!..r..(.|.9f...}.....(...s..N...[..~.%6QF..g..r.....CN.e"(..uY.h._1.H.e....r.k..%^S.c..<..0.s.j..,D.....]..y.2(..OC.o\.3..".....cw...:.btq.....w=.....R-[].4..]...?.....o..K../cC.<O...y..O.....{.-'Ln9..M.*6t.(.....o.K.$....bz.X._d.....Z].U.....t....Bf.Zl.^vA._..g.{l....V...{....=.jua..[...k.....j....Y\...!..+.m..X..t(.....".Mz.26l....7X.C...-...Z.lvl.....y}x.....7.m.VV....IEND.B`. ... .i..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2801455510-postmessagerelay[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9879
Entropy (8bit):	5.579296703325767
Encrypted:	false
SSDEEP:	192:1TyJwMuoQ7zM1ueeFWLCivp3YiIJ1MfWXxPKPo5ulhIEkvwt:1TowMuoQ7zM1yC3ZIJvBiPKWaot
MD5:	F2BD1D2E00DEDBD451AA5003CEDF69CC
SHA1:	1A368F9C023F244F6DE111C8E213F47ACEC891E5
SHA-256:	0B38E24497A006357613322357AF9D5D3CD270F8498A1E78D773620F0910C6E6
SHA-512:	0E076191531E579AF4BD941F5B09579D05097456ACC9294FD29AF730345D262503F9685A9DA6D19874F120DC3E3A72E34D43FB305D287C9F90CAF1534CFFE5ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/accounts/o/2801455510-postmessagerelay.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2801455510-postmessagerelay[1].js	
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var m=this||self,w=function(a,b){a=a.split(".");var c=m;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var e;a.length&&(e=a.shift());)a.length||void 0===b?c=c[e]&&c[e]!==Object.prototype[e]?c[e]:c[e]={}:c[e]=b},x=function(a,b){function c(){}c.prototype=b.prototype;a.A=b.prototype;a.prototype=new c;a.prototype.constructor=a;a.v=function(e,d,h){for(var l=Array(arguments.length-2),n=2;n<arguments.length;n++)l[n-2]=arguments[n];return b.prototype[d].apply(e,l)}};function y(a){if(Error.captureStackTrace)Error.captureStackTrace(this,y);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a))}x(y,Error);y.prototype.name="CustomError";var z=function(a,b){a=a.split("%s");for(var c="",e=a.length-1,d=0;d<e;d++)c+=a[d]+(d<b.length?b[d]:"%s");y.call(this,c+a[e])};x(z,y);z.prototype.name="AssertionError";var B=function(a,b,c){if(!a){var e="Assertion failed";if(b){e+=": "+b;var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\4UabrENHsxJlGDuGo1OIlLV154tzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26216, version 1.1
Category:	downloaded
Size (bytes):	26216
Entropy (8bit):	7.981777815901356
Encrypted:	false
SSDEEP:	384:Sg4TzCs2RY3zVuzsjaV8NN/gL7JWwOCYagoTqUE+KTiXxzOH50RrzhRgAkua:v4SNRYZuz6A8N1gL7JRgoT2+KIxOaJ0
MD5:	D6CC7164BC67A74418DDC5334DB07720
SHA1:	7B92694ACF8EE4F16A745892F5475CC3D6AC9E97
SHA-256:	37F9CFD34965C916FDB5F549F2EE8FC56C20A0AAD2C281B799595396105C4316
SHA-512:	B95636C8A21EE26370D70E81B8D7478BB3F15A905480CDAA2EBBC85C2376E402A3983BD843AE764BFACA64680B04816BEEB2C2351A4037EFB0E42A0FDA9A5A60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLV154tzCwA.woff
Preview:	wOFF.....fh.....GDEF.....q.....GPOS.....#..+..G.PGSUB.....OS/2.....U...`j(..cmap.....~n..cvt .....(...fpgm...x.....uo..gasp...@.....glyf...L..=...k..N.dhead..Z`...6...6.x'.hhea..Z.... ...$....hmtx..Z.....&.loca..]H...~....:...maxp..._.... ... .name..._.....Z.L3.post..`.....O...prep..dX.....t...x.E.....E.}&$.....A.. ...,....`..}....q....+o...9 ....B.J..WS..w2.{...o.D~!X.D:..Muq...[1 ..[.I...]..#...2...x..Z..$..}....e...333333333.aA..2.8....N.l..h...W....s;.u@.....j`.....t.mwE.!g.\|,..q.a.`.c.:.x.....J;V:.....N>.].O.....\|..@..r..`..(`s.J.sq3..#(.x.....w.n....Y.....j.&c.f.....,Y.....?....x?...~.....s..)#s.bn..v.....J.j.:..`.,.:.V8....V....K..=aE..w3e...z..A\|..2.K.BX.+.....#z.Q>.R.(...$..x..Z.F.....<^._.7..7.....p!....dT.....I.BxxSk...|H$.6pM..<8.q'A....!..A..$.Ex.+.^\....q..0..h"..C.....G...a..#*...#|.|W....k..K....Y....._v..N..5.Ju..f.XR..)....T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\CheckConnection[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	modified
Size (bytes):	31710
Entropy (8bit):	5.441897200069707
Encrypted:	false
SSDEEP:	384:pzjSqwWVuEwpMxYHbeS+G7hW2+nJptuV5zFL78aUFW3Mk2ES2aBSgyx0Kin:pHWnpYYHbeVnHJptuJ78L4mSgy+n
MD5:	6AEE57203937DBA53836657E9F03C51E
SHA1:	1F47B3E7B21A98C3662373670BA3DA3FE77BE9C9
SHA-256:	C3BA55D5E7DDD7A957E397D208BE370ACC430A618A3C7B1968179A5D2D76D88E
SHA-512:	EA94C16595D6F9D010D3E6EDF077EF304551C613395587880798F51C4DEFCFDC4E2CE831C849F72CCA07B7DBE544DD5AA2E601900E84774EB656B6CC554B33A
Malicious:	false
Reputation:	low
Preview:	<html><head><script nonce="3FizLk0dLusrlTB3meOaWA">"use strict";this.default_AccountsDomaincookiesCheckconnectionJs=this.default_AccountsDomaincookiesCheckconnectionJs||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var k=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,k);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a))},aa=function(a,b){a:{for(var c=a.length,d="string"===typeof a?a.split(""):a,e=0;e<c;e++)if(e in d&&b.call(void 0,d[e],e,a)){b=e;break a}b=-1}return 0>b?null:"string"===typeof a?a.charAt(b):a[b]},ca=function(a,b){b=ba(a,b);var c;(c=0<=b)&&Array.prototype.splice.call(a,b,1);return c},da=function(a){l(a)},ha=function(){var a={};a.location=document.location.toString();.if(ea())try{a["top.location"]=top.location.toString()}catch(c){a["top.location"]="[external]"}else a["top.location"]="[external]";for(var b in fa)try{a[b]=fa[b].call()}catch(c){a[b]="[error] "+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\callout[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31277
Entropy (8bit):	5.7552359251505365
Encrypted:	false
SSDEEP:	768:e7b7/d9SvRuKxv/S60ZwDqIrBycUknoVkZq7stfnsuiCPO8CPmzUlgDL6QPFJ/Nr:Eu0ZwDXnoJKk2UgJ1SKea
MD5:	D437FACBB1295E6B31DAFBE1A0FF72D0
SHA1:	4B48FCABD7A58EF963295D502087174BB82B2F70
SHA-256:	44309CCCC03696AC32B3D9D9A9C8C26423F19D5A5EFFAE79A57327D37BEB0AA8
SHA-512:	6DC80C783E34E48984C66E1878EF48A1CD200A241BDC1054F0EAE86E1F7674E6B00B0C6FEF31A70973A70B097E3C004E7755D88E62A95B1E01B935938387C5F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/callout?prid=19016401&pgid=19010599&puid=46b57e6661f85f&cce=1&origin=https%3A%2F%2Fdrive.google.com&cn=callout&pid=25&spid=25&hl=en-GB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\callout[1].htm	
Preview:	<!doctype html><html lang="en" dir="ltr"><head><base href="https://ogs.google.com/"><meta name="referrer" content="origin"><link rel="canonical" href="https://ogs.google.com/widget/callout"><link rel="preconnect" href="https://www.gstatic.com"><link rel="preconnect" href="https://ssl.gstatic.com"><link rel="preconnect" href="https://apis.google.com"><link rel="prefetch" href="https://apis.google.com/js/api.js"><script data-id="_gd" nonce="SMRLRi55YzZqFxuyMIebzw">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"1698387055069193713","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1610383976184326,151685786,2634245766]\n","ZwjLXe":25,"cfb2h":"boq_onegooglehttpserver_20210105.03_p0","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333,45695529],"gGcLoe":false,"ikfjnc":["https://drive.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"OneGoo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	100373
Entropy (8bit):	5.527492554700324
Encrypted:	false
SSDEEP:	1536:pWf2UtyeudISqZV9McRuq5tKNDW9U5JSt8coYpCNUceDLN0944aYDaQF9PEzUsHB:p2tyeudIzbUa8cotNUcILYafQ0HxM4
MD5:	C0E9524A212DBFFE60A027A8775DE68E
SHA1:	DDE359D93BFBA539BFA183D15857CEB0AFAD3A8D
SHA-256:	21F3ECA68A88A3C174C1DA1011A2694D4767EE5DFA69D59563C211D64A5C533F
SHA-512:	3261DA6931EFDE03645584CCAD502CDCBC086C5E779474623551C965CCC3B891AA7C3A90BD8341A603CCD2596BDD37C6FF68422B019D63C7F253EFF1165AF6C
Malicious:	false
Reputation:	low
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,ra,za,Ca,Ea,Ja,Ta;_.da=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ra=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};za=ra(this);Ca=function(a,b){if(b)a:{var c=za;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ka(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	51253
Entropy (8bit):	5.5573013771777795
Encrypted:	false
SSDEEP:	1536:pWf2UtyeudISqZV9McRuq5tKNDWDE7UcjF9PEzUsj:p2tyeudIzZE7Ucj0j
MD5:	04EE38D70EF26E91A9B235B100609960
SHA1:	36BD118C3AED296F11415C7AE3C6499D30D419C5
SHA-256:	139F92250A2E3B7BCDEA5610ED309F4D25D79F8787BA3A9BB21DBD83648AD028
SHA-512:	91799A8750DB92A7D67F2F19702653F5627A801B35BB7D54418842320A14F105C36D5DD9902A90DA5D2AF73B71331B1B5297559C32BF755051E726AB829F2C85
Malicious:	false
Reputation:	low
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,ra,za,Ca,Ea,Ja,Ta;_.da=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ra=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};za=ra(this);Ca=function(a,b){if(b)a:{var c=za;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ka(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	646
Entropy (8bit):	5.179300405984408
Encrypted:	false
SSDEEP:	12:UJO6940FF5O6ZRoT6pWqoSEqFF5O6ZX6pWJ6qFF5O6ZN76pW5Y:G9X3OYsRqPv3OYXRD3OYN7Ra
MD5:	26AF74654DD745D30F539E1169FC30BA
SHA1:	5FD629CBC75C6E99A37727F8AA719506BBBDA11A
SHA-256:	69C710F842A04AD1AF6D63A1F73969E13803AC2238B4CC9AE431868E0C4FF44E
