ID: 324363
Cookbook: browseurl.jbs
Time: 17:07:23
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report https://plus.google.com/+InvorderingsbedrijfNl-Incasso/posts
Overview 44
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 11
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 47
No static file info 47
Network Behavior 47
Network Port Distribution 47
TCP Packets 47
UDP Packets 49
DNS Queries 50
DNS Answers 51
HTTPS Packets 51
Code Manipulations 53
Statistics 53
Behavior 53
System Behavior 53
Analysis Process: iexplore.exe PID: 5776 Parent PID: 792 53
General 53
File Activities 54
Registry Activities 54

Analysis Process: iexplore.exe PID: 244 Parent PID: 5776 54
General 54
File Activities 54
Registry Activities 54
Disassembly 55

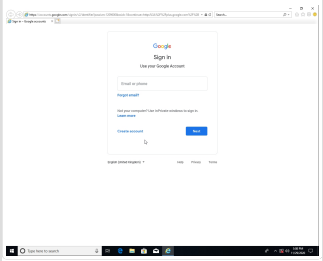
Analysis Report https://plus.google.com/+Invorderingsb…

Overview

General Information

Sample URL:	http://https://plus.google.com/+InvorderingsbedrijfNl-Incasso/posts
Analysis ID:	324363

Most interesting Screenshot:



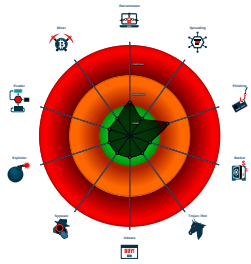
Detection

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

Signatures

- Found iframes
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5776 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 244 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5776 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

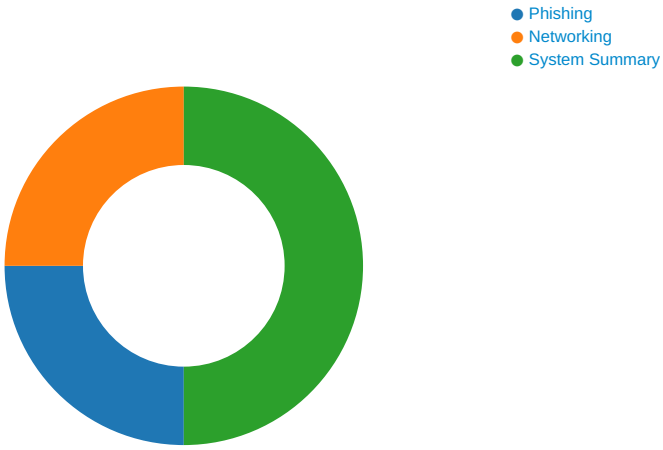
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



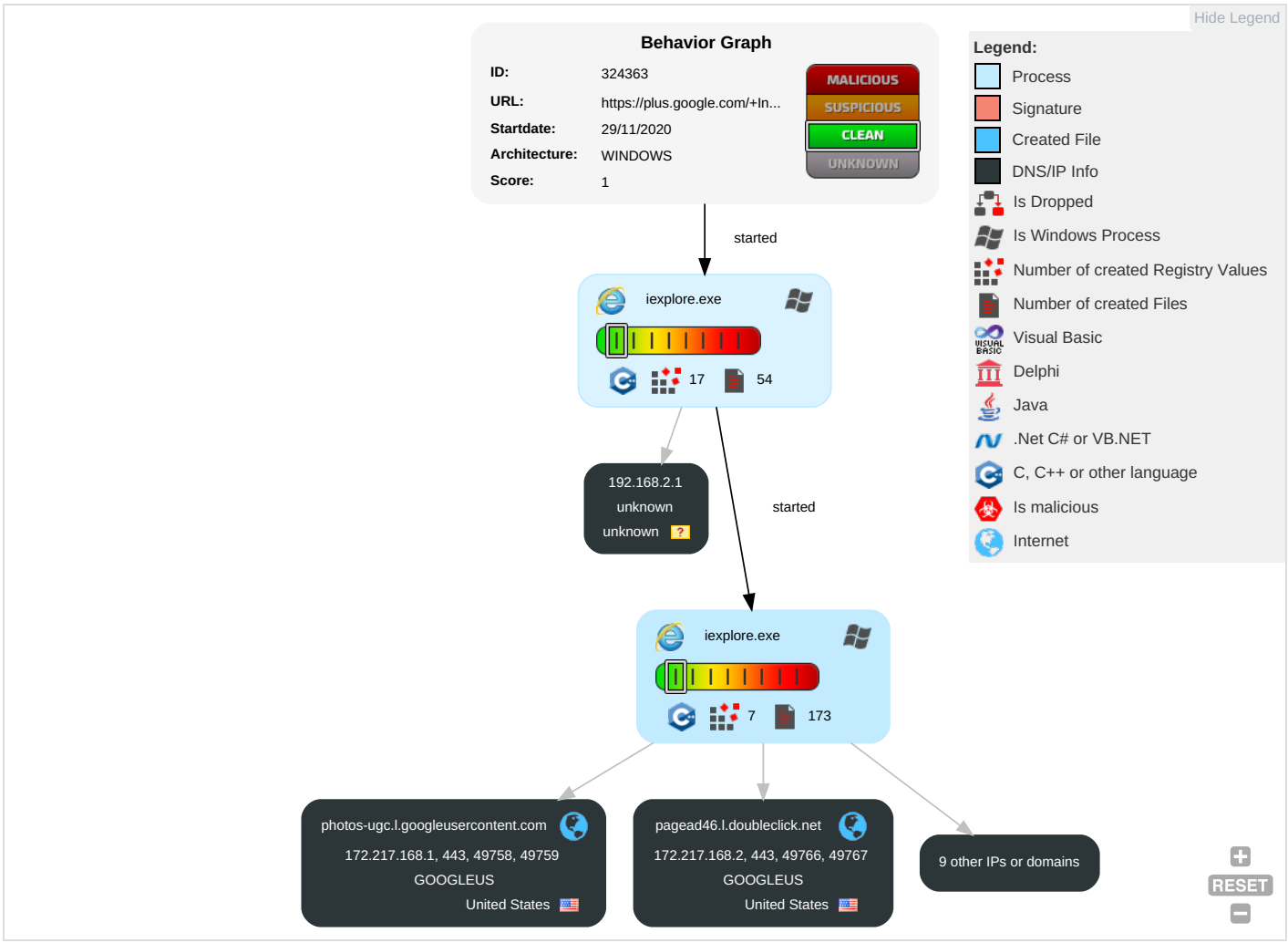
Click to jump to signature section

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	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

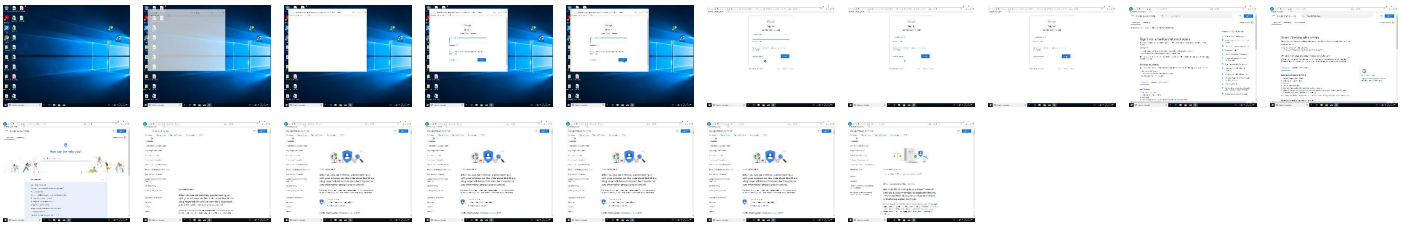
Behavior Graph

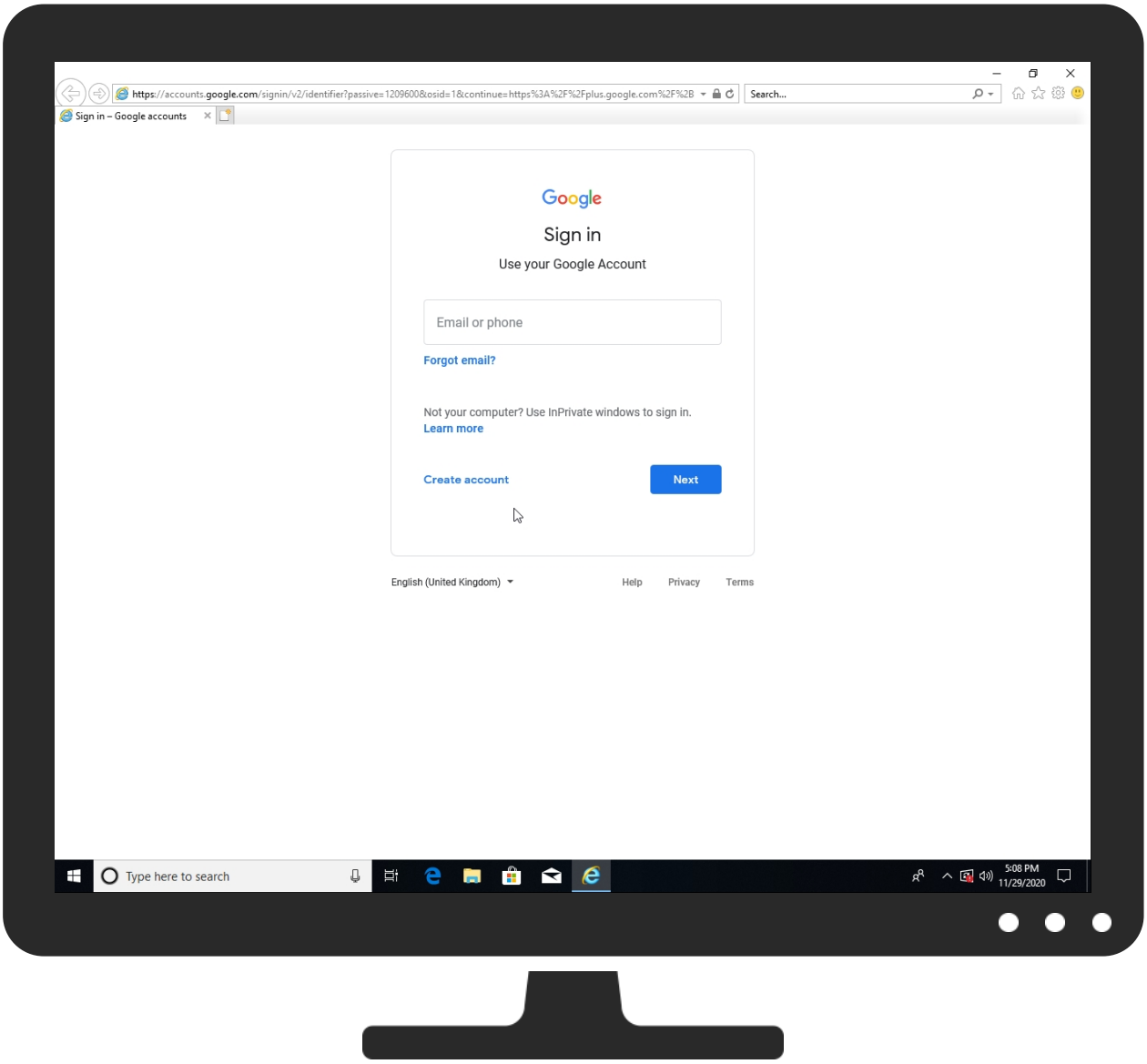


Screenshots

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://plus.google.com/+InvorderingsbedrijfNl-Incasso/posts	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://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	

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://www.broofa.com	0%	URL Reputation	safe	
http://https://translate.google.co.uk/?hl	0%	URL Reputation	safe	
http://https://translate.google.co.uk/?hl	0%	URL Reputation	safe	
http://https://translate.google.co.uk/?hl	0%	URL Reputation	safe	
http://https://translate.google.co.uk/?hl	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/webhp?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/webhp?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/webhp?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/webhp?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://policies.Root	0%	Avira URL Cloud	safe	
http://https://readalong.google/intl/en-GB_GB/privacy	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/save	0%	URL Reputation	safe	
http://https://www.google.co.uk/save	0%	URL Reputation	safe	
http://https://www.google.co.uk/save	0%	URL Reputation	safe	
http://https://www.google.co.uk/save	0%	URL Reputation	safe	
http://https://www.google.co.uk/webhp	0%	Virustotal		Browse
http://https://www.google.co.uk/webhp	0%	Avira URL Cloud	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://books.google.co.uk/bkshp?hl	0%	URL Reputation	safe	
http://https://books.google.co.uk/bkshp?hl	0%	URL Reputation	safe	
http://https://books.google.co.uk/bkshp?hl	0%	URL Reputation	safe	
http://https://books.google.co.uk/bkshp?hl	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products	0%	Virustotal		Browse
http://https://www.google.co.uk/intl/en-GB/about/products	0%	Avira URL Cloud	safe	
http://https://policies.e.com/terms?gl=GB&hl=en-GB382296Root	0%	Avira URL Cloud	safe	
http://https://www.gstatic.	0%	URL Reputation	safe	
http://https://www.gstatic.	0%	URL Reputation	safe	
http://https://www.gstatic.	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance	0%	Avira URL Cloud	safe	
http://https://policies.googl	0%	URL Reputation	safe	
http://https://policies.googl	0%	URL Reputation	safe	
http://https://policies.googl	0%	URL Reputation	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://www.google.co.uk/shopping?hl	0%	URL Reputation	safe	
http://https://www.google.co.uk/shopping?hl	0%	URL Reputation	safe	
http://https://www.google.co.uk/shopping?hl	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://support.google	0%	URL Reputation	safe	
http://https://support.google	0%	URL Reputation	safe	
http://https://support.google	0%	URL Reputation	safe	
http://https://readalong.google	0%	URL Reputation	safe	
http://https://readalong.google	0%	URL Reputation	safe	
http://https://readalong.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	172.217.168.2	true	false		high
stats.l.doubleclick.net	74.125.128.157	true	false		high
photos-ugc.l.googleusercontent.com	172.217.168.1	true	false		high
googlehosted.l.googleusercontent.com	216.58.215.225	true	false		high
accounts.youtube.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
lh4.ggpht.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://staging-realtimesupport-googleapis.sandbox.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://schema.org/Thing	2917834[1].htm.2.dr	false		high
http://https://www.google.co.uk/intl/en/about/products?tab	so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.broofa.com	rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/user/googlehelp?sub_confirmation=1	2364824[1].htm.2.dr	false		high
http://https://translate.google.co.uk/?hl	so[1].htm.2.dr, so[2].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/embed/	Z2QQ58E8.js.2.dr	false		high
http://https://www.youtube.com/watch?v=ggoJFaE71W8	ggoJFaE71W8[1].htm.2.dr	false		high
http://https://casespartner-pa.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://www.google.co.uk/intl/en-GB/about/products?tab	so[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/embed/ZdEIZNg3epQ?rel=0&showinfo=0&theme=light&version=3&hl=	privacy[1].htm.2.dr	false		high
http://https://www.youtube.com/embed/ZdEIZNg3epQ?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pr	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://www.google.co.uk/webhp?tab	so[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/feed/history?utm_source=pp&hl=en_GB	privacy[1].htm.2.dr	false		high
http://https://signaler-pa.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://support.googlee.com/signin/v2/identifier?passive=1209600&osid=1&continue=https%3A%2F%2Fplus.	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://g.co/recover	ServiceLogin[1].htm.2.dr	false		high
http://www.youtube.com/watch?v=48l-xdS4pXg	48l-xdS4pXg[1].htm.2.dr	false		high
http://https://realtimesupport.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://www.google.co.uk/finance?tab	so[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://youtube.com/streaming/otf/durations/112015	base[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://policies.Root	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://readalong.google/intl/en-GB_GB/privacy	privacy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/YlmVKT3Zvhw?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pr	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://www.youtube.com/feed/history/search_history?utm_source=pp	Z2QQ58E8.js.2.dr	false		high
http://youtube.com/streaming/metadata/segment/102015	base[1].js.2.dr	false		high
http://https://www.youtube.com	iframe_api[1].js.2.dr, www-widgetapi[1].js.2.dr	false		high
http://https://youtu.be/	base[1].js.2.dr	false		high
http://https://www.youtube.com/iframe_api	Z2QQ58E8.js.2.dr	false		high
http://https://www.google.co.uk/save	so[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.co.uk/webhp	so[2].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://admin.youtube.com	base[1].js.2.dr	false		high
http://https://www.google.	Z2QQ58E8.js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/embed/ggoJFaE71W8?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pr	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://www.youtube.com/feed/history?utm_source=pp	Z2QQ58E8.js.2.dr	false		high
http://https://books.google.co.uk/bkshp?hl	so[1].htm.2.dr, so[2].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lh3.googleusercontent.com/fKYxJWmqWKS5JTWJUHJSE6u4tKZ6JbFx7YGMbbH0cI72r3E2MhU0vPrE6uaflUm94Q	2364824[1].htm.2.dr	false		high
http://www.youtube.com/watch?v=ggoJFaE71W8	ggoJFaE71W8[1].htm.2.dr	false		high
http://https://www.google.co.uk/intl/en-GB/about/products	so[2].htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://www.blogger.com/?tab	so[1].htm.2.dr	false		high
http://https://www.youtube.com/embed/YlmVKT3Zvhw?rel=0&showinfo=0&theme=light&version=3&hl=	privacy[1].htm.2.dr	false		high
http://https://policies.e.com/terms?gl=GB&hl=en-GB382296Root	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	2364824[1].htm.2.dr, operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://lh4.ggpht.com/WnIr0x3yhEpMTql4DCrl_ZOc9vdK_yV0WPig_suRjHQCv4B-2CmQoQu3nE-Eo7_MZ-yZQbq30w=w72	accounts[1].htm0.2.dr	false		high
http://https://www.youtube.com/generate_204?cpn=	base[1].js.2.dr	false		high
http://https://www.gstatic.	Z2QQ58E8.js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://youtube.com/api/drm/fps?ek=uninitialized	base[1].js.2.dr	false		high
http://https://about.google/	privacy[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://schema.org/BreadcrumbList	2917834[1].htm.2.dr	false		high
http://https://www.google.co.uk/finance	so[2].htm.2.dr	false	• Avira URL Cloud: 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://policies.googl	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://maps.google.co.uk/maps?hl	so[1].htm.2.dr, so[2].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.co.uk/shopping?hl	so[1].htm.2.dr, so[2].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://schema.org/ListItem	2917834[1].htm.2.dr	false		high
http://https://www.youtube.com/watch?v=ZdEIZNg3epQ	ZdEIZNg3epQ[1].htm.2.dr	false		high
http://youtube.com/yt/2012/10/10	base[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/embed/48l-xdS4pXg?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pr	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://www.youtube.com/watch?v=ZdEIZNg3epQ	ZdEIZNg3epQ[1].htm.2.dr	false		high
http://https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history	2917834[1].htm.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.youtube.com/watch?v=48l-xdS4pXg	48l-xdS4pXg[1].htm.2.dr	false		high
http://https://support.google	{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/videoplayback	base[1].js.2.dr	false		high
http://https://kids.youtube.com/privacynotice	Z2QQ58E8.js.2.dr, privacy[1].htm.2.dr	false		high
http://https://client-channel.youtube.com/client-channel/client	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://www.youtube.com/?gl	so[1].htm.2.dr, so[2].htm.2.dr	false		high
http://https://www.blogger.com/	so[2].htm.2.dr	false		high
http://https://www.youtube.com/feed/history/search_history?utm_source=pp&hl=en_GB	privacy[1].htm.2.dr	false		high
http://www.youtube.com/watch?v=YlmVKT3Zvhw	YlmVKT3Zvhw[1].htm.2.dr	false		high
http://youtube.com/drm/2012/10/10	base[1].js.2.dr	false		high
http://https://accounts.youtube.com/accounts/CheckConnection?pmpo	ServiceLogin[1].htm.2.dr	false		high
http://https://readalong.google	Z2QQ58E8.js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/watch?v=YlmVKT3Zvhw	YlmVKT3Zvhw[1].htm.2.dr	false		high
http://https://staging-casespartner-pa-googleapis.sandbox.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://www.youtube.com/embed/48l-xdS4pXg?rel=0&showinfo=0&theme=light&version=3&hl=	privacy[1].htm.2.dr	false		high