SHA-512:	15A61D765F6A783E49E6F1FBD862ADBB2FE6D51E869F33129F79341026BA6ED478238D8998F44EBB1EFEF5D9703D32AA910B3C28E719782FB47E81560138B815
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLV154tzCwA.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gm_add_grey600_36dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 36 x 36, 2-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	133
Entropy (8bit):	5.222391927901063
Encrypted:	false
SSDEEP:	3:yionv//thPl8lUzNgZ7QwbdSSvgXRRPiifewwXjp:6v/lhPqNNQIdSBBoxp
MD5:	9E4B3B711000FF89777C47458243FDB7
SHA1:	C38AE0080C66C8451AC535F7E38F358BA288D766
SHA-256:	BB09F466C21A6C52CBDD1180C6E0D592E9A141B3FE6230596E3105B5A43B429C
SHA-512:	D0EE79D6BCB3C242A3EB0008FE91E0BA5D7279A480AABEB4398D9C5F2DA74078DDFCAA086882E24DEC1A85747C59C503406A773503F57393BC879648FFB6E52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/i/googlematerialicons/add/v6/grey600-36dp/1x/gm_add_grey600_36dp.png
Preview:	.PNG.....IHDR...$...$.....np.....PLTE...tttuuuuuu.....tRNS....$.....$IDATx.c..d.....:44...Z....,.,..B!.....U..xJ....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=NpD4ec,SF3gsd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,oWOIDb,n73qwf,MpJwZc,bIf8i,omf1Od,zbML3c,zy0vNb,K0PMbc,otPmVb,rlNAl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2752
Entropy (8bit):	5.3175035426861434
Encrypted:	false
SSDEEP:	48:x76E0E5ElEtEEEfEWEzEeE9EDoEuE3LEfErE+FD7B8oSBUeH2dEUAAkzktkGl:xDFD7aNb0AAcktkG
MD5:	77BA26ACC6C3678D93CDE0BF843F1CD7
SHA1:	1E9EB478BFFD9CD7940E89E47F6AEC0FE6371D85
SHA-256:	F572B9318BD28E4C35740CA440901895ADB37D03E862C4EE553DC8407EFF2807
SHA-512:	BEF49ABEEE4515D1E5A17750270418C439FED4065295B789827371E9149735FE41C0DFC1B2F2AE865668A12DEE806CEC1368B035BC3F52B266AA24BFBA372E95
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("NpD4ec");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("SF3gsd");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("YLQSd");._.zu(_.ty);.._.l();..}catch(e){_._DumpException(e)}.try{._.k("lCVo3d");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("o02Jie");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("rHjpXd");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("pB6Zqd");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("QLpTOd");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("oWOlDb");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("n73qwf");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("MpJwZc");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("bIf8i");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("omf1Od");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("zbML3c");.....,_.l();..}catch(e){_._DumpException(e)}.try{._.k("zy0vNb");.._.l();..}catch(e){_._DumpException(e)}.try{._.k("K0PMbc");.._.l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\octet-stream[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	164
Entropy (8bit):	6.125350632626513
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lqk32D3j22CHtEU10TmHLE2a3bB74Gx868lPs3v/lsg1p:6v/lhPakqUHtOTmHY386bveup
MD5:	4FF1D3A32EF4FB230E32609C2D54B592
SHA1:	E940F717FAE3DCD312D72A275B1F5379C31728B0
SHA-256:	628519B3986983140E9CCCFCB35FAE7395B57BE4CD8CB4E786A1561FA05F557C
SHA-512:	1C08F1030C0B87A532E0555CA875831CAC824FE8646C1BDE80278AE598C106DA0D224E1D117774941D92A8B0D21B2B14AECFBF55F950C8B3B603C91D490189B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drive-thirdparty.googleusercontent.com/16/type/application/octet-stream
Preview:	.PNG.....IHDR.....a...kIDATx.c.....R./...E/....|....B.....3.....C.1.....D.P.....k...../.c.@..a.....<o ...%.....j...L.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AO0039tymOY0r_jJiutTtjdfJABMq2LBUw[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AO0039tymOY0r_jJiutTtjdfJABMq2LBUw[1].css	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	591266
Entropy (8bit):	5.684311815795506
Encrypted:	false
SSDEEP:	6144:FvZFfP9oN8/LXxDzB9RRGCOiOWLp0uix3HkGY4t4vzvgUPSzD+rgTspsE4tKWodA:FvZFfP9oNOZggEygJ/tvaps
MD5:	FDFE130238EA53B11290CCED59E9E005
SHA1:	10599E61923F78A458F8F64127A9F3601A153CAE
SHA-256:	253574212D9E1271EAE4896DF96FCAD49EC14DC25585884D387FD83B2F72B32F
SHA-512:	0DD9BD2783447EE96605C844B52D97CFE47A2169A32F4EFE1E8D3D4788E3711ED5F8B0664E3D3E264276F8AC9F73346EC905E60EE66E6D48A90AE76F8D62FE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/apps-fileview/_/ss/k=apps-fileview.v.BeAX3cDGtBo.L.I11.O/d=0/ct=zgms/rs=AO0039tymOY0r_jJiutTtjdfJABMq2LBUw
Preview:	.tk3N6e-LgbsSe{font-family:arial,sans-serif}.VIpgJd-INgbqf-LgbsSe,.VIpgJd-INgbqf-xl07Ob-LgbsSe{font-weight:700;font-size:11px;font-size:var(--docs-material-font-size-12,11px)}.HB1eCd-UMrnmb #docs-editor,.HB1eCd-UMrnmb #docs-editor-container{background:#f8f9fa}.VIpgJd-AznF2e{font-family:arial,sans-serif;font-weight:700}.VIpgJd-Kb3HCc-xl07Ob-LgbsSe-cHYyed{font-weight:700;font-weight:var(--docs-material-font-weight-normal,700)}.XKSfm-Sx9Kwc-c6xFrd{font-family:arial,sans-serif}.tk3N6e-F79BRe .VIpgJd-VgwJlc-PBWx0c,.tk3N6e-eLJrl,.tk3N6e-rugWtd-xGWjg,.tk3N6e-rugWtd-xGWjg:hover{font-weight:700}.IyROMc-t6O8cf-r4nke-haAclf,.IyROMc-w3KqTd-r4nke-haAclf{font-family:Roboto,RobotoDraft,Helvetica,Arial,sans-serif;font-family:var(--docs-material-header-font-family,Roboto,RobotoDraft,Helvetica,Arial,sans-serif)}.HB1eCd-UMrnmb .HB1eCd-E90Ek-haAclf{font-family:Roboto,RobotoDraft,Helvetica,Arial,sans-serif}.HB1eCd-UMrnmb .HB1eCd-tCYPLb-LkdAo,.HB1eCd-UMrnmb .HB1eCd-tCYPLb-DbqQVb,.HB1eCd-UMrnmb .HB1eCd-jEqmy

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\view[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	73664
Entropy (8bit):	5.615270495262711
Encrypted:	false
SSDEEP:	768:+nBcV9d8PccFqnFRQQARCexAbT09FlvWBLFguC/rYNBEB3RHFQSYoSK3lQWde8J9:p8QRDsmT01WaeaUDvDNUYe4nWW9MpmA
MD5:	241DF8329AADD61B4F012B19ECED7F09
SHA1:	28C6BB7BCA880C1175558FDD6DEDD3EDBDCE380B
SHA-256:	3BB9BBDB2481658A7DC5E9799FF7A362624CEE1A23C2C489DCC56379A40237AC
SHA-512:	3F77ACD7D9FB52A87FB6A8AD151F8297667A1F583C32763FE055B4E48681D138FAB648456290BA19E752CB33A6B0A53D5EAD2BE00CB38EE0A631A2E8B3E37DE2
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html><head><meta name="google" content="notranslate"><meta http-equiv="X-UA-Compatible" content="IE=edge;"><style>@font-face{font-family:'Roboto';font-style:italic;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xIIzQ.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:300;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fBBc-.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:700;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc-.woff)format('woff');}</style><meta name="referrer" content="origin"><title>SSI_License_Granite_DBB04D675F7306FD.sys - Google Drive</title><meta property="og:title" content="SSI_License_Granite_DBB04D675F7306FD.sys"><meta property="og:type" content="article"><meta property="og:site_na

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\CTRY69B1.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	219056
Entropy (8bit):	5.519291124653364
Encrypted:	false
SSDEEP:	3072:/3pNn0kfT8JSfhZQ7fFNmu0CB5vw53nKJ9:Pp5r4GZQxN5JB5vw56f
MD5:	0ED081D197F05B334F842B1583F27740
SHA1:	DF8049E03F62F344B99216179C50B30EC412B24B
SHA-256:	C9014A141CC32D43F477AB4EB9657459E082EAD4017B700EBC76776A27D2477B
SHA-512:	A2B3893976CEF91590EFDED3FDC06A3F48122F91B060CE964BC719F51857864E8E594B892E207966CF167CC69DBBF822F30495B60941CC42D1ADA6911F6712C2
Malicious:	false
Reputation:	low
Preview:	"use strict";_F_installCss(".KL4X6e{background:#eeeeee;bottom:0;left:0;opacity:0;position:absolute;right:0;top:0}.TuA45b{opacity:.8}sentinel{}");.this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{._.xB=function(a,b){return a==b?!0:a&&b?a.width==b.width&&a.height==b.height:!1};_.r("sy2f");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var zB;_.yB=function(a){_.yi.call(this);this.g=a||window;this.i=_.mi(this.g,"resize",this.s,!1,this);this.j=_.ff(this.g)};_.H(_.yB,_.yi);_.AB=function(a){a=a||window;var b=_.va(a);return zB[b]=zB[b]||new _.yB(a)};zB={};_.yB.prototype.Qa=function(){_.yB.Gb.Qa.call(this);this.i&&(_.ui(this.i),this.i=null);this.j=this.g=null};_.yB.prototype.s=function(){var a=_.ff(this.g);_.xB(a,this.j)||(this.j=a,this.dispatchEvent("resize"))};._._.u();._._.r("n73qwf");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var BB=function(a){_.yi.call(this);thi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Chrome_Owned_96x96[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Chrome_Owned_96x96[1].png	
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6177
Entropy (8bit):	7.941892268309048
Encrypted:	false
SSDEEP:	96:iYr3dN0F+QXKWXPTdNVeVTGTe+24Usw2i2DDF2ryznZE4OYF3ETHKI2HAr9UXPDf:iY8FXrf5N2TuB2Rvc2ryzZhtG7drgb
MD5:	C101133ECB2D66F0EA98131267D2A10A
SHA1:	8C038B9B39FA23E0AD2226F0016BF51FA0B86E37
SHA-256:	E3654539251DF82D59096E81C875D1244FFB7AB92DBF3CE26F63F675121D8918
SHA-512:	751E9BFD75D1685A490972FE0D40FDBCDA97607F6A500D051B400B002ED8C1D7CF9DAB019388B74796C9AFEAED4E317AC6B40A7E936D234536AEB0CB6C0D84 34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/images/hpp/Chrome_Owned_96x96.png
Preview:	.PNG.....IHDR...`...`.....w8....IDATx..]y....}..-.z.....P#" (.q...*.K.K..`.'9N.q.sb....1F.1..".D..3.!.5...EQ.....M.....?...o...5...y...W..}....8<.....8<.^.._/l....Q.....5[.C3@f.a{.....B.P...b.. .....S0o...Qg...].b.N....(1.6.....I(.D@.....L..q.q2...8I.6.mP(.V*F.^..$.....W.....%..|...@.h...6E.-I@>...%.H.l.w.8.H4y..=....K..qX_....J.....`.~..*..m.6.:y...;.'..j.6_....~....MV2.".os. [.J....P .D..B.;C...7.....,.....9...Vb.E.)"....A...m...{.}"...+....mW_....=.G...1.....H..4....z..I...#.=rgR.O[.(.....<.....@..''..ig..&wv.?0..q.....W..M.pi.....zj...oA<z.GWm.5V....."\ .*9':4.....}.....=.....mPo.q.....p.....R.....v.BQ?.....a..w;~....t.!$`.E!3..QJ....("....y_.! ...A.....CN...#.#.OJ4v..H..P..Q..a! e....q..\<..mH>`...CM.*..8.YC.H.2.....`....k5.~.n..!!`.....I..X. <1.&A.....R6....a.@.#..~@.`I.&..^t.....3./..K.....W.DM...k.E...~.9w.T.^..c_..\)..\.....z..R.....#.@...o_z.....9.g:...A.....5S...-.u..(.1.(....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20012, version 1.1
Category:	downloaded
Size (bytes):	20012
Entropy (8bit):	7.966842359681559
Encrypted:	false
SSDEEP:	384:Yc6bX9TagDCXKqs4+W5XVgaflKHjsGdZtlh3K/qzWz/scZpuB:YcCVaeCaF4ea9KHYQZtlh3Kgy4B
MD5:	DE8B7431B74642E830AF4D4F4B513EC9
SHA1:	F549F1FE8A0B86EF3FBDCB8D508440AFF84C385C
SHA-256:	3BFE46BB1CA35B205306C5EC664E99E4A816F48A417B6B42E77A1F43F0BC4E7A
SHA-512:	57D3D4DE3816307ED954B796C13BFA34AF22A46A2FEA310DF90E966301350AE8ADAC62BCD2ABF7D7768E6BDCBB3DFC5069378A728436173D07ABFA483C1025 AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....N,.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....R...`t.#.cmap...4.....L....cvt .....\...\1..Kfpgm...@...2.....$.gasp...t.....glyf.. ....:...j.'..hdmx..G,...f.....head..G....6...6...rhhea..G.....$....hmtx..G....a.....MOloca..JP.....\v@zmaxp..L,... ... .name..LL.....:.post..M(..... .m.dprep..M<.....S...)x...1.. P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T].....K=..K2 S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw...9..e!.....Q....f.. ....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....\|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	211319
Entropy (8bit):	5.516707088052012
Encrypted:	false
SSDEEP:	3072:pSQqRMTpptOl9LQhqzjCf3UtNSoj6bAjVovPl82D1UIP2cxPNBNo/:pJBkkhcj6LMsPlzD1UIPxPNBNo/
MD5:	4842C82192336E2603209B70D665CE1B
SHA1:	F4257376AF8C14CACAF191A61FD0BD10A2505641
SHA-256:	87E9018B97D7F5FFE9B793E73BEFEC37AD23C48EA3F728A0AF2708AE4CF6BB02
SHA-512:	47D53E94DEDD306F9A83BEE0B87FF75C5F91A300CFD0809EE9104F71E59FC6D0121A0B820E1488C68BF720E5081C4427178FA750C5129F8C2767637A3FC703D7
Malicious:	false
Reputation:	low
Preview:	/* JS */ gapi.loaded_1(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var Lx=function(){};Lx.prototype.H G=null;Lx.prototype.getOptions=function(){var a;(a=this.HG)||(a={},_.Mx(this)&&(a[0]=!0,a[1]=!0),a=this.HG=a);return a};.var Ox;Ox=function(){};_.A(Ox,Lx);_.Mx=function(a){if(!a.FJ&&"undefined"==typeof XMLHttpRequest&&"undefined"!=typeof ActiveXObject){for(var b=["MSXML2.XMLHTTP.6.0","MSXML2.XMLHTTP.3.0","MSX ML2.XMLHTTP","Microsoft.XMLHTTP"],c=0;c<b.length;c++){var d=b[c];try{return new ActiveXObject(d),a.FJ=d}catch(e){}}throw Error("ka");}return a.FJ};_.Nx=new Ox;. ._.Oe=_.Oe||{};.(function(){function a(c,d){return String.fromCharCode(d)}var b={0:!1,10:!0,13:!0,34:!0,39:!0,60:!0,62:!0,92:!0,8232:!0,8233:!0,65282:!0,65287:!0,65308:!0 ,65310:!0,65340:!0};_.Oe.escape=function(c,d){if(c){if("string"===typeof c)return _.Oe.escapeString(c);if("Array"===typeof c){var e=0;for(d=c.length;e<d;++e)c[e]=_.Oe.esc ape(c[e])}else if("o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\drive_2020q4_32dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\drive_2020q4_32dp[1].png	
Category:	downloaded
Size (bytes):	831
Entropy (8bit):	7.690596689293278
Encrypted:	false
SSDEEP:	24:ars5HGJLO4eG5bQxWGUpbIW779bHBoLU489YmBZo:arssA4L6hvaZ7wv8mmI
MD5:	916C9BCCCF19525AD9D3CD1514008746
SHA1:	9CCCE6978D2417927B5150FFAAC22F907FF27B6E
SHA-256:	358E814139D3ED8469B36935A071BE6696CCAD7DD9BDBFDB80C052B068AE2A50
SHA-512:	B73C1A81997ABE12DBA4AE1FA38F070079448C3798E7161C9262CCBA6EE6A91E8A243F0E4888C8AEF33CE1CF83818FC44C85AE454A522A079D08121CD8628D0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/images/branding/product/1x/drive_2020q4_32dp.png
Preview:	.PNG.....IHDR... ... .szz.....IDATx.b .....+.....m..dW.@..tm.Y.....m.....m.m..L.|.....{..b...t.....=H..qt..V..X..<jQc...p...fdU.\2.....9T...Jz!9...L.)&.....n....`~.T.\.\.$.....qQ.....LFOx .....^&,"bB..Lh9$_.6<...A...Q.T&y.,'...p...W`.2.?X(.o.4.J?.2...@.4...*..X..c.....[UZJ...MN.].z..f..DFe.J.....:Ir...0X.....).....^*..!....u..c..R4.GH....Y....E....Q.....+!..)...e".....,.Ge.r.T..!. .r..(.|.9f...}.....(...s..N...[..~.%6QF..g..r.....CN.e"(..uY.h._1.H.e....r.k..%^S.c..<..0.s.j..,D.....]..y.2(..OC.o\.3..".....cw...:;.btq.....w=.....R-[].4..]...?.....o..K../cC.<O...y..O.....{.-'Ln9..M.*6t.(.....o.K.$....bz.X._d.....Z].U.....t....Bf.Zl.^vA._..g.{l....V...{....=.jua..[...k.....j....Y\...!..+.m..X..t(.....".Mz.26l....7X.C...-...Z.lvl.....y}x.....7.m.VV....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\googleapis.proxy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12544
Entropy (8bit):	5.459759534754589
Encrypted:	false
SSDEEP:	192:8iApwYKUa9u5vocJJBA1UwgZCwm5Mi0+Sczl6:83pw9dk9JO1UkwmR0+Scx6
MD5:	EA48FD87996FB0F28A88587F004E6FB0
SHA1:	C9C3978DC99B6C1FFE24FD3647DF844B35F7BAA9
SHA-256:	3AD1AEEF90943035E2D354FAE106B8A8CA83F2C23D9DF3A7E92BA0C8EAD48204
SHA-512:	357C1525FDE4340DB7C8DAD05C9251F73B9187118D7190030CF42EDEC135EDA788720D46621CF15118C8999FE3BC3EC8D221CEB72F09B2CFC5FC9B9BE2B450 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/googleapis.proxy.js?onload=startup
Preview:	var gapi=window.gapi=window.gapi||{};gapi._bs=new Date().getTime();(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var g=this||self,h=function(a){return a};/*. gapi.loader.OBJECT_CREATE_TEST_OVERRIDE &&*/.var m=window,n=document,aa=m.location,ba=function(){},ca=/\[native code\]/,q=function(a,b,c){return a[b]=a[b]||c},da=function(a){a=a.sort();for(var b=[],c=void 0,d=0;d<a.length;d++){var e=a[d];e!=c&&b.push(e);c=e}return b},v=function(){var a;if((a=Object.create)&&ca.test(a))a=a(null);else{a={};for(var b in a)a[b]=void 0}return a},x=q(m,"gapi",{});var C;C=q(m,"___jsl",v());q(C,"I",0);q(C,"hel",10);var D=function(){var a=aa.href;if(C.dpo)var b=C.h;else{b=C.h;var c=/([#].*&|[#])jsh=([^&#]*)/g,d=/([?#].*&|[?#])jsh=([^&#]*)/g;if(a=a&&(c.exec(a)||d.exec(a)))try{b=decodeURIComponent(a[2])}catch(e){}}return b},fa=function(a){var b=q(C,"PQ",[]);C.PQ=[];var c=b.length;if(0===c)a();else for(var d=0,e=function(){++d===c&&a()},f=0;f<c;f++)b[f](e)},E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=ZdZQ6b[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	133
Entropy (8bit):	5.140362864588393
Encrypted:	false
SSDEEP:	3:VH/J0LTkLfgsevYXJEE3TgPRNYgNNw6eG+NpQXCn:VH/6LTkL5ZrT4NYINw6IpF
MD5:	1DA628D37E1B2A9DDA33F6C73C144B38
SHA1:	47542B3DDE5FC4D4C41962EEE31981CCCC99AFCF
SHA-256:	AD92244748720D7998AA79C99786D9E763F8F662EDEFF61F8D65AF897ED2C4C7
SHA-512:	B0921F28A60ABC1B896FA540B06673275E338DF332084583B6D4C2C7D7E358FD42D39C6481C5775EF398E6D0806542E8E6E2F0D0E7B5E73BEEE505D0DF02F66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/apps-fileview/_/js/k=apps-fileview.v.en_GB.PwnGz1jGsEk.O/d=0/ct=zgms/rs=AO0039uPH5M6znZvcCMu5D5-Kl3a1bdnTw/m=ZdZQ6b
Preview:	try{.p("ZdZQ6b");.var j_b=function(a,b){Hy.call(this,a,b)};J(j_b,Hy);fb(dya,j_b);..t();..}catch(e){_DumpException(e)}.// Google Inc..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=sym,i5dxUd,RAnnUd,syj,syk,uu7UOe,soHxf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	19178
Entropy (8bit):	5.634813585677532
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=sym,i5dxUd,RAnnUd,syj,syk,uu7UOe,soHxf[1].js	
SSDEEP:	384:7AiAvATOgNHm05h919g1iL/URBo6v27KuBzSkM9vjZ4IBcWkm:8vYagDo0/LIvjZ4IBDt
MD5:	D51A77322325229021AE01E2CE29BBA3
SHA1:	E4C27F5DB83F934609B1A03AA70894482F93BEF1
SHA-256:	CEB964DEF8E3425D83AC4C8ADBD5306A90BE75341D67D48DB8F96D013E0FE2C7
SHA-512:	5A3A4EF4B92565B30B246EDEA81C5691F99D97CF2051331D391BF1348B6DE39D850190F95E2A38A78FAAA05274C6D5E6EEADC7D716C9052679EB1142BD7D233
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sym");/*.. Copyright 2016 Google Inc... Permission is hereby granted, free of charge, to any person obtaining a copy. of this software and associated documentation files (the "Software"), to deal. in the Software without restriction, including without limitation the rights. to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. copies of the Software, and to permit persons to whom the Software is. furnished to do so, subject to the fol lowing conditions:.. The above copyright notice and this permission notice shall be included in. all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHAN TABILITY,. FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE. AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER. LIABILITY, WHETHER IN AN ACTIO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\proxy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	382