Contacted IPs

Public

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

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324363
Start date:	29.11.2020
Start time:	17:07:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://plus.google.com/+InvorderingsbedrijfNl-Incasso/posts
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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/128@7/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://support.google.com/accounts?p=signin_privatebrowsing&hl=en-GB • Browsing link: https://support.google.com/accounts?hl=en-GB • Browsing link: https://accounts.google.com/TOS?loc=GB&hl=en-GB&privacy=true • Browsing link: https://accounts.google.com/TOS?loc=GB&hl=en-GB

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 104.83.120.32, 172.217.168.14, 172.217.168.45, 172.217.168.3, 172.217.168.68, 216.58.215.238, 172.217.168.46, 51.104.144.132, 172.217.168.78, 216.58.215.227, 216.58.215.234, 23.210.248.85, 172.217.168.10, 172.217.168.74, 152.199.19.161, 172.217.168.70, 2.20.142.210, 2.20.142.209, 51.103.5.159, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, arc.msn.com.nsatc.net, policies.google.com, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, e11290.dspg.akamaiedge.net, audownload.windowsupdate.nsatc.net, realtimesupport.clients6.google.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, plus.l.google.com, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, youtube-ui.l.google.com, www3.l.google.com, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, scone-pa.clients6.google.com, au.download.windowsupdate.com.edgesuite.net, support.google.com, ogs.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, plus.google.com, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, static-doubleclick-net.l.google.com, skypedataprdcoleus17.cloudapp.net, play.google.com, go.microsoft.com.edgekey.net, apis.google.com • Report size getting too big, too many NtDeviceIoControlFile calls found.

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\8P7RGF10\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	5.131843547454303
Encrypted:	false
SSDEEP:	96:WAXd4QC5teIeHIeIea5Iea5dIea5Iea5sIea5Iea5yIea5a:p
MD5:	3323F4AAE157345802493306ACAFCBC9
SHA1:	3298906DCD6558D24CF647FE7EB19D43E71F9BDA
SHA-256:	D704D6C578C9A493ABBB275F3124A6AD9077F93277A1772A2062E3DD4CC7271B
SHA-512:	03585B2A8B29CC5B3A6B2AF7F4AC25110C73DDC85484098C8B4EBEE4D79E2B23F83EA24C5BC3463C2703532F0235251D7435C1CE295490A1711929A5F85A4883
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="__sak" value="1" ltime="1512141456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1527621456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1543141456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1560301456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1574261456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1643581456" htime="30852789" /></root><root></root><root><item name="__sak" value="1" ltime="1654861456" htime="30852789" /></root><root></root><root><item name="yt-remote-device-id" value="{"data":"6dd4b24e-60a0-4fbf-b612-7cc1b97eda41","expiration":1638234546505,"creation":1606698546516}" ltime="1720101456" htime="30852789" /></root><root><item name="yt-remote-device-id" value="{"data":"6dd4b24e

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\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):	174
Entropy (8bit):	4.669955750681471
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsR0pqqUlB9uAGBJAqSSXSXoaK1ryRtFwsoIcDAqFf3uAGBJAqSSZ:JFK1rUFWcqa/ubBiSXMw1rUFxmAq93uP
MD5:	3A5EF90DC4D3F79F353DB8537BDED77C
SHA1:	946BB1574514533FA11E7E269DF9CB03E779781E
SHA-256:	73B293F3D0B0EF09F2AD8B10F84AE519F1F926F552A2C2C58B662334CC02D2A0
SHA-512:	63CAE284530BAD6D7CBFD18D413357BF36567BBE64452CD819B40609504756EE761C29684AACCB4FF24374BD4241FF8A203C2517C85FD11E39B2A571F6FF4BA
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__sak" value="1" ltime="1235551456" htime="30852789" /></root><root><item name="promo" value="{}" ltime="1235551456" htime="30852789" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\support.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4199
Entropy (8bit):	5.106758029708853
Encrypted:	false
SSDEEP:	96:D72W2S4z0LG72W2S4z0LG72W2S4z0LG7LG777a:1SzswSzswSzsAP
MD5:	534352C9AB4B1B13E2D926DC04BDB085

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\support.google[1].xml	
SHA1:	5186975856191636AA452F8D30B11413B298F947
SHA-256:	18CC1FC1CCBA22F2B1323F0485071D2D919B3D5815472C9DCB1F973E1B08A8A5
SHA-512:	403C55BCFA085B10B8F81295A66C57018BFCE5E1E36720EA7EBEABC1E33A945A2330175DA2DD122DB949D9B1EC6AE9C385C3D25DAAB61711D42F121820EED EF
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="refererViewId" value="1257488782" ltime="1406071456" htime="30852789" /></root><root><item na me="refererViewId" value="1257488782" ltime="1406071456" htime="30852789" /><item name="StatsDeferredClearcut" value="[["accounts","en- GB",[[55,[]]],[],[],null,null,[],null,null,null,"en",[["gg_split","accenture"]],1,17515,[],1,null,1,[],[10800235,10800244,10800253,1080 0284,10800286,10800300,10800352,10800403,10800436,10800559,10800112],null,null,"accounts",null,null,[],null,null,null,null,1,[[4,["2917834", 1257488782,1,[]],null,null,[1,35,8,"https://support.google.com/chrome/answer/2364824?"],[],[],null,0]],"637422629137283870-597027064",2,null ,null,false,null,null,"GB",[],1,null,22,3,null,null,1257488782,null,null,null,1,null,2,[]],"support.google.com"]" ltime="1406071456" htime="30852789" /> <item name="ScaledStatsDeferredClearcu

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{843B75DD-32A8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8560083829727145
Encrypted:	false
SSDEEP:	96:rgZ4Zd2Eg9WEutEdbfEfwHKMEL/qEClQEYxfEpw+6X:rgZ4Zd2n9WTtwfoRMhqHf2sX
MD5:	17173B7CB5E34C5246FA2A979A0AF404
SHA1:	7C70C9F1D8D7EE3FC0118993658365DA291D3BEC
SHA-256:	16DE42BD89C765C6BB3FD48F707277FCFB94209CF367ECC5A85E4487F54252D8
SHA-512:	6257CD233157B6BE34CE84024CB7DA4C9DE186A3B6750FCD004A26269479A0590140162CB6323CD3866765D9813A39CF7E34776E49C89B3FBC4044E668D4DC6
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\{843B75DF-32A8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	142998
Entropy (8bit):	3.033280317124735
Encrypted:	false
SSDEEP:	384:rAc5xWh8cUez91tC8dxAHNi8daAHmqF/vigaqgjRG2AiZPBe/ExeYKSzOfC3evrf:mY0xAHk0aAHaRG2AiDu0DYNl
MD5:	9ED6AB8475096CFDB25044DC4858D7BF
SHA1:	0ED6E59E94C0497BB0D4338A6FF65C4603C93F0B
SHA-256:	07F4F15F96BDFAC6748F93C88E9FCEDB343D8CECFD4406A6FDC726E6C95434AF
SHA-512:	F6210C0DD6956D855F7D229EC426E2C50D7773B17EF783512626728FE7593F563BCA19C2B9A810566ED5BB8EE4642F92F5ABB075ECF4F3187C4A7FA4CE43230
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\{8A40D23A-32A8-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5670837292654696
Encrypted:	false
SSDEEP:	48:IwFGcpr4GwpaxG4pQJGrapbS6oXrGQpKvG7HpRRsTGIpG:rbZgQj6pBS6oXFA+TR4A
MD5:	34CC4E87334970241C16EF021C4251ED
SHA1:	FABD288C00DE8DF0866A538A7EA9848D5A4B79C3
SHA-256:	C270D94130E0DD8413AF7D3E81A70B965BE0534834B2B424983DED30EB96B8B8
SHA-512:	AE2944B43488FE7CB034F09A964BD3CE3FD434F97F2F24543544D2BBB31DB54822D515DBB1B552B6656365F08E54644760A001DA245AA6D9C9B0C477CD5A64C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8A40D23A-32A8-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	11312
Entropy (8bit):	3.7474373628081197
Encrypted:	false
SSDEEP:	96:YvIJct+wP47v+rcqlBPG9lHvIJct+jH8HP47v+rcqlBPG9OH/:YvI6tpPqWceBPGzvI6tpPqWceBPGc
MD5:	2E327F3379613FAA717EE74F6504AB59
SHA1:	351380D824B1B7F4B35083AB03C8ECB2307B30FF
SHA-256:	E6AB896A1874B412799887C9AE793C3E33177307C4A2F7C5524E6DF8764FB09F
SHA-512:	D4C9072AB13A835F60C0F8365E37839EE244C7250EE8D02048ED01E367BD80207F2FF878E26FA462158740809EC5D25944D40D5E6BCA09166E7CD344FA71A8C1
Malicious:	false
Reputation:	low
Preview:	".h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... .....v.].X.:.X.:.r.Y.....q.X.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..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\02f8664b95445de6f27ba682f3c5f9ab[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4026
Entropy (8bit):	5.165425025048119
Encrypted:	false
SSDEEP:	96:+O2aTjjawLtBx0tdmK9YYlfBWX5oM4rLEa:DTj+wVeY0S4r7
MD5:	02F8664B95445DE6F27BA682F3C5F9AB
SHA1:	EFF0C42E5C642D81EF76995CE6B6C059CB38DCB6
SHA-256:	343B575C37BF08A1FDC972D0D86BCFAFF9C405DE625516C8656B60D37DCBA927
SHA-512:	2F58F0E0D46B9DE2F47CA8EC41B15E4B78A02EF9C7172B7C673CF85A3FD8D8870F00AF04C82768893A86B3F787B64464DF5613C801B6D85F1FC16A614F25CCF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/02f8664b95445de6f27ba682f3c5f9ab.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="108" y1="165" x2="180" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="242" y1="149" x2="284" y2="149" xlink:href="#linear-gradient"/>. <linearGradient id="linear-gradient-3" x1="34" y1="149" x2="76" y2="149" xlink:href=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\0d6da8d8c44e7e3ee95c4d56c19f04e1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2705
Entropy (8bit):	5.15375624281808
Encrypted:	false
SSDEEP:	48:+GzHx4GLZ/W1wHxJCXvGUQj+ek/Ij0jiO0ijy1uo:+G2UEJIj0jH0PH
MD5:	0D6DA8D8C44E7E3EE95C4D56C19F04E1
SHA1:	9DE1568D596F174CD4646DB5745B58695677B069
SHA-256:	FAA35DC181EB792DB0A4BE4E7031EEC86C044E52773CB082652B788D3B838E72
SHA-512:	D47689B9681F4D5DFF7FD18B4F76F9FBB372B4EB9ADC3FE7C177ED79D19CF2D912831729C73589C4DA833D3D83746DAD3C593A92A5A81440AAE17874F8DDC7C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/0d6da8d8c44e7e3ee95c4d56c19f04e1.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\0d6da8d8c44e7e3ee95c4d56c19f04e1[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linearGradient id="linear-gradient" x1="24" y1="77" x2="48" y2="77" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.116" stop-color="#9aa0a6" stop-opacity="0.054"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.201"/>. <stop offset="0.546" stop-color="#9aa0a6" stop-opacity="0.44"/>. <stop offset="0.823" stop-color="#9aa0a6" stop-opacity="0.768"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="48" y1="80" x2="48" y2="16" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#1967d2"/>. <stop offset="0.043" stop-color="#1967d2" stop-opacity="0.942"/>. <stop offset="0.305" stop-color="#1967d2" stop-opacity="0.611"/>. <stop offset="0.54" stop-color="#1967d2" sto