Entropy (8bit):	5.27625641887306
Encrypted:	false
SSDEEP:	6:hxuJLzLMb038GAB7fVBeQDXY2F6YkAbvOm/esHeOAS4Nhdx434QL:hYA0AB79hLFBkAb2m/esH2S4Nbx4IQL
MD5:	9F42164D397D054564B76F101EBA7DE5
SHA1:	5B071C1F5299862168A142F59C85D4FC40F597BF
SHA-256:	C08F127D5C7E5B4B1A9B1F21A913676088E7F2AB494F965A388A32AB811BEA31
SHA-512:	66E3381349CD77597C1D34ED1195AD654458450C9F6EC9509FF22385BD1DF4ECA5415FF5605E10B2FA6A30585E1B5BE72CF5D7ACB70B71A61A71D1B26CECFC9
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script nonce="vkfgfdhpUjbnqTvgWEJYmg">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async defer nonce="vkfgfdhpUjbnqTvgWEJYmg"></script>.</head>.<body>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\rs=AA2YrTucMMNgqLmXYRNewc0YuAWHKDjStA[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.038769514836251
Encrypted:	false
SSDEEP:	6:cZZwTcqcA2n6gt9VvKcZWbnRVIM6RoeSjIUVY/:kZfqcA26gAcZWfp6SVY/
MD5:	463A672A4B41F84482E3006A892107A7
SHA1:	ED47D2FA3202645D107183691617AC5ACD3E30D8
SHA-256:	D48E06992A89C3D7936C5C7F5E9416F6AEB9A494F7EE4A2C7926F5953D8CE965
SHA-512:	44567F0321338E44AE8A00C69E2DB47CD6CD5C004BF5246A58C0EFD40B7B963392F8A1306587D1F0B61D74963AF89E80CC02BB43802D5DB1D62AA52A62C5DF
Malicious:	false
Reputation:	low
Preview:	.gb_1e{background:rgba(60,64,67,0.90);border-radius:4px;color:#ffffff;font:500 12px 'Roboto',arial,sans-serif;letter-spacing:.8px;line-height:16px;margin-top:4px;min-height:14px;padding:4px 8px;position:absolute;z-index:1000}sentinel{}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\rs=AA2YrTvOGTt_rCDwY7qtNXydqo2XoBaJFw[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	173134
Entropy (8bit):	5.504660979761093
Encrypted:	false
SSDEEP:	1536:EoJJl0HzR8ucqmTTzyQmZFF3BkSnfqeTzEWwqZXfdbuqG0/meA+wzpMyREmjU6LT:EA0F8KfTZfCe/Td7ueA9emjC5f7jt0
MD5:	674C67AB1D83BF8DD03D111CCE34F495
SHA1:	878084FE404A226028DBC1F6886D35F72165BEDD
SHA-256:	78DFFB4DF29E86B42D03D48082683F4584921074C2433368B740D6ECF3A81DB8
SHA-512:	FF0D08EEC6987DB2404187DA34431941BAF5EF6B1C855CE51BD2B5FCCCBE8C72E7641B76724DC3DCD93B6504930D55F76E956904878210557E0EE6155E23496
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\rs=AA2YrTvOGTt_rCDwY7qtNXydqo2XoBaJFw[1].js	
Preview:	this.gbar_=this.gbar_||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/..}catch(e){_._DumpException(e)}.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var De=function(a,b){this.A=a;this.B=b;this.o=0;this.j=null};De.prototype.get=function(){if(0<this.o){this.o--;var a=this.j;this.j=a.next;a.next=null}else a=this.A();return a};var Ee=function(a,b){a.B(b);100>a.o&&(a.o++,b.next=a.j,a.j=b)};.var Fe=function(a){_.p.setTimeout(function(){throw a;},0)},Ge,He=function(){var a=_.p.MessageChannel;"undefined"===typeof a&&"undefined"!==typeof window&&window.postMessage&&window.addEventListener&&!_.w("Presto")&&(a=function(){var e=_.xe("IFRAME");e.style.display="none";document.documentElement.appendChild(e);var f=e.contentWindow;e=f.document;e.open();e.close();var g="callImmediate"+Math.random(),h="file:"==f.location.protocol?"*":f.location.protocol+"//"+f.location.host;e=(0,_.q)(funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\2295042476-docos_binary_i18n__en_gb[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1158543
Entropy (8bit):	5.577281746740191
Encrypted:	false
SSDEEP:	12288:HAkDYybgSlc78fxjJ2iYYtXaicXflkgjD60YCjE:gEYybhE2xEiYYoicXflkgjD5jE
MD5:	062FF425C956D7CF9BB647E75C9F7EFF
SHA1:	6DEB8374C9026C895F0209B08152E5562D15F1A3
SHA-256:	F4F3CFA519F32E767608CB4C8376C5B8A84B3B965AFECEF5219DDB35C796B721
SHA-512:	399C1FEA614B222727CDB5F94D4FD662A4B9394570CB188C433359AB939E6B5266E517AA144C117F6F9696E5B161AE40FF3BF017FD9B8D0CCCFCAB7BF0A0A19C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://docs.google.com/static/comments/client/js/2295042476-docos_binary_i18n__en_gb.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa="\r\n",ba=' class="',ca=' data-hovercard-id="',da=' data-name="',fa=' dir="ltr"><div class="',ha=" not supported",ia='" aria-hidden="true">• ',ja='" aria-hidden="true">• ',la=' " class="',ma='" peoplekit-id="',na='" role="button" tabindex="0" style="display:none">',oa='" role="button" tabindex="0" title="',pa='" role="button" tabindex="0">',qa='" role="heading">',ra='" style="display: none">',sa='" style="display: none"> ',.ta='" style="display: none"> ',wa='" style="width: ',xa='"/><label for="',g='">',ya='"> ',za='"> ',Aa='"> ',Ca='"> <table><tr><td

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26180, version 1.1
Category:	downloaded
Size (bytes):	26180
Entropy (8bit):	7.9847487601205405
Encrypted:	false
SSDEEP:	768:axmLo3N7711ZHlB8N6yt/DvXjXjmDNzv6:bLodN78li7jKJv6
MD5:	4F2E00FBE567FA5C5BE4AB02089AE5F7
SHA1:	5EB9054972461D93427ECAB39FA13AE59A2A19D5
SHA-256:	1F75065DFB36706BA3DC0019397FCA1A3A435C9A0437DB038DAAADD3459335D7
SHA-512:	775404B50D295DBD9ABC85EDBD43AED4057EF3CF6DFCCA50734B8C4FA2FD05B85CF9E5D6DEB01D0D1F4F1053D80D4200CBCB8247C8B24ACD60DEBF3D739A4CF0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF.....fD.....GDEF.....\.....QGPOS.....#..+...QGSUB.....y.....m.OS/2...|...U...`h...cmap.....~n...cvt .....y.....fpgm.....uo..gasp.....glyf.....=...m...5head..Z....6...6..'.hhea..Z.... ...$.0.5hmtx..[.....).loca..].....y.....K.6maxp..`H... ... .=..name..`h.....r.i6Ppost..a.....i]\prep..d....p..... ..x.U....Q.F..=#.0ZD.@@<.....''...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.....x..Z..+..=Z...~.....0.8....r.\|...=s&oG....q.Fg...Y....:Wc..>..p..p....).....{.aX..}.?.k... .....N.=.c.Do.....~2.=.i$....0..>..!.'v.....q.....>>.....o....30..0.w..|hR&mrf....,.Y.....%<..0.#.~...._a.c.....K.z...H1..u.2.Y_..0.9..`.,.:.=(.N~..*.a.<.D=....*.V....\..>./.B.`iE..A9.S.|?.g).Rj..8Q...h.y.G.^.kx.o.....(...#....9...,4I8...7..o.I|@x..1.>'...H.m..$.yp..f..%..F$0.0.I.1...WR...E..8?a..|''.....A.(...ZJ.q.K|...S.1..ht.ck....e...T.Zs,W..0..%.i.R...Ku.K.y.....j.RD..~..dpsh.fc.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21528, version 1.1
Category:	downloaded
Size (bytes):	21528
Entropy (8bit):	7.973887568128485
Encrypted:	false
SSDEEP:	384:uy/NCb8EbjU+Fos6gaUFZ3qR474EAqAG3w/Qpt/uxMsucMgwtDw031F:7/4zb7o6XqR4+3QptcuLg0w031F
MD5:	9680D5A0C32D2FD084E07BBC4C8B2923
SHA1:	8020B21E3DB55FF7A02100FAEBD92C2305E7156E
SHA-256:	2CFE69657C55133DAC6EA017B4452EFFF2131422ABD9E90500A072DF7CA5A9C8
SHA-512:	E19A498866F69F3D8136A65A5AB4E92CC047170673ED00B506E325165A84216267B9FEF1E5CFD66458E85ED820C12E9C345CEC9BEE4DE48E1C2E2B1A784F179
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xIIzQ.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#gcmap.....L....cvt .....R...R..-.fpgm.....4....s...gasp...<..... ....glyf...H..@...o..Na.hdmx..M....g.....head..Mp...6...6...ehhea..M....".$..{hmtx..M....k.....1<.loca..P8.....6...maxp..R.... ... .name..R4.....:.post..S..... .a.dprep.. S$.....D..].x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo. ...E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V. A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19916, version 1.1
Category:	downloaded
Size (bytes):	19916
Entropy (8bit):	7.96782347282656
Encrypted:	false
SSDEEP:	384:JiNCb8EbT1rG/3rjJmQ8uLc5ZiRE5HWSiPTI45tKVr6+F7gLLdz:k4zbM3rjEQ8uQPiRERWSGIWtKVrWJ
MD5:	A1471D1D6431C893582A5F6A250DB3F9
SHA1:	FF5673D89E6C2893D24C87BC9786C632290E150E
SHA-256:	3AB30E780C8B0BCC4998B838A5B30C3BFE28EDEAD312906DC3C12271FAE0699A
SHA-512:	37B9B97549FE24A9390BA540BE065D7E5985E0FBFBE1636E894B224880E64203CB0DDE1213AC72D44EBC65CDC4F78B80BD7B952FF9951A349F7704631B903C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`t.#.cmap.....L....cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L.:...j...w.hdmx..F....d.....head..GD...6...6.Y.ihhea..G|.....$...vhmtx..G....k.....\].loca..J.....g.L.maxp..K.... ... ...\name..L.....|..9.post..L..... .m.dprep..L.....: z/.Wx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D.. .`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG. .....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19888, version 1.1
Category:	downloaded
Size (bytes):	19888
Entropy (8bit):	7.96899630573477
Encrypted:	false
SSDEEP:	384:0c6bX9TSzYzCrQH+qXM6C0ouF0xcYye+5x/U3S0X5v+obEgm:0cCV8GuPVyzx/MS0X5v+oI/
MD5:	CF6613D1ADF490972C557A8E318E0868
SHA1:	B2198C3FC1C72646D372F63E135E70BA2C9FED8E
SHA-256:	468E579FE1210FA55525B1C470ED2D1958404512A2DD4FB972CAC5CE0FF00B1F