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2231879498-postmessagerelay[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9850
Entropy (8bit):	5.576810213157962
Encrypted:	false
SSDEEP:	192:vyewMuoQ7zSbvG1WoezWLZmiOezjM8qpCACPTvE3kKFo5uh7IezcvrR:vTwMuoQ7zSrG1VmKzjM8qXELwFKMUjR
MD5:	22FC1676BA30ECC84F2C80BE86436A1F
SHA1:	617A45C0149D4AD4450387E817AB1D7E107159DD
SHA-256:	D3C4D7BC0A3C613FC567C17277F187935F31EE7614783C463A3C1C3B042668C6
SHA-512:	6D7022852EE226B19954F15B7BAC8297C988F6628BB03C66CFB1F5FBA8FE53BF89B14C063F1A01341BCCE280AF24874DC1F48CC604F9EA1F5F658E78ADB34BD1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/accounts/o/2231879498-postmessagerelay.js
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,w=function(a,b){a=a.split(".");var c=l;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.o=b.prototype;a.prototype=new c;a.prototype.constructor=a;a.m=function(e,d,h){for(var p=Array(arguments.length-2),m=2;m<arguments.length;m++)p[m-2]=arguments[m];return b.prototype[d].apply(e,p)}};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\4PB7FJMT\2364824[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	738152
Entropy (8bit):	5.605864194354715
Encrypted:	false
SSDEEP:	12288:i9KiZ2IAALojYaiEzSCRyRmDoxqeT0XzJkiaV/nOSBc:i9KiZiwojYai2SCR8mDoxqeT0DBatnOt
MD5:	2B734897F61ECC59DB600AAF02AE3972
SHA1:	255E7D5199E97FB7EAFADDEF550BDBB4A98F82AF
SHA-256:	C01EFF6E08FF521ED01C98CAF0E14D9B58403F18C08D1F86C1D6988F78C5B1B3
SHA-512:	FF7F586978114E26A3D5C2CB25069C522A19B6BF4E952E2BCA6C7DEF394B085605F25E4519A64026DA26FD671A6B391FFEAE18539878474194E4838375500E02
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.google.com/chrome/answer/2364824?
Preview:	<!doctype html><html class="hcfe" data-page-type="ANSWER" lang="en-GB"><head><title>Share Chrome with others - Computer - Google Chrome Help</title><meta content="email=no" name="format-detection"><meta content="nofollow,noindex" name="robots"><meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible"><meta content="With profiles, you can keep all your Chrome info separate, like bookmarks, history, passwords and other settings.
Profiles are ideal for: Sharing a computer with multiple people. Keeping your d" name="description"><link href="https://support.google.com/chrome/answer/2364824?co=GENIE.Platform%3DDesktop&hl=en-GB" rel="canonical"><meta content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=no" name="viewport"><style>@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(https:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2951277d4c35389d7d304ed78d4fb6f6[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3437
Entropy (8bit):	5.159691776325374
Encrypted:	false
SSDEEP:	48:+GzHx4GLZ/W1wHxJCXvGUQoHxno+e//lj0jiO0ijy1uHldlzvgYx:+G2UCv0lj0jH0P+ldlzvgYx
MD5:	2951277D4C35389D7D304ED78D4FB6F6
SHA1:	936A9062B6E78E198BA1CD7ACDB42DEA29920890
SHA-256:	F3E55293686B1A4BCB8095896F8ADA506D3CE3E8BAD1DE89EAB56AFBEF3AD793
SHA-512:	8A9B5F0DAE9DFBD5C1FC7FCBEE51FD9A40302856C2F305FF0343DB2BA46D9C05B5F25A6F90AAE4AAFCEB6ACEFF7813157617773E2147954928B1E9227B58145
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2951277d4c35389d7d304ed78d4fb6f6[1].svg	
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/2951277d4c35389d7d304ed78d4fb6f6.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linearGradient id="linear-gradient" x1="24" y1="77" x2="48" y2="77" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.116" stop-color="#9aa0a6" stop-opacity="0.054"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.201"/>. <stop offset="0.546" stop-color="#9aa0a6" stop-opacity="0.44"/>. <stop offset="0.823" stop-color="#9aa0a6" stop-opacity="0.768"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="48" y1="80" x2="48" y2="16" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#1967d2"/>. <stop offset="0.043" stop-color="#1967d2" stop-opacity="0.942"/>. <stop offset="0.305" stop-color="#1967d2" stop-opacity="0.611"/>. <stop offset="0.54" stop-color="#1967d2" sto

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\3394102be0315326fd760e503b31c7b6[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1997
Entropy (8bit):	4.972761923159453
Encrypted:	false
SSDEEP:	48:+G0uMHxFi+eeunuGuQmDjuf3XU8MtUPFWl:+3vHxAr8Cn4tgWl
MD5:	3394102BE0315326FD760E503B31C7B6
SHA1:	8D80ABE58002CB8CF2A9C05EC5CE61F6A528AA6C
SHA-256:	FD266CACD5FD6FACBA81DEB7274AD226D7916B8883F23480A86F6F9C015913C8
SHA-512:	769DDC47AAA142961A8E00CDE3566DE62A6A6CA28D6EF568D5ECF67A0A5D8EF8806CF2428B653D58B9313E86161B6099D73362E6CEA6097D0B48DF4846253FE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/3394102be0315326fd760e503b31c7b6.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <clipPath id="clip-path">. <circle cx="48" cy="48" r="41" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient" x1="51" y1="78" x2="93" y2="78" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6"/>. <stop offset="1" stop-color="#9aa0a6" stop-opacity="0"/>. </linearGradient>. </defs>. <title>site_sec_C_01</title>. <g style="isolation: isolate">. <g id="Content">. <g>. <g>. <g>. <circle cx="48" cy="48" r="41" fill="#e8eaed"/>. <circle cx="48" cy="48" r="41" fill="none"/>. <circle cx="48" cy="48" r="41" fill="none"/>. <g clip-path="url(#clip-path)">. <path d="M89.981,22.441,67.05,68.843c-1.63,3.328-5.58,3.008-7.182-.581L51.8,50.168c-1.613-3.616-5.6-3.907-7.208-.526l-6.8,14.3C36.141,67.408,32.029,67,30.5,63.224L25.63

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\39b031d352a2e1586cf50ac7f2bbc18b[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	12378
Entropy (8bit):	5.041888208682257
Encrypted:	false
SSDEEP:	96:+RoMM2anrsHcxjBBN49qDLj5QeUFUDzi3pnDseedgejR7cestQoumbNvR4VBdwH6:PAHZ9q/j2eUqvi+/QNvOVBMwsV8
MD5:	39B031D352A2E1586CF50AC7F2BBC18B
SHA1:	5F714582443C158EAC42F4A2368E29488A01E365
SHA-256:	9EE03AE2943928AEA61E62DA6BD2338CA4B244C756D78B8888C1693731401A21
SHA-512:	44C3255DAC07BA0D8A5CA849649515A095AA40BAE13BF1710E009F8E9FFE96BF4EE573B073DC4340DE738CA110653FB48A83C5BE1008C61F3EB41A76FD741789
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/39b031d352a2e1586cf50ac7f2bbc18b.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="52" y1="49" x2="52" y2="71" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#202124"/>. <stop offset="1" stop-color="#202124" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="52" y1="85" x2="52" y2="157" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#188038"/>. <stop offset="1" stop-color="#188038" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-3" x1="24" y1="154" x2="44" y2="154" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\CheckConnection[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):	31707
Entropy (8bit):	5.430639129455834
Encrypted:	false
SSDEEP:	384:7a0Sdh/cVoe7/MwwqGCZXCLWhBw32WjlocfNwS585F/Lxks2+w9lhcAkkhK1n:7f4O/pwqHSKfw32+locf25F/KllWAkdn
MD5:	2ACBC257904CE62FA9CB6C541E5ADE8F
SHA1:	E5CBC4348E3A21B0F37E236A740CB1E2A56BA0E8
SHA-256:	1B92BF4CE03B99D2A57D21E77A819176A04F7107AC0D8003994280CFA4097060

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\CheckConnection[1].htm	
SHA-512:	5D9481C1FD26203C92F0E4CA7C30CF5BE369CE3339AFC07D6220C353D11F8B73EB60634F821B518EE35CD0426C4986736A5ED75D34AEBFF9C8631DCBCC33EE7
Malicious:	false
Reputation:	low
Preview:	<html><head><script nonce="uFNQY9dYHidT5HIRzLa1mw">"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){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ea="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},fa="function"==typeof Object.defineProperties?Object.defineProperty:functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	37B9B97549FE24A9390BA540BE065D7E5985E0FBFBE1636E894B224880E64203CB0DDE1213AC72D44EBC65CDC4F78B80BD7B952FF9951A349F7704631B903C63
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\4PB7FJMT\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
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$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..\|..\|..\|..\|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG. .....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o..&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\KFOmCnqEu92Fr1Mu4mxM[2].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0cIWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\KFOmCnqEu92Fr1Mu4mxM[2].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....O,.....P.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp.....glyf.....;Q..ID..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....hmtx..H....t.....Xdloca..KD.....BC%.maxp..M0... ... .(..name..MP.....t.U9.post..N ..... .m.dprep..N4.....l.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.*.....Q...JT.:Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9.....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S."j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Z2QQ58E8.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	444272
Entropy (8bit):	5.716369623284821
Encrypted:	false
SSDEEP:	6144:HuWciKTjMQo9fhQ0/sl+/91PzatJpCerDaYX:BP9fHTm1Nr/
MD5:	AD478083F2DEAC0E17C9D8914EB94A2A
SHA1:	17E070CE5BD24ADF3A4B8DAAF4388074E3ABDBAF
SHA-256:	F8D81F79F01AD79F5239BCC10A13AFE8C29242766F343CD15E8B458EAFD67210
SHA-512:	A616B5F5B0F4BAD1EC85ECFFC1BB72576CA425C8383CCB60119C53E068235238008DD900DD3DA6FBB64258C3727BE6AF481ABCBC09AA655A7A2305932570603
Malicious:	false
Reputation:	low
Preview:	"use strict";_F_installCss(".EDId0c{position:relative}.nhh4Ic{position:absolute;left:0;right:0;top:0;z-index:1;pointer-events:none}.nhh4Ic[data-state=\"snapping\"],.nhh4Ic[data-state=\"cancelled\"]{transition:transform 200ms}.MGUFnf{display:block;width:28px;height:28px;padding:15px;margin:0 auto;-ms-transform:scale(0.7);transform:scale(0.7);background-color:#fafafa;border:1px solid #e0e0e0;border-radius:50%;box-shadow:0 2px 2px 0 rgba(0,0,0,0.2);transition:opacity 400ms}.nhh4Ic[data-state=\"resting\"] .MGUFnf,.nhh4Ic[data-state=\"cooldown\"] .MGUFnf{-ms-transform:scale(0);transform:scale(0);transition:transform 150ms}.nhh4Ic .LLCa0e{stroke-width:3.6px;-ms-transform:translateZ(1px);transform:translateZ(1px)}.nhh4Ic[data-past-threshold=\"false\"] .LLCa0e{opacity:.3}.rOhAxb{fill:#4285f4;stroke:#4285f4}.A6UUqe{display:none;stroke-width:3px;width:28px;height:28px}.tbcVO{width:28px;height:28px}.bQ7oke{position:absolute;width:0;height:0;overflow:hidden}.A6UUqe.qs41qe{animation-name:quantumWiz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\b18d13e9ea8a362642b7d25bce665039[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	16764
Entropy (8bit):	5.015659059704473
Encrypted:	false
SSDEEP:	96:+7oy39iUOhxSoUhWBIBGNdByrJZeGyHObsjXDRKRpQ7wvkoln1WIGeDNc6ei52Ki:6vQ6JZoRKRa05Z9GImZAJgwEWZBYF
MD5:	B18D13E9EA8A362642B7D25BCE665039
SHA1:	928BE33E3ABE8071A068BE98084F406D5F4C07E2
SHA-256:	10F69DBA0842572682B65444464A1F8879BF29B201E730D5F824BB6636536555
SHA-512:	651CB5E1435A1E72392D425E73487413EF0A035574E84F738D775D29668CA7222AFA56C5AE77AB3A0AF15ECF94467C7070727EF10C0F38820545D5C81ABE2255

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\b18d13e9ea8a362642b7d25bce665039[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/b18d13e9ea8a362642b7d25bce665039.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="180" y1="77.807" x2="144.01" y2="77.807" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#1967d2"/>. <stop offset="0.133" stop-color="#1967d2" stop-opacity="0.98"/>. <stop offset="0.271" stop-color="#1967d2" stop-opacity="0.921"/>. <stop offset="0.411" stop-color="#1967d2" stop-opacity="0.822"/>. <stop offset="0.553" stop-color="#1967d2" stop-opacity="0.683"/>. <stop offset="0.696" stop-color="#1967d2" stop-opacity="0.505"/>. <stop offset="0.84" stop-color="#1967d2" stop-opacity="0.287"/>. <stop offset="0.983" stop-color="#1967d2" stop-opacity="0.033"/>. <stop offset="1" stop-color="#1967d2" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="191.997" y1="77.804" x2="168.003" y2="77.804" gradientUnits="userSpac

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	51236
Entropy (8bit):	5.5548258121036955
Encrypted:	false
SSDEEP:	1536:pIjKdByen4KOw9McPis5wfmYWpIaJtTY2O2s+oB:pxByen4mpIavY2O9B
MD5:	7ADDFAF8F1613468F3946F64B2CE9181
SHA1:	4426DE0E35D08C9D888902D60AAB85E290AE9783
SHA-256:	361B94A0601C90071F6B6AD5B28B603DB6218ED8442379765F551A076D4C070E
SHA-512:	0675EE14FFAB080375D985FF0FDE07CCBE2EB16690AB56BC4BF113EAD9E09B2387EF0B12C5F670CB44FD2C1C1553B45C95675BB21AF6E5407C086F8E18D303 5
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 ja,na,ta,xa,Ba,Da,Ia,Ra;_.ea=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ja=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};na="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};.ta=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");};xa=ta(this);Ba=function(a,b){if(b)a:{var c=xa;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&&na(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.157298093683682
Encrypted:	false
SSDEEP:	12:UJO6940FD7O6ZRoT6pYwEmr37uqF/iO6ZRoT6pixuGEqF/iO6ZN76pixuyvJY:G9XD7OYs/UrR/iOYsNxDv/iOYN7Nxw
MD5:	DC8AE9686BDE8C1517953AAF4C645E68
SHA1:	A95E59D8DDFECBE128C05B8C30E14688F135CA03
SHA-256:	AC7E61AF97048090E29FE6561A86B5FCD8F7BEF016C399D0C32683B02F059AD6
SHA-512:	5728E987376AE9209E44E677BACFE41F03FBC97B468D5BEE6F43D0CAE95B7F6AF7666DC05094B11C77F7BA72A2C963E4C4CB8C438F0B893B2D0A9C47DCB318 D6
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Product Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/productsans/v12/pxiDypQkot1TnFhsFMOfGShVF9eI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\e79ea0ed464fc8952d5b5582f9f9ae53[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	13232
Entropy (8bit):	5.004489515608496
Encrypted:	false
SSDEEP:	96:+9luEGZ2aRcZGDTBmQLBnEGRDzQeqzNOo4HFvdRX1ju6RGumD6k9i4AlkwNgFFro:HBBJQeq07fXDIumDf9lAuNgFFrpi
MD5:	E79EA0ED464FC8952D5B5582F9F9AE53
SHA1:	7C64CD9D283C3E87EC34160A70688A52D6144766
SHA-256:	FC432273DBD2B5233238B2BCA3E167CE7DD6BCB5318B3D06DC664ED15F309637
SHA-512:	3A5DE44AF0E40C6E226E4AACCE0BB7C9F78FE4DFB301B0FAB28586D7112456CC812F399DE163285CB6B79E1316DC87BF04ADA33A20AF9825417E33C122063A A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\e79ea0ed464fc8952d5b5582f9f9ae53[1].svg	
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/e79ea0ed464fc8952d5b5582f9f9ae53.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="-56.701" y1="323.063" x2="3.299" y2="323.063" gradientTransform="matrix(0, 1, -1, 0, 614.584, 137.96)" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#202124" stop-opacity="0"/>. <stop offset="0.023" stop-color="#202124" stop-opacity="0.079"/>. <stop offset="0.257" stop-color="#202124" stop-opacity="0.751"/>. <stop offset="0.4" stop-color="#202124"/>. <stop offset="0.615" stop-color="#202124" stop-opacity="0.751"/>. <stop offset="0.965" stop-color="#202124" stop-opacity="0.079"/>. <stop offset="1" stop-color="#202124" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="273.911" y1="117.637" x2="297.393" y2="102.387" gradientTransform="translate(333.87 -192.271) rotate(78)" gradientUnits="userSpaceOnUse">. <stop off