SHA-512:	1866D890987B1E56E1337EC1E975906EE8202FCC517620C30E9D3BE0A9E8EAF3105147B178DEB81FA0604745DFE3FB79B3B20D5F2FF2912B66856C38A28C07EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....P...`u.#.cmap...0.....L....cvt .....H...H+~..fpgm...(...3...._...gasp...\..... ....glyf...h..:q..i..+ Ohdmx..F....f.....head..GD...6...6...\hhea..G|.....$.&..hmtx..G....d.....E#loca..J.....\s@.maxp..K.... ... .name..K.....~..9.post..L..... .m.dprep..L.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c.._..72.. ." z.+..F.....&.&...`e..T]. ....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw. ..9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19824, version 1.1
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	7.970306766642997
Encrypted:	false
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C773527542228478CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf...L...:+..j.....hdmx..Fx...g.....head..F....6...6.j.zhhea..G.....$....hmtx..G8...].....Vlloca..I.....?.#.maxp..Kt... ... .name..K.....t.U9.post..Ld..... .m.dprep..Lx.....I.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D..`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|..|.|....o....l%.4.L.SI.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bscframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.906890595608518
Encrypted:	false
SSDEEP:	3:PouVn:hV
MD5:	FE364450E1391215F596D043488F989F
SHA1:	D1848AA7B5CFD853609DB178070771AD67D351E9
SHA-256:	C77E5168DFFDA66B8DC13F1425B4D3630A6656A3E5ACF707F4393277BA3C8B5E
SHA-512:	2B11CD287B8FAE7A046F160BEE092E22C6DB19D38B17888AED6F98F5C3E936A46766FB1E947ECC0CC5964548474B7866EB60A71587A04F1AF8F816DF8AFA221E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	63834
Entropy (8bit):	5.578341756797371
Encrypted:	false
SSDEEP:	1536:pWf2UtyeudISqZV9McRuq5tKNDW1TvE7UcjF9PEfLDwm:p2tyeudIz/TvE7Ucjvm
MD5:	99C6F3C3E2A14AAFEE2CEAAFE3912EC6
SHA1:	4E32CD0F03D6A2B48C5065F5C62E676BF75F3BD3
SHA-256:	02C0AAFF852E6114FB38BAFA13BA13DA41AF5B723E53299BF62CF4DE98302969
SHA-512:	7727111E481083264B9BE27E7716D53748BBE903F60A00298867E55F42CD842E0C7B81148744EBA9D037DD8EB3F9727E0E77779B49F4D5458167FDC353677757
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.GhYSaDTWhs4.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_CcmyUNBPTBtz4hsH0C6OHKqodVQ/cb=gapi.loaded_0
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,ra,za,Ca,Ea,Ja,Ta;_.da=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ra=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};za=ra(this);Ca=function(a,b){if(b)a:{var c=za;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ka(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=Wt6vjf,_latency,FCpbqb,WhJNk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	5680
Entropy (8bit):	5.496512765165309
Encrypted:	false
SSDEEP:	96:8bJaBq761HTZeaRWtU00xhbgkxuKFUu3oIo8bhDPV6RcAhg6Sk5ZY3yx:WslVh0kxusjbhmDh5RXYw
MD5:	58C3EAC6CE7891AFF0CC431251BA8E06
SHA1:	77FC74A4C6A4E23C7715FFD5A371EBAF94AF605E
SHA-256:	360959ED7C194B47F9784F4CC4CD482B1780F1477A7A4F7ACE0D5DD55DE668A6
SHA-512:	95502367859D0E5C77537A84B58E95D6BE72570A87C7F4500F6DDD095E3B670475D7BC03F6C880C0EF5BC3A8DE7A8ADEE340A08071E6E3BEA007CDDC4DB7757
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=Wt6vjf,_latency,FCpbqb,WhJNk[1].js	
Preview:	"use strict";this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{._.r("Wt6vjf");.var oJ=function(a){_.L(this,a,"f.bo",-1,null,null)};_.H(oJ,_.x);oJ.Cc="f.bo";oJ.prototype.Wa=function(){return _.yh(this,1)};.var pJ=function(){_.yi.call(this)};_.F(pJ,_.yi);pJ.prototype.Qa=function(){this.tn=!1;qJ(this);_.yi.prototype.Qa.call(this)};pJ.prototype.g=function(){rJ(this);if(this.Wh)return sJ(this),!1;if(!this.uo)return tJ(this),!0;this.dispatchEvent("p");if(!this.Hn)return tJ(this),!0;this.Kk?(this.dispatchEvent("r"),tJ(this)):sJ(this);return!1};.var uJ=function(a){var b=new _.Du(a.Ft);null!=a.tm&&b.g.set("authuser",a.tm);return b},sJ=function(a){a.Wh=!0;var b=uJ(a),c="rt=r&f_uid="+_.pe(a.Hn);_.Jl(b,(0,_.G)(a.i,a),"POST",c)};.pJ.prototype.i=function(a){a=a.target;rJ(this);if(_.Sl(a)){this.Sj=0;if(this.Kk)this.Wh=!1,this.dispatchEvent("r");else if(this.uo)this.dispatchEvent("s");else{try{var b=_.Tl(a),c=JSON.parse(b.substring(b.indexOf("\n")));va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=byfTOb,lsjVmc,LEikZe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	36246
Entropy (8bit):	5.469591338998175
Encrypted:	false
SSDEEP:	768:69MHE7rge8KHbtkhI9Nd07tHobXVxQirHhR+JTwAYtiFPIWRX+o:69MHRdtHcXVrmJkAvRXP
MD5:	765B42DAA6D94C1AF71D7D63DA4D2515
SHA1:	B93B561EEC980E4B582E5FD7285260B6393AFF68
SHA-256:	287770502E858A9D39A72581161E1082FCC97DE0577C6C526F74135BDC5CE989
SHA-512:	FA23A7E932A00DC16562FE5108F6F43AC8702D3BF5C1FD6812CE36A8BC026139AD0879C7C7DED484D52D0317C97D50E73C09267B44CCD0F73C274D1C6140A8
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{._.r("sy2o");.._.u();.._.Bu=function(a,b,c,d){a=d||a;b=b&&"*"!=b?String(b).toUpperCase():"";if(a.querySelectorAll&&a.querySelector&&(b||c))return a.querySelectorAll(b+(c?"."+c:""));if(c&&a.getElementsByClassName){a=a.getElementsByClassName(c);if(b){d={};for(var e=0,f=0,g;g=a[f];f++)b==g.nodeName&&(d[e++]=g);d.length=e;return d}return a}a=a.getElementsByTagName(b||"*");if(c){d={};for(f=e=0;g=a[f];f++)b=g.className,"function"==typeof b.split&&_.ia(b.split(/\s+/),c)&&(d[e++]=g);d.length=e;return d}return a};._.Cu=function(a,b,c,d){var e=_.Ri(a,b,function(f){_.Si(e);return c.call(d,f)},null)};_.r("syw");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var Gu,Iu,Ku,Ru,Lu,Nu,Mu,Qu,Ou,Su;_.Du=function(a,b){this.j=this.v=this.o="";this.S=null;this.s=this.i="";this.u=!1;var c;a instanceof _.Du?(this.u=void 0!==b?b:a.u,_.Eu(this,a.o),this.v=a.v,this

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=sy1a,sy1b,sy1c,sy1e,sy1f,sy2z,pwd_view[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	14968
Entropy (8bit):	5.587314380291293
Encrypted:	false
SSDEEP:	192:zpTmjh9lX7GTIiRxBWPd8hQjTGYXW+1mcYhdoydID766RdI/azhAtezTURI1l4jb:zpTmjpIMThrmvdoydID26HqEg8y7kQ
MD5:	45BA773E21E145A5690F896365BDF5A2
SHA1:	703532E80D79F42CB9D8145E27DC3380CBCFF5A7
SHA-256:	4F26A5B7DB1D42F54F15B2A14D373C9CE1C50E5AB73D40D27B362654639671FD
SHA-512:	52006BC0476E2CB13A5D02756971D03147288D8058AE89412834C1B8629FA29D9A53B4BED8951996485FC139FB8460EAB21457C8687A0093A9BD73DAC8564CCD
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sy1a");._.pS=function(){return"Try another way"};._.qS=function(){return"Enter code"};.._.l();..}catch(e){_._DumpException(e)}.try{._.k("sy1b");._.rS=function(){return(0,_.D)("Account recovery")};._.sS=function(){return"Verify that it's you"};.._.l();..}catch(e){_._DumpException(e)}.try{._.k("sy1c");._.T5a=function(a){a=a||{};return _.S5a(a)};._.S5a=function(a){a=a||{};return _.wt(a.qn,1)?"Enter your password":"Enter a password"};._.H("Db","",0,function(){return"Wrong password. Try again or click Forgot password to reset it.")};._.H("Eb","",0,function(){return"Forgot password?"});.._.l();..}catch(e){_._DumpException(e)}.try{._.k("sy1e");._.tS=function(a,b){a=a.oa&&(a.oa.ha||a.oa);var c=b.locale;b="";var d=c=_.xt(_.vt("en,en-US,"),c+",");d&&(d=a.tb(),d=_.G(null==d?null:d.getGivenName()));!d&&(d=!c)&&(d=a.tb(),d=_.G(null==d?null:d.Qc()));return b=d?b+(c?"Hi "+a.tb().getGivenName():""+a.tb().Qc()):b+"Welcome"};.._.l();..}catch(e){_._D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\postmessageRelay[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	567
Entropy (8bit):	5.191387721899702
Encrypted:	false
SSDEEP:	12:haxyErYfhVkrC9sAaQwERwPcQRAJmWmM8ytrI:haJspVkO9sF4wBiaSI
MD5:	B6309C01C376D86B4F1304BFCF0A925F
SHA1:	DC832A9D290A2403075498A628D38A6FC4496D6E
SHA-256:	C52B03C2DEF091F6B825325C93906FB06A4B32C2A42D2A398A1BAD4BFC98B9B6
SHA-512:	309F4613A55FC2B77074A29FD7DDAB2A5447119F71F98BD4BDF269002B2C611D6932FC7E54A7E4BFCAC96B85A9630B54A3C54F963F823DA75FA70CE79FE0416
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html><head><title></title><meta http-equiv="content-type" content="text/html; charset=utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1, user-scalable=0"><script nonce="hQqSOcXxr+hpADJ+aMLXag" src='https://ssl.gstatic.com/accounts/o/2801455510-postmessagerelay.js'></script></head><body ><script nonce="hQqSOcXxr+hpADJ+aMLXag" type="text/javascript" src="https://apis.google.com/js/rpc:shindig_random.js?onload=init"></script></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26228, version 1.1
Category:	downloaded
Size (bytes):	26228
Entropy (8bit):	7.98323449413518
Encrypted:	false
SSDEEP:	768:DBOEuz6T0146JY/J6unqhOYK0GJenzOoyo6:DBHuea4j/vnqo304enzUo6
MD5:	6DD4AD69D53830BDF5232A13482BD50D
SHA1:	6FFF1079D7E5D02A2259CB5D7833E790239E01CF
SHA-256:	5CE48D9E9D748AD4686094D3CC33F5AE1E272A5B618F5C6D146C4D12EF02E4A6