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0Jj6tZcUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/yts/jsbin/fetch-polyfill-vfl6MZH8P/fetch-polyfill.js
Preview:	/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining. a copy of this software and associated documentation fi les (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or s ell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the following 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. MERCHANTABILITY, 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, WHETH ER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\m=sy1a,sy1b,sy1c,sy1e,sy1f,sy34,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):	14951
Entropy (8bit):	5.5986908090144665
Encrypted:	false
SSDEEP:	384:zFwnMB7ztsU8aqdVRyCCoSDpQKx54rFswsMh:zFuM5ts6+Cfpn5OFspMh
MD5:	99665D5F1358CD7760E438668DBF1459
SHA1:	977AFEC5D45F27E876FC8E99D25F3CBC37A2B959
SHA-256:	EA50FD06F270387CD516C563C1218FD0A762FB1E1C59D4755BD5468A0A5AE199
SHA-512:	29A79C67776D9913641E774A0B4ECF8FE2BEFAE115007C1AE110E6C1231FD9E91C4D2637E3BAD93A718702FC5930DA368DB912DCA97E5BCB68338B0780AC2E 2
Malicious:	false
Reputation:	low
Preview:	this._G=this._G||{};(function(_){var window=this;.try{._.k("sy1a");._.zT=function(){return"Try another way"};._.AT=function(){return"Enter code"};..._.l();..}catch(e){_._Du mpException(e)}.try{._.k("sy1b");._.BT=function(){return(0,_.D)("Account recovery")};._.CT=function(){return"Verify that it's you"};..._.l();..}catch(e){_._DumpException(e) }.try{._.k("sy1c");._.Q4a=function(a){a=a||{};return _.P4a(a)};_.P4a=function(a){a=a||{};return _.Ws(a.Um,1)?"Enter your password":"Enter a password"};_.H("Ob","",0,funct ion(){return"Wrong password. Try again or click Forgot password to reset it."});_.H("Pb","",0,function(){return"Forgot password?"});..._.l();..}catch(e){_._DumpException(e)}.try{._.k("sy1e");._.DT=function(a,b){a=a.oa&&(a.oa.fa||a.oa);var c=b.locale;b="";var d=c=_.Xs(_.Vs("en,en-US,"),c+",");d&&(d=a.qb(),d=_.G(null==d?null:d.getG ivenName()));!d&&(d=!c)&&(d=a.qb(),d=_.G(null==d?null:d.Jc()));return b=d?b+(c?"Hi "+a.qb().getGivenName():""+a.qb().Jc()):b+"Welcome"};..._.l();..}catch(e){_._D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\m=wmlPKb[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	757
Entropy (8bit):	5.294473700964131
Encrypted:	false
SSDEEP:	12:kgEAgSyFPcEb8VEvt/iSZV/FKUSAKb6r2vcTcGCYjilir9kbRNeQ0:kAy5cs8udiSZtFKcS/qiir+rG
MD5:	51E522DF951BAC8B4F728CFE2B416ABB
SHA1:	86B2661DA13AD6696799E0556EAB68B494C5118F
SHA-256:	0BD3BD4A1244195931BC947FEDAC19D3A614673DC92D15EE7A9AB93A9A031E75
SHA-512:	BE6E45CDA3DE14E551EB57E43E109A27EDB2158D8E981FCE31AE616FD78A63ACB2AE3F80ECF58D295B563F075310436F0733C31A901CFDABC8C63F6E6307E7 33

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\m=wmlPKb[1].js	
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{._.m("wmlPKb");.var X1=function(a){_.V.call(this,a.ma);this.i=a.W.Sj;this.o=a.W.view;this.j=this.getData("trackerId").Qa(void 0)};_.w(X1,_.V);X1.T=function(){return{W:{Sj:_.U1,view:_.CK}}};X1.prototype.KF=function(){var a=this.i,b=this.o.getCurrentView().g.j,c=this.j,d=void 0,e=void 0;d=void 0===d?a.i.location.href:d;b=void 0===b?a.g.title:b;e=void 0===e?a.g.referrer:e;_.W1(a,"location",d,c);_.W1(a,"title",b,c);_.W1(a,"referrer",e,c);_.V1(a,"send",["pageview"],c)};_.W(X1.prototype,"wKZqRb",function(){return this.KF});._.NK(_.Jda,X1);.._.n();..}catch(e){_._DumpException(e)}.}).call(this,this.default_IdentityPoliciesUi);.// Google Inc..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	5.209319938570761
Encrypted:	false
SSDEEP:	12:haxyErYfhVkrC9sAkTulWEJU2XwP2TulMJmWmM8ytrI:haJspVkO9slTuI2PXwuTucaSI
MD5:	5D53322433805CAE55025FB267B292F0
SHA1:	B50AC49410B6B46CF967DFAC81DA2C7E7B3C8CA7
SHA-256:	AC6BF0E15F19FA6A33B915B23FF0FC6B70BDC3C490F20816014269FE570BCBC4
SHA-512:	278756383703F82A553CA54A97F8E5404A492081AF9ADAC23CD76A23A2020134BFB0162F518EBA5FE812F6C42CF9399C492EF707368CE4BCF8F88E69375BD670
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="yX6Z4b/n+vEf/dyAdkIK1A" src='https://ssl.gstatic.com/accounts/o/2231879498-postmessagerelay.js'></script></head><body ><script nonce="yX6Z4b/n+vEf/dyAdkIK1A" 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\4PB7FJMT\related_item_external_avatar[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 80 x 80, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2577
Entropy (8bit):	7.781446647389294
Encrypted:	false
SSDEEP:	48:hIClmS5juJIIPoy8mJgii5Je64GRWEcaGuFAHvUu3olwHCMtToF3PNxXPqoE:hIQj5jLlwXmJIasRXGhPywHo19P5E
MD5:	DBB859BB594B6AB827C4A148D9343720
SHA1:	BD7E94CCCAEB4B244E0D6A333450013F35FCC817
SHA-256:	679EC39C5CCB27D18357D6E23DE0DFA22D07ED435B09E85F7003FFC3870150D4
SHA-512:	9EA39C37EA3A6395B7E9CD63DA3BAAD1F2585B9BAB598D73B5FEBC7399B8532AC8FE57ED2E77537F9D7E689CE8CC289E20D29060023CD2AAD7ADFF4E03944C71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/content/images/static/related_item_external_avatar.png
Preview:	.PNG.....IHDR...P...P.....PLTE.....F.....?.....@..-..2..:..'.....4.....1..5..A.....*.....k..i..[....I.....*..(.....T..3..9....!.....}.....*.....%..... .t.....8..v..'..+.....k.....x.....S.....S.....E.....>..5.....A.....G..Y.....&.....".....@..%..... .....>.....(..`..:.....C..O..1..9.....s..M.....m.....?..V..2..a..e..j..&..$..:.....R..&.....4.....(.... .....B..9.....-..".-../.....E..\..2..*..7.....0.....<..l..<..!..... $..*.....D..5.....B.....;.f.....tRNS.@..f....IDATx..eTTi.....a...k.....6....(..H.2 .5...42.H.!.....H.....;.;qa.....y.J<..=..+....)cL@..a-..N..u.w....2..H}..q.....WD... <i.W.W_.}&5=...p..Q.....1.....|..T....4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\remote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93362
Entropy (8bit):	5.453537838405744
Encrypted:	false
SSDEEP:	1536:7ngfYk2BLQZtuqbJ2dKdWvaqfV7tfZjyH+N56/5JeaPwARYeDn18ngC0LH6n:y0BL2tBt2dKdWvakVZjyeN56/5JeaPwf
MD5:	7A643EB2BAD5AF5A41A7603AA54E2848
SHA1:	D98E79F7B44451FFB9DA1F5CEC062880FC6C1561
SHA-256:	F228B1A8A3137B796AA26BFE3D6E2D8B2209D9E85C69D8D8B18088A83A9FF41C
SHA-512:	D3A69B87FE75E5F90FA87D6EA8C1E197C41933AC43054BAE19FE4A57451531DD4BBEAE1502D9C0F2FD7A2E8F5B4430EFF2541158C43E482E34AA99FAD50E794
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/77da52cd/player_ias.vflset/en_GB/remote.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\remote[1].js	
Preview:	(function(g){var window=this;var zHa=function(a,b){return g.Tb(a,b)},Z5=function(a,b,c){a.C.set(b,c)},$5=function(a){Z5(a,"zx",Math.floor(2147483648*Math.random()).toString(36)+Math.abs(Math.floor(2147483648*Math.random())^g.A()).toString(36));.return a},a6=function(a,b,c){Array.isArray(c)||(c=[String(c)]);.g.Pm(a.C,b,c)},AHa=function(a,b){var c=[];.g.$i(b,function(d){try{var e=g.Dn.prototype.B.call(this,d,!0)}catch(f){if("Storage: Invalid value was encountered"==f)return;throw f;}void 0===e?c.push(d):g.Cn(e)&&c.push(d)},a);.return c},BHa=function(a,b){var c=AHa(a,b);.g.Fb(c,function(d){g.Dn.prototype.remove.call(this,d)},a)},CHa=function(a){if(a.be){if(a.be.locationOverrideToken)return{locationOverrideToken:a.be.locationOverrideToken};.if(null!=a.be.latitudeE7&&null!=a.be.longitudeE7)return{latitudeE7:a.be.latitudeE7,longitudeE7:a.be.longitudeE7}}return null},DHa=function(a,b){g.nb(a,b)||a.push(b)},b6=function(a){var b=0,c;.for(c in a)b++;return b},EHa=function(a,b){var c=b instanceof

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rs=AA2YrTur8uQVb0PS_fZQNu3wmpDiwcWuQQ[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	950
Entropy (8bit):	5.266722855579648
Encrypted:	false
SSDEEP:	24:+fqcbAOWx3VY2Fff0gqbNKONAHODYgq3YHUQ:+iVNFff0gI9NAuDYgtv
MD5:	B36D5F56DED69FCC03F607966E435893
SHA1:	0F61F717ACCE4CEDEE936CDAE0AD30AE2A5907CE
SHA-256:	17092AA427D02F06DDFABD57DCDD12F2F21EDAF382B926AED4E25529BE21DE9F
SHA-512:	4BA9C98BCDD208DE0B7B718CBFFB443EBB3A8E5EEBFCD46840EA05A4B1B063F76D57815AF678B74573A1FCBAF04301FB99C82C5BBEE19B39BA0EFA372CB308B3
Malicious:	false
Reputation:	low
Preview:	.gb_3e{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}.gb_Lc .gb_Hc{overflow:hidden}.gb_Lc .gb_Hc:hover{overflow-y:auto}.gb_6e.gb_7e{background:rgba(255,255,255,1);border:1px solid transparent;box-shadow:0 1px 1px 0 rgba(65,69,73,0.3),0 1px 3px 1px rgba(65,69,73,0.15)}.gb_6e.gb_7e .gb_qf{color:black;opacity:1}.gb_6e.gb_7e button svg{color:#5f6368;opacity:1}.gb_rf{background:#fff;border:1px solid transparent;border-radius:0 0 8px 8px;border-top:0;font:normal 16px Google Sans,Roboto,RobotoDraft,Helvetica,Arial,sans-serif;position:absolute;z-index:986;box-shadow:0 1px 1px 0 rgba(65,69,73,0.3),0 1px 3px 1px rgba(65,69,73,0.15)}.gb_sf{cursor:pointer;line-height:24px;padding:8px;padding-left:64px}.gb_tf{color:#999;font-weight:normal}.gb_uf{background-color:#f5f5f5}sentinel{}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	99949
Entropy (8bit):	5.563288450424643
Encrypted:	false
SSDEEP:	1536:2aCeBYGw2mpgkkbea/lEHvwUM0XIAjsQ+1+l3Tv3wXOd8Yg:fUkHEHTXIJ+l3Tv3wXj
MD5:	78F37DC1977920BE1804363059E1E5AD
SHA1:	74B3B601F084859FC5C15C31A739DB2D38E1CF53
SHA-256:	61CAB2B4FDBC9A1218FD03B881D6C96A606E911DB4ACB36E9EF38A007895DE5B
SHA-512:	B023278DCC521C1BF33312C4BD92CE04894383246C00D496A804FA80D86EF03BEC0667EE3F4EE69233E6EECC5DAF0D96AB11F82660CC647387ED1251180ADE4
Malicious:	false
Reputation:	low
Preview:	this.gbar_=this.gbar_||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Pj=function(a){switch(a){case 200:case 201:case 202:case 204:case 206:case 304:case 1223:return!0;default:return!1}};._.Qj=function(){};._.Qj.prototype.o=null;.var Sj;Sj=function(){};._.v(Sj,_.Qj);Sj.prototype.j=function(){var a=Tj(this);return a?new ActiveXObject(a):new XMLHttpRequest};Sj.prototype.B=function(){var a={};Tj(this)&&(a[0]=!0,a[1]=!0);return a};var Tj=function(a){if(!a.A&&"undefined"==typeof XMLHttpRequest&&"undefined"!=typeof ActiveXObject){for(var b=["MSXML2.XMLHTTP.6.0","MSXML2.XMLHTTP.3.0","MSXML2.XMLHTTP","Microsoft.XMLHTTP"],c=0;c<b.length;c++){var d=b[c];try{return new ActiveXObject(d),a.A=d}catch(e){}}throw Error("U");}return a.A};._.Rj=new Sj;..}catch(e){._.DumpException(e)}.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Uj=function(a,b,c){a.j||(a.j={});if(!a.j[c]){for(var d=_.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	95484
Entropy (8bit):	5.56707799490618
Encrypted:	false
SSDEEP:	1536:2aCeBYGw2mpgkkbea/lEHvwUM0XIHQ+1+l3Tv3wXOd8Yg:fUkHEHTXIT+l3Tv3wXj
MD5:	35DA1E5321FA1E99350E4133A5BF848F
SHA1:	B91458F25690923E968983E4078D1FC5870CBA50
SHA-256:	653A14AF74CAF5E019AF9FE3E211984A16727B75EE6CB0BEE5E3C36563BF77D3
SHA-512:	011B0F778F5D81928D0DC4AEC9045CA07C6C34518BA2B21A2F13D9A903D02DD9CB832D4F53BA650D7D58433D7E16D679F8F3A88F9DCDE908A7323C08A29794
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[2].js	
Preview:	this.gbar_=this.gbar_||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Pj=function(a){switch(a){case 200:case 201:case 202:case 204:case 206:case 304:case 1223:return!0;default:return!1}};._.Qj=function(){};_.Qj.prototype.o=null;.var Sj;Sj=function(){};_.v(Sj,_.Qj);Sj.prototype.j=function(){var a=Tj(this);return a?new ActiveXObject(a):new XMLHttpRequest};Sj.prototype.B=function(){var a={};Tj(this)&&(a[0]=!0,a[1]=!0);return a};var Tj=function(a){if(!a.A&&"undefined"==typeof XMLHttpRequest&&"undefined"!=typeof ActiveXObject){for(var b=["MSXML2.XMLHTTP.6.0","MSXML2.XMLHTTP.3.0","MSXML2.XMLHTTP","Microsoft.XMLHTTP"],c=0;c<b.length;c++){var d=b[c];try{return new ActiveXObject(d),a.A=d}catch(e){}}throw Error("U");}return a.A};._.Rj=new Sj;..}catch(e){._.DumpException(e)}.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Uj=function(a,b,c){a.j||(a.j={});if(!a.j[c]){for(var d=_.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\so[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):	47130
Entropy (8bit):	5.726247227015624
Encrypted:	false
SSDEEP:	768:t6l/d9SvRuFs3M0E0IfnoVajDIxwQPFJ/N4o5SmIgwE/n3d6q42O:e2MfnoEPIxb16gwE/nt6q42O
MD5:	5C5BA81EC7C2FBB97AAE9B1E49A9A451
SHA1:	12B02FB3AA0CEADF9933E1B8F1DA8F5CE26A1097
SHA-256:	C3CDCFEC198D7FAFCBFA0751A017A75F040729D83A2E1C0374EC72EDF7D28A62
SHA-512:	FD190A555B129E6085F98074789584B8865F4762591EBCB1886D6BCFEAA571131623E7CF2FF06226C9227C346E2FCBC3A1C3300B452B999E22FE4887E5BACCBD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/app/so?origin=https%3A%2F%2Fsupport.google.com&cn=app&pid=117&spid=117&hl=en
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/app/so"><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="sZxtQg8xt805XTJuhvCIyg">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"-8102981513115292771","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1606666117002403,173291011,1628103934]\n","ZwjLXe":117,"cfb2h":"boq_onegooglehttpserver_20201123.05_p1","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333,45695529],"gGcLoe":false,"ikfjnc":["https://support.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"One

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\unnamed[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 18 x 18, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	397
Entropy (8bit):	7.208563990444908
Encrypted:	false
SSDEEP:	6:6v/lhPi3WgsyAPLhn+55UhKJ2eCdyYQG1ggh86p2PMt0P1945CMMwyB+lVSDbnMJ:6v/7aDQExuVagh8ASPr4sMMwS+PSDb9M
MD5:	4F8DEB97A4E0BB33DDE438BD444B3DC5
SHA1:	4A3297F9364EEE666FF9F39C68177CFE355904BC
SHA-256:	7346FBB4B75591B361B8BDD30DE31BFD66DC4F704445EA43737E82D9FAAF6BCF
SHA-512:	76B5BF1B3D2742C2AC940EC20AD3035E1BB9641807141FAE5EE6D4C0B91AFDAE6B72F3BB51F707E4492B84E04D30E2528BD7CDC95CD68BF3E1D4BA82359BDCFE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/yl0EzS1GixeU9QVLJtHu7hom-4PIHwYylP17hRk9_UasgFCCc6lo6E0-ReGn8R1ny3A=w18-h18
Preview:	.PNG.....IHDR.....F.....sBIT..U.F....FIDAT(.u.MN.A....n.....0Q...`.....#.x.....'...\.....].....W.U..WmHg9f(].@..N.....}..nAQ@../t....}x.....{}.L...ofb....p....a..X.J.G.w6...1..u'.....|#..v..c{..1<..p..0..@."]M.....7E.f....&.VHf..()..gdd..p.r.....W8@..h...f.`..v.9d...N5.Ap=...d....'.h.....t.fb..6%[.F.! x...Ype....5..]8..@..p.".:SNZ.|,.|._...S}$.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\www-widgetapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101705
Entropy (8bit):	5.512775318887572
Encrypted:	false
SSDEEP:	1536:whWwsKea8H8pW8bXrvI9KRghWdixOhe0+N5239SMAaGv6hi2K:whB8cvPe129nGD
MD5:	0A9CD1BA386CFDDE02132DB7586E949C
SHA1:	FA8FB84BC9448C0FA2E7BD28F0E2F095FDCD2EB5
SHA-256:	4A99F96133F0B18CB2CD2CF95FD8CEEFD21CC214E3889B26ED2797A44754A547
SHA-512:	9327036E0349B6EAE41E399ACC5507F0FBB13B256518D2AB744B4CC85B70F1E8101F9939EE66B0E478F174398D341A18FB5D018F13ADD12EB987AD76F8870DA7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/77da52cd/www-widgetapi.vflset/www-widgetapi.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\www-widgetapi[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var r;function aa(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}}.var ba="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};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof glo bal&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}.var fa=ca(this);function t(a,b){if(b)a:{for(var c=fa,d=a.split("."),e=0;e<d.length-1;e++){var f=d[e];if(!(f in c))break a;c=c[f]}d=d[d.length-1];e=c[d];f=b(e);f!=e&&null!=f&&ba(c,d,{configurable:!0,writable:!0,value:f})}}.t("Sy mbol",function(a){function b(e){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c("jscomp_symbol_"+(e||"")+"_"+d++,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\02698a3383765bd3c250471c53a86c5a[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6789
Entropy (8bit):	4.942475749260986
Encrypted:	false
SSDEEP:	96:hHSTqdQTHkjKYk7MPEQDgJUf7qC7n+olFhT7n+olVJUf7NTehsY5:9cYk1NIRBHaTs
MD5:	02698A3383765BD3C250471C53A86C5A
SHA1:	CF1BB1E4F5DAE0C3BB0605B77565BDA2C12D75E5
SHA-256:	A1F675A555609FC86E744FA9D86B35F0924803C10D8D3DA2CA01D4171188552E
SHA-512:	BFF93C586263EEB0E70CF8FEE862DA65D5B28B5590685FAE05197F8F13C1567C3D8533C4C7E6C15620F8461B432E9A5EC223D98FE598A52030079375613484B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/02698a3383765bd3c250471c53a86c5a.svg
Preview:	<svg id="Content" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <clipPath id="clip-path">. <path d="M48,7A41,41,0,1,0,89,48,40.989,40.989,0,0,0,48,7Z" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient" x1="54.72" y1= "89.276" x2="92.089" y2="51.907" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#dfe1e5"/>. <stop offset="0.077" stop-color="#e9eaed"/>. <stop offset="0.227" stop-color="#f6f6f7"/>. <stop offset="0.426" stop-color="#fdfdfd"/>. <stop offset="0.875" stop-color="#fff"/>. </linearGradient>. <clipPath id="clip-path-2">. <rect x="53.811" y="50.998" width="39.187" height="39.187" rx="3.104" ry="3.104" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient-2 " x1="29.406" y1="65.093" x2="66.594" y2="27.905" xlink:href="#linear-gradient"/>. <clipPath id="clip-path-3">. <rect x="28.501" y="27" width=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\1fa3e4ce8ac456f39ed02a6f9eb49b14[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6422
Entropy (8bit):	5.145755305279271
Encrypted:	false
SSDEEP:	96:h2Cy4en2j0yQldta1TvQT6oj0cDGXTmg1t0UUIPLynG6+bRP14N/3UmXjMUz:y5cK9DiTFT0UUyynGAbjz
MD5:	1FA3E4CE8AC456F39ED02A6F9EB49B14
SHA1:	11E1FEC7C61FC6E168E47FA9C2316BA83B2A883F
SHA-256:	404919D82E7FCAF8F8B31573F9483B45482988CFD984F0463C9CFD322E58F08A
SHA-512:	3DD1B9136CFEB7C1FFF636C7B735CF18F1BFF2C80FC7426113BE2219C2BBCFEF3F37036DF8D8D2BDBE0EA7EE822FA0E9C7EFD45BFD328C7C8FD264ECC0C0 945
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/1fa3e4ce8ac456f39ed02a6f9eb49b14.svg
Preview:	<svg id="Content" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linear Gradient id="linear-gradient" x1="35.79" y1="10.115" x2="49.214" y2="10.115" gradientUnits="userSpaceOnUse">. <stop offset="0.001" stop-color="#23893c"/>. <stop offset="1" stop-color="#34a853"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="50.448" y1="27.536" x2="63.288" y2="19.416" gradientUnit s="userSpaceOnUse">. <stop offset="0" stop-color="#e09108"/>. <stop offset="0.021" stop-color="#e19308"/>. <stop offset="0.37" stop-color="#efa906"/>. <stop offset="0.703" stop-color="#f7b605"/>. <stop offset="1" stop-color="#fabb05"/>. </linearGradient>. <linearGradient id="linear-gradient-3" x1="37.583" y1 ="34.548" x2="53.68" y2="24.367" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#b7251d"/>. <stop offset="0.126" stop-color="#c32b21"/>. <st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\2917834[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	744609
Entropy (8bit):	5.612125622411195
Encrypted:	false
SSDEEP:	12288:a9KiZ2IAALojYaYpzSJDylxX3JXaT0f2LkiaV/nikkS64:a9KiZiwojYaYZSJDyXX3JXaT0u/atniA
MD5:	960E8D248C62D2134DC0EFC238DDDFA9
SHA1:	BFA733F3FFB512F10B1DF3DF358E66BD90F05AAC
SHA-256:	D99CD76EA881927E9DA142CCC1AF827CBC370B0AA7E37855980F5599C2028793
SHA-512:	0850C8D839D1336C76936D00A06044566E8D84C6C0BD358764B1AD01B4A5836B1F4243F374336F323DDDB741B09647AC2149DFA5BF9F985A168E6C6DD19FDFC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\2917834[1].htm	
IE Cache URL:	http://https://support.google.com/accounts/answer/2917834?visit_id=637422629137283870-597027064&p=signin_privatebrowsing&hl=en-GB&rd=1
Preview:	<!doctype html><html class="hcfe" data-page-type="ANSWER" lang="en"><head><title>Sign in on a device that's not yours - Computer - Google Account Help</title><meta content="email=no" name="format-detection"><meta content="nofollow,noindex" name="robots"><meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible"><meta content="If you sign in temporarily on a computer, phone, or tablet that doesn't belong to you, use a private browsing window.
For example: A public computer that's available to lots of people, like at a" name="description"><link href="https://support.google.com/accounts/answer/2917834?co=GENIE.Platform%3DDesktop&hl=en" rel="canonical"><meta content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=no" name="viewport"><style>@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	775404B50D295DBD9ABC85EDBD43AED4057EF3CF6DFCCA50734B8C4FA2FD05B85CF9E5D6DEB01D0D1F4F1053D80D4200CBCB8247C8B24ACD60DEBF3D739A 4CF0
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\B87Z87FM\4f19891c43001db11efc8048f9bc7cdb[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2184
Entropy (8bit):	5.006709078848764
Encrypted:	false
SSDEEP:	24:t4Lu3K0HxEGSGjGeGxGE+ePCgXP/jN4J9ZQu5x/MTFJv3/ufn7d79C7RudPfdjrf:+GnHx16ZAE+eV/iUZt/iPFGsXJ2kx
MD5:	4F19891C43001DB11EFC8048F9BC7CDB
SHA1:	FB001AFC35E6B79D7771DD3893102C14718A58CD
SHA-256:	4F0D0BECD3F8A0496FA98581492B85F53AAFDF0CD51E5626B5FD0B6AB2DB9379
SHA-512:	A59528BAB7A538E4F221BCA27440EB88C873950D1595AA7718FF9613D7CE14CE40CBD29D209B0BCC3C8029360E2BC3740AB723802492E75D13C91A153D7DF45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/4f19891c43001db11efc8048f9bc7cdb.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linearGradient id="linear-gradient" x1="48" y1="71" x2="48" y2="33" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#5f6368"/>. <stop offset="0.232" stop-color="#5f6368" stop-opacity="0.699"/>. <stop offset="0.568" stop-color="#5f6368" stop-opacity="0.32"/>. <stop offset="0.836" stop-color="#5f6368" stop-opacity="0.086"/>. <stop offset="1" stop-color="#5f6368" stop-opacity="0"/>. </linearGradient>. </defs>. <title>site_sec_C_08</title>. <g style="isolation: isolate">. <g id="Content">. <g>. <path d="M48,7A41,41,0,1,0,89,48,40.989,40.989,0,0,0,48,7Z" fill="#e8eaed"/>. <g>. <path d="M16,33H80a0,0,0,0,1,0,0V68a3,3,0,0,1-3,3H19a3,3,0,0,1-3-3V33A0,0,0,0,1,16,33Z" fill="#fff"/>. <path d="M77,71H19a3,3,0,0,1-3-3V33H80V68A3,3,0,0,1,77,71Z" opacity="0.3" fill="url(#linear-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5959e84c2197c8a27da0a717f1cd47d5[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1812
Entropy (8bit):	5.137605121069892
Encrypted:	false
SSDEEP:	24:tDLu3OP/je+R5kHxEG5GCGoGBG8+eiCfP/jNQJQce+vlUDlnlUD5/z6jERC6TlYd:hGO/pWHxYFbw8+er/BIRz6w7rT+
MD5:	5959E84C2197C8A27DA0A717F1CD47D5
SHA1:	717BD4592135C09EF42DE6767EA4C2D7FE844C1D
SHA-256:	EC86659A0D1607B58CF5E3ED06414FA776ED65BC97F9F6B7BDF184EF2D607973
SHA-512:	F1D0CB152D197415D55DB3D274941E100257A40453379BF4502CB6AA6C0218D5D5BA29C417B6D3AD925B331248A16AA5B141B0E2541AD4876088FEADDE49DE1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5959e84c2197c8a27da0a717f1cd47d5[1].svg	
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/5959e84c2197c8a27da0a717f1cd47d5.svg
Preview:	<svg id="Content" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <clipPath id="clip-path">. <path d="M48,7A41,41,0,1,0,89,48,40.989,40.989,0,0,0,48,7Z" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient" x1="29.091" y1="71.218" x2="66.018" y2="34.291" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#2c66bf"/>. <stop offset="0.201" stop-color="#3572d4"/>. <stop offset="0.446" stop-color="#3c7de6"/>. <stop offset="0.704" stop-color="#4183f1"/>. <stop offset="1" stop-color="#4285f4"/>. </linearGradient>. </defs>. <title>site_sec_C_09</title>. <g>. <g>. <path d="M48,7A41,41,0,1,0,89,48,40.989,40.989,0,0,0,48,7Z" fill="#e8eaed"/>. <g clip-path="url(#clip-path)">. <path d="M35.543,42.584a10.048,10.048,0,1,0-2.421-19.789,12.572,12.572,0,0,0-22.647,4.788,7.546,7.546,0,0,0,.992,15Z" fill="#fff"/>. </g>. <g>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5e7cd445f8861a262a3da876f855a4cc[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1068
Entropy (8bit):	5.114357448467999
Encrypted:	false
SSDEEP:	24:tDLu30ureO+exC/urN9uraurz9dde61Lj1uj+FhlHcsuUCZXHcmD0HWi4I:hG0uN+eOuvuGu4mDjuf3fi
MD5:	5E7CD445F8861A262A3DA876F855A4CC
SHA1:	B0CBB7191D67F8553B3292D5B721710F1C3994E5
SHA-256:	3F4E4B6EDE035C2ACD2917EEE9DB73B3FB4774179D03762E25C945F48C197979
SHA-512:	742E9F9D2AE39DAEFECE21516E1EEDAA4B7F531EB86801D8FE44904B49156ADC3B2B5854C519AD6AD92F9DB2FBA3431ECE3B03B8986C2A725573565D291C6954
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/5e7cd445f8861a262a3da876f855a4cc.svg
Preview:	<svg id="Content" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <clipPath id="clip-path">. <circle cx="48" cy="48" r="41" fill="none"/>. </clipPath>. </defs>. <title>site_sec_C_06</title>. <g>. <g>. <circle cx="48" cy="48" r="41" fill="#e8eaed"/>. <circle cx="48" cy="48" r="41" fill="none"/>. <circle cx="48" cy="48" r="41" fill="none"/>. <g clip-path="url(#clip-path)">. <path d="M89.981,22.441,67.05,68.843c-1.63,3.328-5.58,3.008-7.182-.581L51.8,50.168c-1.613-3.616-5.6-3.907-7.208-.526l-6.8,14.3C36.141,67.408,32.029,67,30.5,63.224L25.637,50.7a4.25,4.25,0,0,0-7.675-.708l-9.3,15.345" fill="none" stroke="#fbbc04" stroke-linecap="round" stroke-miterlimit="10" stroke-width="6"/>. </g>. <circle cx="48" cy="47.981" r="11.526" fill="#fff" stroke="#34a853" stroke-miterlimit="10" stroke-width="6"/>. <circle cx="87.5" cy="27.5" r="8.5" fill="#fbbc04"/>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	57D3D4DE3816307ED954B796C13BFA34AF22A46A2FEA310DF90E966301350AE8ADAC62BCD2ABF7D7768E6BDCBB3DFC5069378A728436173D07ABFA483C1025AC
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=..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\B87Z87FM\ServiceLogin[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	1525475
Entropy (8bit):	5.821912044792781
Encrypted:	false
SSDEEP:	12288:E23RkYpvasjTm+LlTxK6B2QzEkgmN08DR1Ve6CzO+F1gFjPNIKIG0FfQMCBVJ:ZfvasjTm+T/B2uEK+b1gVNIKKQM2J
MD5:	E31A75CFC36DABEF4D59F6E8157016C6
SHA1:	B71B017E94A1A2B2BC5A3AD288EE1E555B265F8F
SHA-256:	6D5DA3B652EA763485EFC91E2D3836F56979B55928469EE4EAEB782194FC4EF1
SHA-512:	C7DE516C2A19325B4E09E2B649B448907369B102BDCCB97DCE41A9A48F03EF5AE8685E819527A2AF02BB1E6C4B5D9314E8F25D764FEF9FC49505548426F60E1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ServiceLogin[1].htm	
Preview:	<!doctype html><html lang="en-GB" dir="ltr"><head><base href="https://accounts.google.com/"><script data-id="_gd" nonce="kLfgpUdryxuqBACdvnFuqg">windo w.WIZ_global_data = {"Mo6CHc":5587774787723431857,"OewCAd":"%.@.\"xsrf\",null,[\"\"]\n,\"AFoagUWhlxPFPGnsFzPacnIbY2rClYeClA:1606666094865\"]\n","Qzxix c":"S-553236310:1606666094846304","thykhd":"AKH95esgffh0sse3ZlTJcEqzMRTDhIowh_S0v5_mfdhcgYInrna93qNncVXNpjlnJ5MFgcN74fPigP2IlHFCLV0rAbabjnEG c3l8xySOIAUI1p-Vh9IFSFE\u003d","w2btAe":"%.@.null,null,\"\",false,null,null,true,false]\n"};</script><meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" c ontent="IE=edge"/><link rel="shortcut icon" href="//www.google.com/favicon.ico"/><noscript><meta http-equiv="refresh" content="0; url=https://accounts.google.co m/ServiceLogin?continue=https%3A%2F%2Fplus.google.com%2F%2BInvorderingsbedrijfNl-Incasso%2Fposts&rip=1&nojavascript=1&followup=h ttps%3A%2F%2Fplus.google.com%2F%2BInvorderingsbedrijfNl-Incasso%2Fposts&osid=1"><style nonce="kL