SHA-512:	FC91E8C4EAE384D38667E330C5A5E4BF82EBAC9A23AB88439D7C22CCDD125DE7F1371DD953F18DEE60EF68B680DF49A32F684157D90F20E1DAC3BFFC9DF84 18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF.....ft.....`.....GDEF.....\.....RGPOS.....#..+..P.LGSUB.....OS/2.....U...`h...cmap.....~n..cvt .....y.....fpgm...$.....uo..gasp.....glyf.... ..=...m..N..head..Z....6...6..'.hhea..[.... ...$.0.6hmtx..[<.....})9loca..]....z.....&..maxp..`p... ... .>..name..`.....r.i6Ppost..a<.....O...prep..e....p..... ..x.U....Q.F..=#.`ZD.@@<..... "...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.....x..Z.....%.....033333333...e....r.....U..u.r.....sV..Z..^..c..>v..p7.x...w.i...Y.....X...N<.k...0...kc];.u.....4.j...@....y."......,....#.;..... ....9...1....q..b..c...{....i2.H..g..:.....du.FX.].w3...{y...G....E.....~..RdX.|.\..U.^.x!....e.|.:.RX.Wxg.*...&.5....2n.Q...5.{..2....Ia.Vb%....:.Yn..QI.Z...x..Z.6..?.....G..W.*^#.e..#|l2p.S+.?'. <E..<....M.H..".>..d....>n%.(..."....<".....U/z.%..=...Le.cL3.4..4..znxgX!JD%.....s....&.a..z1._....O+..g.dm.?.9Vj.1...B...8..S..... ._.E.... .[#_..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26464, version 1.1
Category:	downloaded
Size (bytes):	26464
Entropy (8bit):	7.981932066790926
Encrypted:	false
SSDEEP:	768:OIYb4Auz6mM1gBEL1WuL1BU91c6HJ8Y4mAS:OI84AueNmwHpBU91qY4m7
MD5:	08F80DE0ACF68D82AABAB974A47D9E5F
SHA1:	E6F1C0F5395A9C297AA162468961C1FAF0EC1ED9
SHA-256:	4070911A1BB9CC52C4E4CD5E85CA186DCDE89308A0517A8FAA4715C2E0A9D45E
SHA-512:	720DE47FDDA648AF7CE5F3F574EFA3322191C4D0001E31181739D65FFE0CCECED56635AF58E5E828072A17EEE1ED1E318AF467B8ED7F4185EE0F5155501CD8 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff
Preview:	wOFF.....g`.....d.....GDEF.....q.....GPOS.....$..+..K.MGSUB.....OS/2.....U...`i`..cmap.....~n..cvt .....fpgm...T.....uo..gasp.....glyf...( ..>W..mNU!.)head..[....6...6..'.hhea..[.... ...$...4hmtx..[.....1'jloca..^....~.....t.maxp..a.... ... ....name..a4.....V..4.post..a.....O...prep..e.....^....x.D...Q...3..I.=D.@@....@... .."...}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....i...x..Z...6.=r.....q`.>....m.....fy.g..y4N...tAg.."KWWW.j.....8...n.3.:..1....9.+.}...b]....0..6V..).G.r... .....N...,R(.o.t.LU....;.{.l.y....i..w.{F..;p'.....,.....:3...|..,.`pGPAV.?....q!.....=.(cn.'<.....sK_...].U.W.....b....E|.o..Jp.n.uX....*J.q'SFy...l..Cd..XZ..RP...#.w...C)..s../..D..1.G...Sx ...e.....x.o.mJ...~./L..r...Y..sD./.....>$R`..&.v.....D..w.). .f.Y."<..V/.zQ{.8./...X*.....B..Jp#%.7.e>+L.Q.1..hd..k._...f..u....+....Q...N..|....$Lv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[2].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26412, version 1.1
Category:	downloaded
Size (bytes):	26412
Entropy (8bit):	7.982191465892414
Encrypted:	false
SSDEEP:	768:BXFxTA19K8CdHMT6KHQO8LWhHCWN1ekhzLS:9f29ZYMTwO8qh1nm
MD5:	142CAD8531B3C073B7A3CA9C5D6A1422
SHA1:	A33B906ECF28D62EFE4941521FDA567C2B417E4E
SHA-256:	F8F2046A2847F22383616CF8A53620E6CECDD29CF2B6044A72688C11370B2FF8
SHA-512:	ED9C3EEBE1807447529B7E45B4ACE3F0890C45695BA04CCCB8A83C3063C033B4B52FA62B0621C06EA781BBEA20BC004E83D82C42F04BB68FD6314945339DF2 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff
Preview:	wOFF.....g,.....GDEF.....q.....GPOS.....%..+...RGSUB.....y.....m.OS/2.....U...`i`..cmap.....~n...cvt .....fpgm...@.....uo..gasp..... ..glyf.....>F..m>Q..head..[\...6...6..'.hhea..[.... ...$...3hmtx..[.....<'3loca..^l...{...._.{.maxp..`.... ... ....name..a.....V..4.post..a.....i]\prep..et.....^....x.D...Q...3..IX=D.@ @....@....."...}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....g...x.....6.E..8.....affff.0.B..&.L...B.Nzy..n.T.t~w&..%[.dYzzz.Oe" ..lE.....m..7[s}...[l..)..)... (H.A.@q.57..S.@..._..].*.j.-^N.R...'...]v.0..2n.6...~....X..xN.DN.T..b..*Q5.E.).,Ql.....M....6.P."..|..*.tl5.....t..r.(...{M..T}..@.kbNP.I*.9-...=E.U'.{.....p|.t..qJE.9...'...*...z...L./.....r nXQ.6.|.....n.V.....K.?.G...<..<..Q.....C..K(s.PR.x\(..P@.P..z.DL.1.$*./.8A.8Q.r.Pr[e.Rt+~.}9.)E.'.U..z.G..G..OH/H...L.../..{S...EP.%.....o.....uN...'.}%..9.F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19936, version 1.1
Category:	downloaded
Size (bytes):	19936
Entropy (8bit):	7.969635209849544
Encrypted:	false
SSDEEP:	384:mvNCb8Eb+tS9nAIRMeC4J4h4Il7xtUOTCBGt+GXn/TUnOPgdGRhBg9r:Y4zbwTiMedJNIhkGbXn/TUnS+2hS9r
MD5:	E9DBBE8A693DD275C16D32FEB101F1C1
SHA1:	B99D87E2F031FB4E6986A747E36679CB9BC6BD01
SHA-256:	48433679240732ED1A9B98E195A75785607795037757E3571FF91878A20A93B2
SHA-512:	D1403EF7D11C1BA08F1AE58B96579F175F8DD6A99045B1E8DB51999FB6060E0794CFDE16BFE4F73155339375AB126269BC3A835CC6788EA4C1516012B1465E75
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`s.#.cmap.....L....cvt .....H...H.2..fpgm.....3...._...gasp...0..... ....glyf...<..;...n..e..hdmx..G<...i.....head..G....6...6.G..hhea..G.....$...`hmtx..H....M.....Wd^loca..JP.....maxp..L,... ... .name..LL.....x..9.post..M ..... .m.dprep.. M4.....+6.x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo.. ..E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|..|....o....I%.4.L.SI.&C.6..!`...{...c..\.J.(.2.C....V.A ..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ServiceLogin[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	1591925
Entropy (8bit):	5.831564409591938
Encrypted:	false
SSDEEP:	12288:yG23RmovafgjTE+Lqd5hVN06G+ZpHlAL30lmdSFw/O6COpVxG:yJFva4jTEL5hB8k4YSmQg
MD5:	59D1A46C215D38627FCEBC8715830DAA
SHA1:	C980DFA2F38F2B603D13962ED1609AB6888A9F23
SHA-256:	CE2A0B5AC69A15D60EA535DE954D3F0ED2AE9477B8311593C394268C9303C6CD
SHA-512:	DB20B4D4D53066826D0ACA1C99F76EE210BADDD3F5C8FCD0113826BD9392FF471D7033D00717EC1870AB870499B8C8DEC4162E170038EFD04039BD4D6ACFAD 1
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en-GB" dir="ltr"><head><base href="https://accounts.google.com/"><script data-id="_gd" nonce="4lB+lOdxi57DUaUwlxPvGw">windo w.WIZ_global_data = {"Mo6CHc":"2739372907586178024,"OewCAd":"%.@.\"xsrf\",null,[\"\"]\n,\"AFoagUWj8TTSh6_Yq6koByQKu46O8vFSIQ:1610383993407\"]\n","Qzxix c":"S-1945389116:1610383993387167","thykhd":"AKH95es60yMCqoQoZS9GBBXcM1-iXXoj5vLT4yX_YbkzZxc0luiPMIOCuUVqIZaoEeI_4mODj311bZUX1lLZLE- rUnbE4azacyPDx9uQFZuoHdbHxaQdG0w\u003d","w2btAe":"%.@.null,null,\"\",false,null,null,true,false]\n"};</script><meta charset="utf-8"/><meta http-equiv="X-UA-Co mpatible" content="IE=edge"/><link rel="shortcut icon" href="//www.google.com/favicon.ico"/><noscript><meta http-equiv="refresh" content="0; url=https://account s.google.com/ServiceLogin?continue=https%3A%2F%2Fdrive.google.com%2Ffile%2Fd%2F1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT%2Fview%3Fusp%3Ddr ive_web&rip=1&nojavascript=1&followup=https%3A%2F%2Fdrive.google.com%2Ffile%2Fd%2F1RxVVBTYMGBSabrzamAJS5QvvM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wIJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wIJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702 563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/favicon.ico
Preview:	..... .h...&... ....(..... ....0.....v.].X.:.X.:.r.Y..... .....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V.8.....F..B..... .....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k.....7R..8F..... .....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv.....]i..<J..:G..Zf..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\m=_b,_tp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\m=_b,_tp[1].js	
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	155456
Entropy (8bit):	5.475981703633856
Encrypted:	false
SSDEEP:	3072:OVIpx9eNt13qrIrPheaFFI32qsWeNLwwt:oE/rIr7Fq/sh+wt
MD5:	F906B95D6B39768E335DA7A6360B627D
SHA1:	D4B0BE3609ACC9813AD29030C12C2975691AD0E9
SHA-256:	60AC04C61BDFE73F7C419069E07477461242E7623DD39568BDBC53BAB936C998
SHA-512:	41440CE57532B70346056329A5045F2BE2E8F6D77803D16F3F9F2C34A460DE0B8776AFB752465D1CCF07DA63F092982D4397F190CB52B10F97C6E2C7649B6AB6
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{.var xa,Ha,Ka,La,Oa,Pa,Ra,Ua,Va,Za,ab,hb,lb,ob,Jb,wb,Nb,Qb,Sb,ac,aa,cc,dc,ec,gc,hc,kc,lc;_.p=function(a){return function(){return aa[a].apply(this,arguments)}};_.q=function(a,b){return aa[a]=b};_.ba=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,_.ba);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a));this.g=!0};_.ca=function(a){return a[a.length-1]};._.da=function(a,b,c){for(var d="string"===typeof a?a.split(""):a,e=a.length-1;0<=e;--e)e in d&&b.call(c,d[e],e,a)};_.fa=function(a,b,c){b=_.ea(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]};_.ea=function(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)if(f in e&&b.call(c,e[f],f,a))return f;return-1};_.ia=function(a,b){return 0<=(0,_.ha)(a,b)};_.ja=function(a){if(!Array.isArray(a))for(var b=a.length-1;0<=b;b--)delete a[b];a.length=0};_.ka=function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\m=v[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1044629
Entropy (8bit):	5.569063227065614
Encrypted:	false
SSDEEP:	12288:d0EahD8oNnsT2pJ3tQJoVqtBIAxD+sk4rkl:dlaBNNnsT2pJ3tQJoVqvIAxD+P4C
MD5:	4A6EA45D8708FE81980BC3E50F1F0FCE
SHA1:	457DBB35CD7B7BE617EF8BB797C6C9A02A1A6F7F
SHA-256:	944131B4510B391A5A0F29832EE7B02F4DD48DDA15CF2F6CF348DEDB931DE001
SHA-512:	9F03EE27F7D0E11E54D1893AF3FACA6FB6A8EB0A7E21184751DEA52B1E410F798236590E3C0D2A612A51E0056CCEEA75147B5617167C3F33674182CD62D8B2E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/apps-fileview/_/js/k=apps-fileview.v.en_GB.PwnGz1jGsEk.O/d=1/ct=zgms/rs=AO0039uPH5M6znZvcCMu5D5-Kl3a1bdnTw/m=v