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\accounts[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	723823
Entropy (8bit):	5.616969573384635
Encrypted:	false
SSDEEP:	12288:p9KiZ2lAALojYaYIrAkxK00jtT0TlakiaV/nD:p9KiZiwojYaYSAkxK00jtT0R8atnD
MD5:	51E2AA7DAB5ED3CEAD5761A5A04DC8F3
SHA1:	57862BA5A24AECD87E9F09202A5AFA50AF349772
SHA-256:	206974AB524F6CB75AE5CD824A7937D89274CC73B349B796FEC692A782DCA66A
SHA-512:	6CF9B0D95952370BE1F4C6A5AC420040B0AFDF5EEF77795C23C0FFC9C1B1F87F24E0418D9BF2EB1196C3056BFFFD0798EB1CE5B68BAA3DF9D08895BCFE2C38 B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.google.com/accounts?hl=en-GB
Preview:	<!doctype html><html class="hcfe" data-page-type="HOMEPAGE" lang="en"><head><title>Google Account Help</title><meta content="email=no" name="format-de tection"><meta content="nofollow,noindex" name="robots"><meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible"><meta content="Official Google Account Help Center where you can find tips and tutorials on using Google Account and other answers to frequently asked questions." name="description"><link href="https:// support.google.com/accounts/?hl=en" rel="canonical"><meta content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=no" name="viewport"><style>@ font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-we

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ad_status[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	29
Entropy (8bit):	4.142295219190901
Encrypted:	false
SSDEEP:	3:lZOwFQvn:lQw6n
MD5:	1FA71744DB23D0F8DF9CCE6719DEFCB7
SHA1:	E4BE9B7136697942A036F97CF26EBAF703AD2067
SHA-256:	EED0DC1FDB5D97ED188AE16FD5E1024A5BB744AF47340346BE2146300A6C54B9
SHA-512:	17FA262901B608368EB4B70910DA67E1F11B9CFB2C9DC81844F55BEE1DB3EC11F704D81AB20F2DDA973378F9C0DF56EAAD8111F34B92E4161A4D194BA902F82 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.doubleclick.net/instream/ad_status.js
Preview:	window.google_ad_status = 1;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\c1b97d74dace7e43a9ccb26841a7cae4[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6217
Entropy (8bit):	5.12197916092655
Encrypted:	false
SSDEEP:	96:hmpCgaDaIvQiJgZMDRzvrphOqqzfHm0TCgGT908uB75T:xPuB75T
MD5:	C1B97D74DACE7E43A9CCB26841A7CAE4
SHA1:	83F78C8D77BF9499B7E839345BB94C22A89616AF
SHA-256:	D9DE9633583A448CAD1268D42FFDF48D0B3C60D2693600B843A7EBE43AD06908
SHA-512:	B3986AF15A3FFB3AB35B8E3C120BC9BA8BECD5892CB7C1DE0BA5AD08A83499ACEC288B20708EE834EA43BFE446FD01ADA8CA55E0893EEBE766241913DB11 A88B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/c1b97d74dace7e43a9ccb26841a7cae4.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\c1b97d74dace7e43a9ccb26841a7cae4[1].svg	
Preview:	<svg id="Content" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linear Gradient id="linear-gradient" x1="41.178" y1="24.308" x2="41.368" y2="32.801" gradientUnits="userSpaceOnUse">. <stop offset="0.004" stop-color="#cdd0d5"/>. <stop offset="0.466" stop-color="#b1b6bd"/>. <stop offset="1" stop-color="#959ca5"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="29.696" y1="67.461" x2="68.387" y2="28.77" gradientUnits="userSpaceOnUse">. <stop offset="0.001" stop-color="#fff"/>. <stop offset="0.131" stop-color="#fff"/>. <stop offset="1" stop-color="#fff"/>. </linearGradient>. <clipPath id="clip-path">. <circle cx="27.84" cy="50.69" r="6.427" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient-3" x1="50.224" y1="35.554" x2="50.224" y2="31.004" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#cdd0d5"/>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\chatsupport[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7496
Entropy (8bit):	5.247731309135412
Encrypted:	false
SSDEEP:	96:jjSPR3tg31YeVJWPgzgxgwg/uR9PwB8YxGjwz3t+GbvFuEq6HnLnJnRLD72aaTgg:jJ31YSGwcref8Yxwyq6HLJRLDyaakGF
MD5:	54E924FF5BF53BB74BDEF08087DF83A6
SHA1:	64261E657658AE9C7E8D82BFDD9F4335FB80FB6E
SHA-256:	97CE0FB0CB0CA5299FB77E2B07388C1FCA7FCF3DFA13DF083E3A9DB88F1C44B1
SHA-512:	AB704C4C0F09166140216A4E90CB44F2AC6B1A95EF635EA6BA8CADC0FBB1ECD0B413C6B2C11686A2B96FFAD5E638A8E59650EB67108B1D2ACB18690196744B7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/realtime/operator/1605690075554/chatsupport.css
Preview:	#topSection{width:100%;height:4px;overflow:hidden}#bottomSection{width:100%;height:calc(100% - 4px);overflow:hidden;box-shadow:0px 1px 2px 0px rgba(60,64,67,.30),0px 2px 6px 2px rgba(60,64,67,.15)}.chatsupport_a{width:12px;height:100%}.chatsupport_b{width:calc(100% - 24px);height:100%}.chatsupport_c{width:4px;height:100%}.chatsupport_d{width:calc(100% - 8px);height:100%;box-shadow:0px 0px 5px #888}.chatsupport_e{width:100%;height:8px}.chatsupport_f{width:100%;height:calc(100% - 8px)}.chatsupport_g{overflow:hidden;display:block;z-index:10000001;bottom:0px;position:fixed}.chatsupport_h{width:100%;height:100%;background:none;vertical-align:bottom;visibility:visible;opacity:1}.chatsupport_i{display:inline-block;vertical-align:top}.chatsupport_j-k.chatsupport_l-k{box-sizing:content-box;font-family:Arial,sans-serif;font-size:13px;position:fixed;width:400px;z-index:10000001}.chatsupport_m .chatsupport_n{cursor:n-resize}.chatsupport_o .chatsupport_n{cursor:n-resize}.chatsupport_m .chatsupport_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.157298093683682
Encrypted:	false
SSDEEP:	12:UJO6940FD7O6ZRoT6pYwEmr37uqF/iO6ZRoT6pixuGEqF/iO6ZN76pixuyvJY:G9XD7OYs/UrR/iOYsNxDv/iOYN7Nxw
MD5:	DC8AE9686BDE8C1517953AAF4C645E68
SHA1:	A95E59D8DDFECBE128C05B8C30E14688F135CA03
SHA-256:	AC7E61AF97048090E29FE6561A86B5FCD8F7BEF016C399D0C32683B02F059AD6
SHA-512:	5728E987376AE9209E44E677BACFE41F03FBC97B468D5BEE6F43D0CAE95B7F6AF7666DC05094B11C77F7BA72A2C963E4C4CB8C438F0B893B2D0A9C47DCB318D6
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Product Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/productsans/v12/pxiDypQkot1TnFhsFMOfGShVF9eI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\e28714c71f217892f72b2698ea5cefef[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4134
Entropy (8bit):	5.054285765130248
Encrypted:	false
SSDEEP:	48:+GOHx16ZAvHxDg+eJ/eux4tBeLDNdBeLSlBeLLpZdrzTPr+UkVr3H2c:+r1XSDQBe7BeeBeBeUkl2c
MD5:	E28714C71F217892F72B2698EA5CEFEF
SHA1:	E4257063DB9DF43DCDE90920CC3F34978BAEA51D
SHA-256:	65845E7CECBF4E88691BFF290F72B427B70887E23879F523BBC5B2B032C7609F
SHA-512:	C693B70D3EDCB32DAEA8BEC867BDF34AC2ED491F9CBC4A57A5433F462DC6EF2D0F01A0C17D7DFD457064D13D45207659ABF116B09191DFDDF38E706FC72A5BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/e28714c71f217892f72b2698ea5cefef.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\e28714c71f217892f72b2698ea5cefef[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <linearGradient id="linear-gradient" x1="48" y1="71" x2="48" y2="25" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#5f6368"/>. <stop offset="0.232" stop-color="#5f6368" stop-opacity="0.699"/>. <stop offset="0.568" stop-color="#5f6368" stop-opacity="0.32"/>. <stop offset="0.836" stop-color="#5f6368" stop-opacity="0.086"/>. <stop offset="1" stop-color="#5f6368" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="76" y1="48" x2="86" y2="48" gradientTransform="translate(129 -33) rotate(90)" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#f29900"/>. <stop offset="1" stop-color="#f29900" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-3" x1="76" y1="15" x2="86" y2="15" gradientTransform="matrix(1, 0, 0, 1, 0, 0)" xlink:hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\e60586c0029adec0bacd3e48470ca6c6[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	15934
Entropy (8bit):	5.044031692686615
Encrypted:	false
SSDEEP:	96:+5rsHBQMyBNWB85GfnAWlkVzLIV2amGj31zBJqDb5PiStUseyXDhMln9UTfQLUQo:LHEQmGb1wgWX1CGkbjf+LJnx
MD5:	E60586C0029ADEC0BACD3E48470CA6C6
SHA1:	2660A543EDC31CC35115F37CFF36CC4DA7B95151
SHA-256:	DA83F15D25A23E295CBA8AF285B22F5AEB46394C6B13DFCD29EA3B6415F90DF7
SHA-512:	2FA00B15E609C22D343901BE202D66ED071A5E9989827DE3F3E486DBC33D62CDA296B66BB30875A905AA3BCC97A068F5ECA62FBD4B10EE5CC60CE2C0AFF37A00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/e60586c0029adec0bacd3e48470ca6c6.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="264" y1="165" x2="328" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6" stop-opacity="0"/>. <stop offset="0.137" stop-color="#bdc1c6" stop-opacity="0.021"/>. <stop offset="0.279" stop-color="#bdc1c6" stop-opacity="0.084"/>. <stop offset="0.424" stop-color="#bdc1c6" stop-opacity="0.189"/>. <stop offset="0.57" stop-color="#bdc1c6" stop-opacity="0.336"/>. <stop offset="0.718" stop-color="#bdc1c6" stop-opacity="0.525"/>. <stop offset="0.864" stop-color="#bdc1c6" stop-opacity="0.753"/>. <stop offset="1" stop-color="#bdc1c6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="175" x2="199" xlink:href="#linear-gradient"/>. <linearGradient id="linear-gradient-3" x1="196" y1="165" x2="252" y2="165" gradientUnits="userSpac

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30248
Entropy (8bit):	5.555327948787822
Encrypted:	false
SSDEEP:	384:2unuG5N+YRgyq+e8bwIr9+eXBryHa35srGmp36vZC9cvjxrhou5CaYIZLr4ze2/B:Pw+1bwIUekO5sSekCe1YSBvk+xH0
MD5:	90332216C0CC7547013609075E4DE0F0
SHA1:	87970E4CD6976A2C8D205DD3E9A2A5537CFD1018
SHA-256:	D9D774312422F4FEA1DA6F05BABB7D328AB47C5262B36CFBBD7D75087F5F4F18
SHA-512:	ADC303F943BC4BFB9DE1F334150D731BA864AA7CABD1477967001B89EB95312E2EEBE49BF783DF45E0FDD2EBCFBF124AE51472D83F58C70717E7B3D880E2FA58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/77da52cd/player_ias.vflset/en_GB/embed.js
Preview:	(function(g){var window=this;var w4=function(a,b){g.jf(a.u,8*b+2);var c=a.u.end();a.C.push(c);a.B+=c.length;c.push(a.B);return c},x4=function(a,b){var c=b.pop();.for(c=a.B+a.u.length()-c;127<c;)b.push(c&127|128),c>>>=7,a.B++;b.push(c);a.B++},fGa=function(a,b,c){null!=c&&(g.jf(a.u,8*b+1),a=a.u,b=c>>>0,c=Math.floor((c-b)/4294967296)>>>0,g.wf=b,g.xf=c,g.kf(a,g.wf),g.kf(a,g.xf))},y4=function(a,b,c){null!=c&&(g.jf(a.u,8*b),a.u.u.push(c?1:0))},z4=function(a,b,c){if(null!=c){b=w4(a,b);.for(var d=a.u,e=0;e<c.length;e++){var f=c.charCodeAt(e);if(128>f)d.u.push(f);else if(2048>f)d.u.push(f>>6|192),d.u.push(f&63|128);else if(65536>f)if(55296<=f&&56319>=f&&e+1<c.length){var h=c.charCodeAt(e+1);56320<=h&&57343>=h&&(f=1024*(f-55296)+h-56320+65536,d.u.push(f>>18|240),d.u.push(f>>12&63|128),d.u.push(f>>6&63|128),d.u.push(f&63|128),e++)}else d.u.push(f>>12|224),d.u.push(f>>6&63|128),d.u.push(f&63|128)}x4(a,b)}},A4=function(a,b,c,d){null!=c&&(b=w4(a,b),d(c,a),x4(a,b))},B4=function(a,b,c,d){if(null!=.c)f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fb61fc4bfc85ad86f11342e699d685e9[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	13663
Entropy (8bit):	4.850378997553469
Encrypted:	false
SSDEEP:	96:+y2aZrsHBAPC0GDy8gUFnD0alywjj/+TjD66Nt1ygnCL1YsrHwITnrU2TJbIrbon:baH/WMJYaNUyXNIr0n
MD5:	FB61FC4BFC85AD86F11342E699D685E9
SHA1:	5EA7B864D6A727F9A7CF5023BB556CC221564FEF
SHA-256:	92C06932C12A74573114DB6FEAA94C43A980FB7B5DC0014A1AEF32F8C222F849
SHA-512:	DD782F29B937B2CB6365C758B246D020BA5B718C797E5208EA0401EE3B599C77826219CE5612F137BADC34F97D59C80A427965F455A56829BEA790D2E756E605
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fb61fc4bfc85ad86f11342e699d685e9[1].svg	
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/fb61fc4bfc85ad86f11342e699d685e9.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="12" y1="143" x2="32" y2="143" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="72" y1="165" x2="144" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6" stop-opacity="0"/>. <stop offset="0.137" s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iframe_api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	810
Entropy (8bit):	5.292728819504826
Encrypted:	false
SSDEEP:	24:E1bWYtpqAK/HJ2TAXC5vuHM8aJLtdRWZ4FhQ:E1bdPcSAXC5kaJLzwYhQ
MD5:	63D19659F78F51528041883187A85557
SHA1:	A3F9D40D962F95785972B24470C232BAE96A44A2
SHA-256:	215215E7C7284D3529A3A4D0CB7B70BDB3B5767DDD7C8D652D292DE64B9433D7
SHA-512:	C7CDA1709358288E9624A658189848BA3DEC6AC42A3841AC101674CA143AE6D1D087455CADDEAE2F3965D614F9DE103DA43F9CCE4C643FB4D6AE2C87A1FC910
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/iframe_api
Preview:	var scriptUrl = 'https:\/\/www.youtube.com\/s\/player\/77da52cd\/www-widgetapi.vflset\/www-widgetapi.js';if(!window["YT"])var YT={loading:0,loaded:0};if(!window["YTConfig"])var YTConfig={"host":"https://www.youtube.com"};.if(!YT.loading){YT.loading=1;(function(){var l=[];YT.ready=function(f){if(YT.loaded)f();else l.push(f)};window.onYTReady=function(){YT.loaded=1;for(var i=0;i<l.length;i++)try{l[i]()}catch(e){}};YT.setConfig=function(c){for(var k in c)if(c.hasOwnProperty(k))YTConfig[k]=c[k]};var a=document.createElement("script");a.type="text/javascript";a.id="www-widgetapi-script";a.src=scriptUrl;a.async=true;var c=document.currentScript;if(c){var n=c.nonce||c.getAttribute("nonce");if(n)a.setAttribute("nonce",n)}var b=.document.getElementsByTagName("script")[0];b.parentNode.insertBefore(a,b)})()};.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\m=NpD4ec,SF3gsd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,oWOlDb,n73qwf,MpJwZc,bIf8i,omf1Od,zbML3c,zy0vNb,K0PMbc,otPmVb,rINAl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2735
Entropy (8bit):	5.342727841609952
Encrypted:	false
SSDEEP:	48:x76E0ED8ElEtEEEfEWEzEeE9EDoEuEJLEfErETNxZKSSQjaQ2aRh2b6Nz5k/kjvw:xFK4Z3T2baR26Nz5k/kE
MD5:	43C1C37F56339E6B6066797CA987330A
SHA1:	B70666B325BEA14595B401C691DC09F43856F868
SHA-256:	F8A4CD67FD516671F84F94E2F86B402D6E56BF993A7163734445EB46E24106EF
SHA-512:	28254CAE62EF1CEAF67115EBF6978B26CA67BD85F664B26A90E5281C270DFA4F98C0AB89DB71C91AC9E7B68EE4D5C48B05047EC434C542B98741DCF8BAB73340
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");._.Vt(_.by);.._.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");.._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\m=_b,_tp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	149058
Entropy (8bit):	5.466893855804824
Encrypted:	false
SSDEEP:	3072:j/XlDIMd3+WpxBL7xEWGIK+9aKiFFaJBGr6RK3dm2CZRFtODtZBJYZpv15QljU+r:j/73dp7p7yQQ
MD5:	69FC540481582501E9D314E8958E09C7
SHA1:	ECBFAE880FE9D3182367080577D4C568885AE3F8
SHA-256:	E34ABA118E2AA31DDDD54F56DBD01080CB3602A9DD467829492B1D26A93B1EB5
SHA-512:	ABFB829716AFF861444D948349BB95814D52598EB5006D3FEB103259BD240248CA878D6B7909AD0D6D1DC4E873BABDE6EB484F0C80B9816291DBE799997A835
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\m=_b,_tp[1].js	
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{.var aaa,la,baa,caa,daa,eaa,faa,gaa,haa,iaa,eb,oaa,maa,paa,aa,Ab,Bb,qaa,Db,Eb,raa,Hb;_.ba=function(a){return function(){return aa[a].apply(this,arguments)}};_.ca=function(a,b){return aa[a]=b};_.da=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,_.da);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a));this.g=!0};_.ea=function(a){return a[a.length-1]};_.fa=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)};_.ia=function(a,b,c){b=_.ha(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]};_.ha=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};_.ka=function(a,b){return 0<=(0,_.ja)(a,b)};_.la=function(a){if(!Array.isArray(a))for(var b=a.length-1;0<=b;b--)delete a[b];a.length=0};._.ma=function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\mspin_googcolor_medium[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	8707
Entropy (8bit):	4.910329849919684
Encrypted:	false
SSDEEP:	48:+fKyolAykoM1ghYipLJqJusZPttpZmD3Xnp9/qgod:+CSomZVfZQ8
MD5:	E9D99136E07244D9B5B24D45FB710BC4
SHA1:	B2405E47C4D87E232D896165314A5BB8314C22FE
SHA-256:	E46138FD8C6D5C3982CDD838F7455EA9B69F1280B684685A74C93966BC1C0090
SHA-512:	15DA65844A8D7539E26FF3632677051AE66702B4F9B2D1E0EAC0CF4A424099ACD8FB37447C16D52A9A38F3B347F5CDB77C50494E4BF2F12D1D458693510FEA2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/content/images/static/mspin_googcolor_medium.svg
Preview:	<svg version="1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="11664" height="36" viewBox="0 0 11664 36"><defs><path id="a" fill="none" stroke-dasharray="58.9" d="M18 5.5A12.5 12.5 0 0 1 1 5.5 18" stroke-width="3" stroke-linecap="square"/><g id="b"><use xlink:href="#a" stroke-dashoffset="176.66"/><use xlink:href="#a" stroke-dashoffset="176.58" transform="translate(36)"/><use xlink:href="#a" stroke-dashoffset="176.32" transform="translate(72)"/><use xlink:href="#a" stroke-dashoffset="175.85" transform="translate(108)"/><use xlink:href="#a" stroke-dashoffset="175.14" transform="translate(144)"/><use xlink:href="#a" stroke-dashoffset="174.13" transform="translate(180)"/><use xlink:href="#a" stroke-dashoffset="172.78" transform="translate(216)"/><use xlink:href="#a" stroke-dashoffset="171.01" transform="translate(252)"/><use xlink:href="#a" stroke-dashoffset="168.78" transform="translate(288)"/><use xlink:href="#a" stroke-dashoffset="166.02" transform="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\operatorParams[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1365
Entropy (8bit):	4.842240275244309
Encrypted:	false
SSDEEP:	24:D76bBSoFvVdG4xp9klH/rgk4oRoROSRv/4QBEwrlcKmlQFHMhfY0ypgkv6RHR/rd:H8PNA4xpKlf8PoaOA34EE6cfAsG4R91r
MD5:	3208B82E41333F3B7CE96A7627C00CB8
SHA1:	F812C8F6AB6F8336CD5C56780C72EFEAE037939E
SHA-256:	FFDF0076C701214B552E47A934A1378BCA38F2AB1633C74E47EA8D22F8F17951
SHA-512:	A239BB790D5515402C234F5C81280B4FA659533A6736841B3B901A9A04F530BEC0E10CE54D8FCC012CEE8178C1551EE5517C068A0ED97FB653C23B1F79E66363
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/realtime/operatorParams
Preview:	{. "operatorDeferredUrl": "https://ssl.gstatic.com/support/realtime/operator/1605690075554/operatordeferred_bin_base.js",. "eagerLoadHostnamePattern": "((https://www\\.google\\.com/express)|(adwords|campaignmanager|support|support-content-staging.sandbox|business|fi|.+\\.corp)\\.google\\.))",. "eagerLoadHostnameFlags": "i",. "cbfVersion": 1605690075554,. "experiments": {. "attachment_upload_url": "https://support.google.com/chat-upload/support-cases/resumable",. "enable_chat_attachment": false,. "enable_chat_attachment_percentage": 5,. "enable_desktop_screenshare_email_fallback": false,. "enable_emojis": true,. "enable_youtube_specific_endpoints": true,. "mole_show_survey_url_percentage": 100,. "mole_skin_version": 2,. "operatordeferred_report_rpc_events_percentage": 10,. "screenshare_skin_version": 3. },. "settings": {. "attachment_upload_url": "https://support.google.com/chat-upload/support-cases/resumable",. "enable_chat_attachment": f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\operatordeferred_bin_base__en_gb[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	379932
Entropy (8bit):	5.196865288101806
Encrypted:	false
SSDEEP:	3072:A033VDAYCFw9+2La7xd2B1iFz1visMSY1wCGA8ix0AAIevFA/Fp2qDA22aYD6DhR:ByC2cB8ixJAIeO/Fp23k
MD5:	85DC4DCAE32506FDDAA96FE005BFD548
SHA1:	D9FBEC608D636F015E31B66503B8A8BCE57DEF2F
SHA-256:	70E4304A71FC141D0C81F37039D54AE919E477A8D2E9F46A0007309E612A501C
SHA-512:	C87BAA75CE88A86A68B864D4C7FC19A3058B516A92AABE251E253EB1F5ABB777808A26926A80E3EFD8629AC3846EBFAAE513737450F75978562D95B2D5E10AF3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\operatordeferred_bin_base__en_gb[1].js	
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/realtime/operator/1605690075554/operatordeferred_bin_base__en_gb.js
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var rtsinternal_,rtsinternal_aa=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},rtsinternal_ba="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},rtsinternal_ca=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("Cannot find global object");},rtsinternal_da=rtsinternal_ca(this),rtsinternal_a=function(a,b){if(b)a:{var c=rtsinternal_da;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&&rtsinternal_ba(c,a,{configurable:!0,writable:!0,value:b})}};.rtsinternal_a("Symbol",function(a){if(a)return a;var b=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\privacy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	304305
Entropy (8bit):	5.758437776809534
Encrypted:	false
SSDEEP:	6144:4vGIPMUDiDHDkhifgSB39FffGiynK1ZORmGc:bwSNGib
MD5:	0E8D8478B01C4202481EDD480DBAB93C
SHA1:	412A42277B45D0312828613240B5B233830CAF46
SHA-256:	B86D30C49C57F1CD822B3097C4AD0A4F5A22B21323066E0EDC58A4A74AF22612
SHA-512:	3B02D73DDB3674FEC4389D7CF39B58405C0A5DCDFD002916C1D0BCF132D1347647A7E55198063F63CF46AB19A38097690C1D9459F78240AF75465517F28AB1B5
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" dir="ltr"><head><base href="https://policies.google.com/"><meta name="referrer" content="origin"><meta name="viewport" content="initial-scale=1, maximum-scale=5, width=device-width"><meta name="mobile-web-app-capable" content="yes"><meta name="apple-mobile-web-app-capable" content="yes"><meta name="application-name" content="Privacy & Terms . Google"><meta name="apple-mobile-web-app-title" content="Privacy & Terms . Google"><meta name="apple-mobile-web-app-status-bar-style" content="black"><meta name="msapplication-tap-highlight" content="no"><link rel="manifest" crossorigin="use-credentials" href="_/IdentityPoliciesUi/manifest.json"><link rel="home" href="/?lfhs=2"><link rel="msapplication-starturl" href="/?lfhs=2"><link rel="icon" href="//ssl.gstatic.com/policies/favicon.ico" sizes="32x32"><link rel="apple-touch-icon-precomposed" href="//ssl.gstatic.com/policies/favicon.ico" sizes="32x32"><link rel="msapplication-square32x32logo" href="//ssl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\rs=AA2YrTur8uQVb0PS_fZQNu3wmpDiwcWuQQ[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	301
Entropy (8bit):	5.1920370610104065
Encrypted:	false
SSDEEP:	6:ea+ZwTcqcA2n6gt9VvKcZWbnRVIM6RoeSjIUVY2f2H2gs8Y2HEIzY/:eZZfqcA26gAcZWfp6SVYqoY/
MD5:	2122313E26FFB1184EB213EE9A780DB9
SHA1:	04A851AFAA376415EC562ED675B4B1157F86B799
SHA-256:	2DB4ADD54D1C078CC5F8DC084365314868C10FA279EABC67AFD187F47D08C59F
SHA-512:	004F6E615FDB7A06986733FBACD4847FAD3BA7487DBA95A72922E18BA72F13ADC15B44AA6B2259F8AA7C53A748A0E5D8393FCF7CE9E1DB1481F654DFEB1850E
Malicious:	false
Reputation:	low
Preview:	.gb_3e{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}.gb_Lc .gb_Hc{overflow:hidden}.gb_Lc .gb_Hc:hover{overflow-y:auto}sentinel{}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	95969
Entropy (8bit):	5.567580078621914
Encrypted:	false
SSDEEP:	1536:2aCeBYGw2mpgkkbeqjX/lEHvwUM0XIHQ+1+l3Tv3wXOd8Yg:fUkNEHTXIT+l3Tv3wXj
MD5:	6020680693D84765D9F3D7B52EA4B679
SHA1:	34BA27AD62CE4A837DE35DFBB0977CF65A4E134D
SHA-256:	437D7BBBBF661E6F3354FEEDD7AEE407A9F86BAD1BAF2FEAB811CB818BA12CBF
SHA-512:	AF5803C2BB677ED28FEA6209C3F0A27C7C8A6E6D003EEC9F00B95E6282714628D24063D53CC7F79E5FD76E9ACE93A1906B3D3E8FEA80D2FE55FFB0A93B14FB80
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\rs=AA2YrTvt_FChtzGjr4wKVQY3jzJEAyfceg[1].js	
Preview:	this.gbar_=this.gbar_||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Pj=function(a){switch(a){case 200:case 201:case 202:case 204:case 206:case 304:case 1223:return!0;default:return!1}};._.Qj=function(){};_.Qj.prototype.o=null;.var Sj;Sj=function(){};_.v(Sj,_.Qj);Sj.prototype.j=function(){var a=Tj(this);return a?new ActiveXObject(a):new XMLHttpRequest};Sj.prototype.B=function(){var a={};Tj(this)&&(a[0]=!0,a[1]=!0);return a};var Tj=function(a){if(!a.A&&"undefined"==typeof XMLHttpRequest&&"undefined"!=typeof ActiveXObject){for(var b=["MSXML2.XMLHTTP.6.0","MSXML2.XMLHTTP.3.0","MSXML2.XMLHTTP","Microsoft.XMLHTTP"],c=0;c<b.length;c++){var d=b[c];try{return new ActiveXObject(d),a.A=d}catch(e){}}throw Error("U");}return a.A};._.Rj=new Sj;..}catch(e){_._DumpException(e)}.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.Uj=function(a,b,c){a.j||(a.j={});if(!a.j[c]){for(var d=_.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\so[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):	47212
Entropy (8bit):	5.730429789215543
Encrypted:	false
SSDEEP:	768:n7Y/d9SvRuKsUM0t/bfnoV9pDnvKQPFJ/N4RlQkSzdMoQ:IMMInoD9nvB1/xMoQ
MD5:	B4AEC56E06030CBF9ED66F8071311609
SHA1:	73D6DB41AB9E734ABAAF81699F7E6D54B5CBBFDF
SHA-256:	1B0E5ABC56014ADDBA04F7E0BF3996D2A2C392A6DCF1645103F1CB2E85C9EC3B
SHA-512:	3050EAD297FD2178D9AB8A82DAB4C39243C5A374DDBDBACE955044E335F436C8795BF14F0C4CDE96FFE21248AE44A26EA98E52BB8A0A890FF3EC9B8D8BCC043C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/app/so?origin=https%3A%2F%2Fsupport.google.com&cn=app&pid=117&spid=117&hl=en-GB
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/app/so"><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="o8BwIFsUHapfo1PQCq0S9g">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"3949140143148630847","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1606666115019533,173291784,3355807101]\n","ZwjLXe":117,"cfb2h":"boq_onegooglehttpserver_20201123.05_p1","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333,45695529],"gGcLoe":false,"ikfjnc":["https://support.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"OneG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\so[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46802
Entropy (8bit):	5.726967607770338
Encrypted:	false
SSDEEP:	768:9N/d9SvRuzsxM06q2fnoV9HDW46QPFJ/N4BT/EkG:F+MVnoTjW4x1GbEkG
MD5:	DB5AD23730406F5F3F31D217CE56831C
SHA1:	77E23750DC4EB3337DDC96255360B2B31C859CD3
SHA-256:	CDF9720B8B1BDEBDEE97B164E5922109E02A39F4C882CD6781ABC8CBCAF2214B
SHA-512:	2C25AF3BA18479EDC5F3B8AD71675499643F6F9773454293C62B8AA5BBB9DBF28AC4EDA3B9F583859686B91CEEFE8F152FC6F18803EE5E6B838F63C4F91F81A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/app/so?origin=https%3A%2F%2Fpolicies.google.com&cn=app&pid=269&spid=545&hl=en-GB
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/app/so"><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="0z4Mo45/upcrkPRWPNLImw">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"3221608897351282256","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1606666122633787,179611406,1308833540]\n","ZwjLXe":545,"cfb2h":"boq_onegooglehttpserver_20201123.05_p1","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333,45695529],"gGcLoe":false,"ikfjnc":["https://policies.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"One

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\unnamed[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2205
Entropy (8bit):	7.875866081017329
Encrypted:	false
SSDEEP:	48:Por0q6wxObS4r9kcVc6NUBJT7Ab/j5AfSsaI3gWxbkExHONr1z+wVR9:PordAc6Nz/j+qsaAfxLxHOTz+09
MD5:	3D553900813C909560ED13B0B8D1B845
SHA1:	C5C30567596401FEF1835A9649C3F2EC598B6EBD
SHA-256:	62C6F83E97D9ADE9ABB474FFEF8503B10150DA0E9215D173E4873BC7AE045667
SHA-512:	D009F707E3B4BFE63873026E4059C91D837B18BF1261AFCA7C62955A1EF3B654D91D4741D731E27A1E8AD2C10FD610EC5172F67AB64462C033D0913878D1E444
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\unnamed[1].png	
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/fKYxJWmqWKS5JTWJUHJSE6u4tKZ6JbFx7YGMbbH0cI72r3E2MhU0vPrE6uaflUm94Q=w64
Preview:	.PNG.....IHDR...@...@.....iq....dIDATx..ip.E...+Ey!".....e..... "B...3.X.)@...#..%..(PB..AH.as`.....!.....v.n.....~=.C....}7...Y..h.. IR.~..eY....'.....G..L...v.....!.6.*D.f. ..fD.Es..Z[.^!....!.T...x.-..H.5..W.....R..C3P%|P.U.fO.:..w_.....ll....c8...l..."L.F.....at.LP..)A.p..:.+<..n4*S.!f.....~~..J[ot....U.H..e....y....B.....a/;..w..}.`j..s..n.(...6.....B.....0i ...555..6....N1H...8m....B.0..+.....hP8.7.|.f....x..Rg*$+.A..... .?.....i.W.<..._.\V.m..;p..I...<}....#.P.'..9.P4~$8R.s.@..S.%...$a.'p.....76 .#j...6..T8.=...yQ.....W....|..+.&..Wq...*., .Ou.`...>U...}..... ....a:...K.O..}.I-x..cs...x..K.0{..3...+.\T..j...,#.u.....a .....e.,..i.<...t~[... ..s..j![...`..0.}E9..L.....D._.Y@.`tX@..c.....=.....[..p.x:.H:`z.(...ry.C.....E.Yn.-.....b.`..!J.....@. ..]...gZ.l....et.....{..!.O.B?.U.g....._F...)...._k./,.....,..W.%p..7...l....l:7...U..X.n.m.....v.i...W..jE@.S._.@..J...n..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\48I-xdS4pXg[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):	43517
Entropy (8bit):	5.9163415929708965
Encrypted:	false
SSDEEP:	768:yECoBR6oVfOuwaYJ9QuINqCrMatUIr4mf/KIF9nJSCxO6eNV:Zwas9QuINrhUIr4mfBQ7jV
MD5:	EC6D07D1BDD4FA83476C3A7F63C5F1B3
SHA1:	13D47AA1F54608FB17C02A43664A20810CE0146F
SHA-256:	A887173F193B2B6324DEC5DABDAEAF763814C2C9362177EBA31DF602C933669D
SHA-512:	94C5867D657AF9BE35F02B7BDB99DD82A04C41CC207A6FED6D0E87E87CFC5AD13CB9B46C64A21AD5B2680EB170361C0D0BF80006C4225305B5E0E1E4C61EB C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/embed/48I-xdS4pXg?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pref=en-GB&cc_load_policy=1&enablejsapi=1
Preview:	<!DOCTYPE html> <html lang="en-GB" dir="ltr" data-cast-api-enabled="true">.<head><meta name="viewport" content="width=device-width, initial-scale=1"><meta name ="robots" content="noindex"><style name="www-roboto" >@font-face{font-family:'Roboto';font-style:italic;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18 /KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFO mCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1 MmEU9fBBc-.woff)format('woff');}@font-face{font-family:'Roboto';font-style:italic;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xII zQ.woff)format('woff');}</style><script name="www-roboto" >if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "");document.fonts .load("500 10pt Roboto", "");}</script>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\4c5ee41d52605ff6f43538d46a1c0d35[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	12773
Entropy (8bit):	5.021780026284317
Encrypted:	false
SSDEEP:	192:s/HeqPFaqW9UXuhX85+dkoEe3jO+HKFvO:0He2K9UMX8563jn
MD5:	4C5EE41D52605FF6F43538D46A1C0D35
SHA1:	5432F87B16A63087A22EDFA0AF1C5ECA4FADE3C4
SHA-256:	89BBCE254FCE9A0F06C8A2C4E491E4811418E25EE92183EE42C5CD6154778C1D
SHA-512:	7F655C5ADE13D276CF4CE6BEDAAF58F8E1A215018A39529B121B64284B1AE54031858CA4907B0715518BC01B146561F00BA4FDE6B1229CA2CDC3256EF44DCD 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/4c5ee41d52605ff6f43538d46a1c0d35.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="16" y1="165" x2="40" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9 aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="200" x2="228" xlink:href="#linear-gradient"/>. <linearGradient id="linear-gradient-3" x1="158" y1="137" x2="186" y2="137" gradientUnits="userSpaceOnUse

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\51cd09d6239edc9652bc05ad1d149a5c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	13177
Entropy (8bit):	4.927867691017123
Encrypted:	false
SSDEEP:	96:+RHGRrrsHa2aDBUKdU1Q7dXphVsVjVArUaNqvqurfGFDJDfQaUZuZyWF2gSM4wEz:4G6HiNq14FvrUaNqvqiGJJjUE8wnI
MD5:	51CD09D6239EDC9652BC05AD1D149A5C
SHA1:	6C88C92D1C01A8ADDDA86322DEB1487CDA763C8E
SHA-256:	96B628232FE1459C56ADFC5E7877CE0AEC28E17D3B137408B7A2EC278181BDDF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\51cd09d6239edc9652bc05ad1d149a5c[1].svg	
SHA-512:	DA5F756FBFBA4EE0540B651D2DA1A5664A2689E55EC3F7124F284C3B2EC7288E447D7CEB5A54CC372E7E782D8DA0DBCB320E68F71D1A3E675F4085BB88BFB8 12
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/51cd09d6239edc9652bc05ad1d149a5c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="293.155" y1="108.155" x2="321.845" y2="79.466" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6"/>. <stop offset="1" stop-color="#bdc1c6" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="46" y1="93" x2="74" y2="93" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6" stop-opacity="0"/>. <stop offset="0.137" stop-color="#bdc1c6" stop-opacity="0.021"/>. <stop offset="0.279" stop-color="#bdc1c6" stop-opacity="0.084"/>. <stop offset="0.424" stop-color="#bdc1c6" stop-opacity="0.189"/>. <stop offset="0.57" stop-color="#bdc1c6" stop-opacity="0.336"/>. <stop offset="0.718" stop-color="#bdc1c6" stop-opacity="0.525"/>. <stop offset="0.864" stop-color="#bdc1c6" stop-opacity="0.753"/>. <sto

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\546f2b674b407304a2570e71a216e509[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	20864
Entropy (8bit):	4.925372381610842
Encrypted:	false
SSDEEP:	192:7HksMYZuvecIQW8rzTLbzDAEIHN8Ssvopa:7HU12wvopa
MD5:	546F2B674B407304A2570E71A216E509
SHA1:	0ADEC43FBC9DFC2AB1587FD3F6A673FE227B625B
SHA-256:	9D42DE0208263D6D6E7F1A627677B426CCB3E492334293B794CC141F9FA0FB3B
SHA-512:	D8CDC2C086A94E00D2D14CED3D87CB17235AC9F541CD2C6A28F438FA8CDFD064D832B53E40D58CAD4C4D5044FDDCF777DF2BBC2C2902874C1B23EF3096FE C05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/546f2b674b407304a2570e71a216e509.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="13" y1="105" x2="49" y2="105" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6" stop-opacity="0"/>. <stop offset="0.137" stop-color="#bdc1c6" stop-opacity="0.021"/>. <stop offset="0.279" stop-color="#bdc1c6" stop-opacity="0.084"/>. <stop offset="0.424" stop-color="#bdc1c6" stop-opacity="0.189"/>. <stop offset="0.57" stop-color="#bdc1c6" stop-opacity="0.336"/>. <stop offset="0.718" stop-color="#bdc1c6" stop-opacity="0.525"/>. <stop offset="0.864" stop-color="#bdc1c6" stop-opacity="0.753"/>. <stop offset="1" stop-color="#bdc1c6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="39" y1="166" x2="75" y2="166" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\6RYML-AXwgKXIEhuMiV2AYgQkEUD0Ei6B6ms7b7P0Jk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	22030
Entropy (8bit):	5.607219130091125
Encrypted:	false
SSDEEP:	384:Fxj+RhI3EKo9yStGTtfdv4hnitKGMyInoFK8rPoM:FR+RC3EKokSwui+kFl
MD5:	0E32A494C72100AFA8320DCF728DDE81
SHA1:	F59CA0C93AA27387A59CBC8905A89F12F670E7FD
SHA-256:	E9160C2FE017C2029720486E322576018810904503D048BA07A9ACEDBECFD099
SHA-512:	B3E406AF3FCD50BB9501D2F993886E9D08F55BEE3F5BE778E5AE68B6B65052072158ED11BC98E1707256A88DB868FB48D35238DEA5A15C9C7D40BF37792F58C A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/6RYML-AXwgKXIEhuMiV2AYgQkEUD0Ei6B6ms7b7P0Jk.js
Preview:	(function(){var Q=this||self,r=function(T,W){if(W=(T=null,Q).trustedTypes,!W||!W.createPolicy)return T;try{T=W.createPolicy("bg",{createHTML:K,createScript:K,createScriptURL:K})}catch(O){Q.console&&Q.console.error(O.message)}return T},K=function(T){return T};(0,eval)(function(T){return(T=r())&&1===eval(T.createScript("1"))?function(W){return T.createScript(W)}:function(W){return""+W}})(Array(7824*Math.random()|0).join("\n")+'(function(){var T0=function(T){return T},t=this||self,q={},U,Wv=function(T,W,K,O,m){for(K=(O=[],0),W=0;K<T.length;K++)m=T.charCodeAt(K),128>m?O[W++]=m:(2048>m?O[W++]=m>>6|192:(55296==(m&64512)&&K+1<T.length&&56320==(T.charCodeAt(K+1)&64512)?(m=65536+((m&1023)<<10)+(T.charCodeAt(++K)&1023),O[W++]=m>>18|240,O[W++]=m>>12&63|128):O[W++]=m>>12|224,O[W++]=m>>6&63|128),O[W++]=m&63|128);return O},f={},QG=function(T,W){return T<W?-1:T>W?1:0},iy,Kh=function(T){return/^[\\s\\xa0]*([\\s\\S]*?)[\\s\\xa0]*$/.exec(T)[1]},OZ=function(T,W){function K(){}T.Xg=((T.prototype=((K.prot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\900a793eae04f4bddd675f8d95c4a794[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4391
Entropy (8bit):	5.07432704633403
Encrypted:	false
SSDEEP:	48:+GO/YWHx4GLZ/W12HxDWj6V7QlWHxjUW+ev/3jZVV8gFOiawwEMqjJ79oqFCB2lK:+Hp2ShN4Q3ji9w8qj1C/JBWgWV
MD5:	900A793EAE04F4BDDD675F8D95C4A794

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\900a793eae04f4bddd675f8d95c4a794[1].svg	
SHA1:	D79FE87CC4B220245AB72251DCF3AE4C71108544
SHA-256:	166EAB00B3516B5AEB1BB114FA70D57E0F4E021D4C06735C6969B08C5B7E1FDB
SHA-512:	E18FC18597424E69987E13E8F4E6E174A56B46C2D1616E203AC9C02EFBEFB47CCABB39ED999B0DF1784CEFC0D7444C19E2DDACA30022F45864554F999587DE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/900a793eae04f4bddd675f8d95c4a794.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="96" height="96" viewBox="0 0 96 96">. <defs>. <clipPath id="clip-path">. <path d="M48,7A41,41,0,1,0,89,48,40.989,40.989,0,0,0,48,7Z" fill="none"/>. </clipPath>. <linearGradient id="linear-gradient" x1="12" y1="68" x2="24" y2="68" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.116" stop-color="#9aa0a6" stop-opacity="0.054"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.201"/>. <stop offset="0.546" stop-color="#9aa0a6" stop-opacity="0.44"/>. <stop offset="0.823" stop-color="#9aa0a6" stop-opacity="0.768"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="46" y1="71" x2="46" y2="25" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#f29900"/>. <stop offset="0.138" stop-color="#f29900" stop-opacity="0.81

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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+tS9nAIRMeC4J4h4II7xtUOTCBGt+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\NUEPGTR9\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20356, version 1.1
Category:	downloaded
Size (bytes):	20356
Entropy (8bit):	7.972919215442608
Encrypted:	false
SSDEEP:	384:of+dt1ebKR28EPpAXxR5wthZZv4B8Te/h4+ctr5NH9NwZaUp4VsEgm:of+P1eeRcU8Hqdy+UHHbEw/
MD5:	ADCDE98F1D584DE52060AD7B16373DA3
SHA1:	0A9B76D81989A7A45336EBD7B48ED25803F344B9
SHA-256:	806EA46C426AF8FC24E5CF42A210228739696933D36299EB28AEE64F69FC71F1
SHA-512:	7B1D6CC0D841A9E5EFEC540387BC5F9B47E07A21FDC3DC4CE029BB0E3C74664BBC9F1BCCFD8FB575B595C2CC1FD16925C533E062C4C82EEE0C310FFD2B4C927
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....Q...`u...cmap...\.....W.cvt ...T...H...H+~..fpgm.....3...._...gasp.....glyf.....;...k....hdmx..H....m....!$..head..H....6...6...\hhea..I,.....$.&..hmtx..IL...y.....XF.loca..K.....`.C.maxp..M.... ... .(..name..M.....~..9.post..N..... .m.dprep..N.....)*v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B......./.)x$.'"j....1LGmaGxQxG....~..:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%.....j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].IQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z..-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\TOS[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	197
Entropy (8bit):	6.748558418265418
Encrypted:	false
SSDEEP:	6:XtwM9CG1f8OaC3TVXZc/S28CGWdjV2K+j:XWGWD0TLubxjU9j
MD5:	D2637B3A0059D2AA6133D587491FCB76

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\TOS[1].htm	
SHA1:	10B4804ACF823EF874069793C27522D190443F79
SHA-256:	13AE332B053348547D338D24907CAA06EF48342A1074661235715B3CA2742A9D
SHA-512:	02E60F72B132C12C09627EFF30B7DF68092D4954CB940AC3662908AE1CA612B355FC45489E26CFF924AF66985329CAFC178365B88CABED7558C8B8C69B4B71B
Malicious:	false
Reputation:	low
Preview:	.....m....0...>EH.....F....E(9.G.....}5.sYvv...9/..y....w^$aifh..m.P.R-.\|..%. ...b.*.G.w..F<y.u=:....mu=....yk.'$..i.....I.`1Mv<.b.....r.... c.Z.P...P...D...n...=..Z..R....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\YlmVKT3Zvhw[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):	43360
Entropy (8bit):	5.922615748531229
Encrypted:	false
SSDEEP:	768:y7aC8R6oVfObeqfhuYqpIDMpi4iNJgBakyH7w:c7qpORBZH0
MD5:	A7903601594162C40421A8F7F253BA48
SHA1:	9A33B3315412ACAD87B9884F1401F4BB2947DD45
SHA-256:	0FAF193BA4BE2158FC950596998FA6BA178FB7F9542E55894015766ACF821AF2
SHA-512:	57C02A8A9B94B0ED71F96C0E6B999B8DD6D26B1DF278BCC98EFBBA451C1C5BADCEDD979DB3E5464F2D795F973DF77A81F419F77C6EE6BB7D8D4C76600447A DA4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/embed/YlmVKT3Zvhw?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pref=en-GB&cc_load_policy=1&enablejsapi=1
Preview:	<!DOCTYPE html> <html lang="en-GB" dir="ltr" data-cast-api-enabled="true">.<head><meta name="viewport" content="width=device-width, initial-scale=1"><meta name ="robots" content="noindex"><style name="www-roboto" >@font-face{font-family:'Roboto';font-style:italic;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18 /KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff)format('woff');}@font-face{font-family:'Roboto';font-style:italic;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFO kCnqEu92Fr1Mu51xIIzQ.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92 Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc- .woff)format('woff');}</style><script name="www-roboto" >if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "");document.fonts .load("500 10pt Roboto", "");}</script>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\ZdEIZNg3epQ[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):	43224
Entropy (8bit):	5.921261655609865
Encrypted:	false
SSDEEP:	768:xCEC8R6oVfOceq87WT2Ym10qgACZ/tKt6C9iGebIpjPJeMddZ+7G:4q87WT2Ym1lgwtpMGl+7G
MD5:	28A9878F08D23209DC04F7F88F9311F5
SHA1:	D114BAAB17B0768E7B0097A8FCA480AF928FE18F
SHA-256:	548A447BAB42E66E45B5D7141AC5A3D65B71ABECA5F494D9F06704F1358B0C7B
SHA-512:	A2B567A98F11ED7D30CFA0D3877D32DE81E84C85D24B8A5C2A32B67CF3D4D1FECB9FA685FFFD2A5E87E3C50B526FEA1B014C0878DFE86724DBEFD12D34862 62
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/embed/ZdEIZNg3epQ?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pref=en-GB&cc_load_policy=1&enablejsapi=1
Preview:	<!DOCTYPE html> <html lang="en-GB" dir="ltr" data-cast-api-enabled="true">.<head><meta name="viewport" content="width=device-width, initial-scale=1"><meta name ="robots" content="noindex"><style name="www-roboto" >@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:italic;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOjCnq Eu92Fr1Mu51S7ACc6CsI.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92 Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc- .woff)format('woff');}</style><script name="www-roboto" >if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "");document.fonts .load("500 10pt Roboto", "");}</script>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a8e78fa7fa279aa946fe1a9d6a0508f2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	20225
Entropy (8bit):	5.08641328988594
Encrypted:	false
SSDEEP:	192:Uzm9EDtDWs9GYb2o0qRn1Zlxdf8x2l+NJCVMZSh8iV11MS9xEWEbXZQOaLvED5:c9p2o0qn1ZlxdEx2zGvm8pLvEN
MD5:	A8E78FA7FA279AA946FE1A9D6A0508F2
SHA1:	F9F8EB782246A6C7BC79B043B66C1F3B3BF4B42B
SHA-256:	2196B3304BAA87751FD4EF3F62B307566487CD03199284BAA1E674E27E2FFA5E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a8e78fa7fa279aa946fe1a9d6a0508f2[1].svg	
SHA-512:	CE6AD1FFD1E76B916259989F8757B8489A13FDFFE30D37A8C8B6F1F5581D9896EAABD842AF38C8E370D0638AD4BE2963D627D89747EA800D6C1DB1391EC016A B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/a8e78fa7fa279aa946fe1a9d6a0508f2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="180" y1="26" x2="180" y2="