Preview:	try{.var g,aa=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,aa);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a));this.D=!0},ba=function(a){return a[a.length-1]},ca=function(a,b,c){for(var d="string"===typeof a?a.split(""):a,e=a.length-1;0<=e;--e)e in d&&b.call(c,d[e],e,a)},fa=function(a,b,c){b=ea(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]},ea=function(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)if(f in e&&b.call(c,.e[f],f,a))return f;return-1},baa=function(a,b,c){b=aaa(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]},aaa=function(a,b,c){for(var d="string"===typeof a?a.split(""):a,e=a.length-1;0<=e;e--)if(e in d&&b.call(c,d[e],e,a))return e;return-1},ja=function(a,b){return 0<=ha(a,b)},la=function(a){return 0==a.length},ma=function(a){if(!Array.isArray(a))for(var b=a.length-1;0<=b;b--)delete a[b];a.length=0},na=function(a,b){ja(a,b)||a.push(b)},pa=function(a,b){b=ha(a,b);var c;(c=0<=b)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\metadata[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1494
Entropy (8bit):	5.236479796099532
Encrypted:	false
SSDEEP:	24:Gv4+jaF9X9xePE1VpVKKePE1VMRePE1Vxw+DeKKePE1V8kVa8TmGqxB:GwdFtLV7iHy7ebYmGS
MD5:	05DB3B46200365A1F6BCF548A88F7AF0
SHA1:	9BD884749982935EEC0D99959EEFCA626DB581C4
SHA-256:	89BF208312A6DBABB4C48E019FA8315A79A119B69DC2138C9CE5D01B49BB78DB
SHA-512:	A083401E508AD4464443CB87A2A093ED5D34C88A915A0DB66F8248DDE29CD78F92CEA03493B2E458FF7EE58445195C9A9054B07947B7D5DEE707A439E925094
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://blobcomments-pa.clients6.google.com/v1/metadata?docId=1RxVVBTYMGBSabrzamAJS5QvvMY1Aq2DT&revisionId=0BzS25sUh1l9pZ3gzNmsyQUlXN1FqODFWdEhUZGFyS0xFSUNNPQ&userLocale=en-GB&timeZoneId=Etc%2FGMT-1&forceImportEnabled=true&key=AIzaSyCMp6sr4oTC18AWkE2Ii4UBZHTHEpGZWZM&%24unique=gc797
Preview:	{. "serializedDocosKeyData": "[\"kd\",\"//docs.google.com/static/comments/client/js/2295042476-docos_binary_i18n__en_gb.js\",[\"\",\"\",\"\",\"\",\"\",\"\"]\n,0,null,null,\"\",[null,0]\n,1,[\"Anonymous\",null,\"//ssl.gstatic.com/docs/common/blue_silhouette96-0.png\",\"ANONYMOUS_105250506097979753968\",1,null,1]\n,1,1,\"AAHRpnXtotJBI0o_lAZgw85osFWndMiTjGeaX1XcfEr22_VKLpdgHGJCTdaannFMkWkrWSFBSzJ98oqJC_23ykH78wY8YE552tg\",0,null,null,null,null,1,null,null,1,\"https://13.docs.google.com/comments/d/AAHRpnXtotJBI0o_lAZgw85osFWndMiTjGeaX1XcfEr22_VKLpdgHGJCTdaannFMkWkrWSFBSzJ98oqJC_23ykH78wY8YE552tg/xpc?id\\u003dAAHRpnXtotJBI0o_lAZgw85osFWndMiTjGeaX1XcfEr22_VKLpdgHGJCTdaannFMkWkrWSFBSzJ98oqJC_23ykH78wY8YE552tg\\u0026anon\\u003dfalse\",null,\"//comments/d/AAHRpnXtotJBI0o_lAZgw85osFWndMiTjGeaX1XcfEr22_VKLpdgHGJCTdaannFMkWkrWSFBSzJ98oqJC_23ykH78wY8YE552tg\",null,1,0,null,null,\"prod\",0,null,null,0,null,null,null,1,0,1,0,null,0,[\"tf\",60000,0,null,null,null,null,null,null,null,null,null,null,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\rpc_shindig_random[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12542
Entropy (8bit):	5.459748218330448
Encrypted:	false
SSDEEP:	192:8iApwYKUa9u5vocJJBA1UwgZCwm5Mi0+Sczlu:83pw9dk9JO1UUwmR0+Scxu
MD5:	822CDA70623F99D31CE02EAF2CDCA26B
SHA1:	603198A0E8E97EEE68433A8EEE91BE4B4AC21FE9
SHA-256:	392799A14B7605CC127E5AE7B525B9CAEF1BDA42337B7ABEA5F5255590898391
SHA-512:	A74E9202AA2C630A493638D555666DE8E8A19A39CB23D8DD94B9C777D1F4B7C8F9F7F9BF1576353A56F912D91BB2EFF3A0E7D671273F64395D2530BD2EC08F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/rpc:shindig_random.js?onload=init
Preview:	var gapi=window.gapi=window.gapi||{};gapi._bs=new Date().getTime();(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var g=this||self,h=function(a){return a};/*. gapi.loader.OBJECT_CREATE_TEST_OVERRIDE &&*/.var m=window,n=document,aa=m.location,ba=function(){},ca=/\[native code\]/,q=function(a,b,c){return a[b]=a[b]||c},da=function(a){a=a.sort();for(var b=[],c=void 0,d=0;d<a.length;d++){var e=a[d];e!=c&&b.push(e);c=e}return b},v=function(){var a;if((a=Object.create)&&ca.test(a))a=a(null);else{a={};for(var b in a)a[b]=void 0}return a},x=q(m,"gapi",{});var C;C=q(m,"___jsl",v());q(C,"I",0);q(C,"hel",10);var D=function(){var a=aa.href;if(C.dpo)var b=C.h;else{b=C.h;var c=/([#].*&|[#])jsh=([^&#]*)/g,d=/([?#].*&|[?#])jsh=([^&#]*)/g;if(a=a&&(c.exec(a)||d.exec(a)))try{b=decodeURIComponent(a[2])}catch(e){}}return b},fa=function(a){var b=q(C,"PQ",[]);C.PQ=[];var c=b.length;if(0===c)a();else for(var d=0,e=function(){++d===c&&a()},f=0;f<c;f++)b[f](e)},E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\v-sprite33[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	33468
Entropy (8bit):	5.254627196981829
Encrypted:	false
SSDEEP:	768:cDAqsYMHpd13D3XPJ+2J+pDP4UHUqGtB4v4k9nURfrmLN/JTU3iU3yhmk92Rrq:cs9HpdJoFF4cSiP9nkDi/JTwiwyhmk9l
MD5:	85842AFF0FBE1725BAA54DF7E2D6C1C2
SHA1:	63322A45D2ACA287D14765137C2F2212479C0974
SHA-256:	BF56A15B0F52A64ED8904A32947E2057EC5C7931B4583D0BF4C118541A458AF4
SHA-512:	28122FF108CEF6EDFBD2DF0FD1F003FE86DC1B7CA52E5689F3240414AB6F3AEA88F2DAA3507EEEF84018AF46854E9BA7E91B03BF2E72229DCAB9814871FC685 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/docs/common/viewer/v3/v-sprite33.svg
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYPE svg PUBLIC '-//W3C//DTD SVG 1.1//EN' 'http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd'>.<svg width="31px" height="3154px" preserveAspectRatio="none" version="1.1" viewBox="0 0 31 3154" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. <g transform="translate(0,1066)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5H7V9h4V5h2v4h4v2h-4v4h-2v-4z"/>. </g>. <g transform="translate(0,3074)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5H7V9h4V5h2v4h4v2h-4v4h-2v-4z" fill="#fff"/>. </g>. <g transform="translate(0,986)" fill="#fff">. <path d="m17.705 10.14-3.405-6.1401h-4.6l-6.1 11 2.1 4h8.1027c0.4644 0.8028 1.1094 1.488 1.8795 2h-9.9822c-0.7 0-1.4-0.4-1.8-1.1l-2.1-4c-0.3-0.6-0.3-1.3 0-1.9l6.2-11c0.3-0.6 1-1 1.7-1h4.6c0.7 0 1.4 0.4 1.8 1l3.9307 7.0882c-0.3348-0.058-0.6792-0.0882-1.0307-0.0882-0.4446 0-0.878 0.0

C:\Users\user\AppData\Local\Temp\~DFA089160FFABE2899.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.5247130083182049
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+hwnO3DHgTX1nYT/9qoy4y:kBqoxDhHjgE+hyygoy4
MD5:	86B9E9D22DC5AA19DDEDA7F0FC872890
SHA1:	0A113DA38716EC605D842BAABE92D5DC60C5142B
SHA-256:	DC71F312D55D280B26EE8D21EE461F31727303F3C35B20BBA067F94520106205
SHA-512:	B2C8C2B997327406A360C993AC04074F34882563895375C976929D34768A0AD14831BD9EE1CA9F9ECED3BA934B1D202D00A778529EC6A4E452E93EAFD662AD0
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFAFE79E2A81027319.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DFAFE79E2A81027319.TMP	
File Type:	data
Category:	dropped
Size (bytes):	62702
Entropy (8bit):	1.069786376640833
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+iEOnUra+kOjEXJtfLfdfFfQfGf0k9tHxfQHxqQHxqQHxFvajJ:+7dlWMp
MD5:	B83E8C593CC4EC7B6ECD041643C45095
SHA1:	0B7B604CA3469FC42DB4BE414A66DDB68312B26F
SHA-256:	812A47AF9140D8D6BE60EA86292A488A6BEBCC5CE627DB358913AA328EAE2A0B
SHA-512:	FEBE532F28AE31416658F501B4C56F68D40CABC9881B5CCC6C82B188C0D4482426B704DD6DB3872AA0CB906D3596EE9671946C06BFF6D338A31BD9FEC0A7EF 3
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD9E42A43549C9786.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4775062271882622
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lomS9lomC9lWmoNi8iNni8iLEbLChTnT3:kBqoIuQD88V8x65
MD5:	DBBC00FEA199F7F8A8901D3C5853E2B4
SHA1:	5FF04E3FB5D50AB047518E1F5F5B335830975822
SHA-256:	1C9ABDACFC25B2016C75D5F6C33F3444E20EC2DDB8E8E253B98DC2B469B61D1C
SHA-512:	0FDAAA5080FAA7E0B37CA9C298CCE5B6F83777A4913A9552CD12EE7D78B3D75E2ED661A10EA4BB63793951A7BF630B8C2B7B7EF29960DFC6ECC5672A47741A 74
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 63

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:52:56.291595936 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.294594049 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.334115982 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.334223032 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.335344076 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.336972952 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.337091923 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.337858915 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.377746105 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.380254984 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.391644001 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.391685963 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.391710043 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.391731024 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.391733885 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.391760111 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.391769886 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.391822100 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.394107103 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.394149065 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.394170046 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.394193888 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.394242048 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.394284010 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.403712034 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.404216051 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.404620886 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.414316893 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.414758921 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.446516991 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.446549892 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.446604967 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.446635962 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.446675062 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.448028088 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.448065042 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.448088884 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.448108912 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.448144913 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.448194027 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.448534966 CET	49753	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.457130909 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.457146883 CET	443	49754	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.457166910 CET	443	49754	172.217.23.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:52:56.457345963 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.458937883 CET	49754	443	192.168.2.4	172.217.23.1
Jan 11, 2021 17:52:56.490979910 CET	443	49753	172.217.23.1	192.168.2.4
Jan 11, 2021 17:52:56.506534100 CET	443	49754	172.217.23.1	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:52:47.244004965 CET	49910	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:47.300930023 CET	53	49910	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:48.220818996 CET	55854	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:48.268826008 CET	53	55854	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:49.192405939 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:49.248864889 CET	53	64549	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:50.342745066 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:50.399200916 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:51.403682947 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:51.451817036 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:51.723139048 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:51.780915022 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:52.847105026 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:52.852031946 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:52.900224924 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:52.911223888 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:53.515664101 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:53.524606943 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:53.592401028 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:53.592775106 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:54.081099033 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:54.149180889 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:55.909779072 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:55.944665909 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:55.991944075 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.024519920 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.209778070 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.211596966 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.268444061 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.288937092 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.370477915 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.421204090 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.452790976 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.461715937 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.496052980 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.519968987 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.525719881 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.543961048 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:56.686860085 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:56.750863075 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:57.333551884 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:57.398190022 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:57.681750059 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:57.748717070 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:57.777832031 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:57.828661919 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 17:52:58.895853043 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:52:58.943866968 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:00.193546057 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:00.244477987 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:01.371407986 CET	62420	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:01.419583082 CET	53	62420	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:02.206788063 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:02.263148069 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:03.578813076 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:03.626775980 CET	53	50183	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:53:04.832047939 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:04.882904053 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:09.950046062 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:10.019881010 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:11.695485115 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:11.743484020 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:16.263722897 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:16.328578949 CET	53	55916	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:19.676480055 CET	52752	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:19.737082005 CET	53	52752	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:21.695044994 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:21.745857954 CET	53	60542	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:22.364124060 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:22.412075996 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:22.703295946 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:22.754188061 CET	53	60542	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:23.359734058 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:23.407851934 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 17:53:23.719271898 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:53:23.770090103 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 17:52:56.211596966 CET	192.168.2.4	8.8.8.8	0x18e7	Standard query (0)	drive-thirdparty.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 11, 2021 17:53:16.263722897 CET	192.168.2.4	8.8.8.8	0xaadc	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 17:52:56.288937092 CET	8.8.8.8	192.168.2.4	0x18e7	No error (0)	drive-thirdparty.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 17:52:56.288937092 CET	8.8.8.8	192.168.2.4	0x18e7	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)
Jan 11, 2021 17:53:16.328578949 CET	8.8.8.8	192.168.2.4	0xaadc	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 17:52:56.391731024 CET	172.217.23.1	443	192.168.2.4	49753	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 17:52:56.394193888 CET	172.217.23.1	443	192.168.2.4	49754	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 6968 Parent PID: 800

General

Start time:	17:52:50
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff79ecb0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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 Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7020 Parent PID: 6968

General

Start time:	17:52:51
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6968 CREDAT:17410 /prefetch:2
Imagebase:	0xfb0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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 Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly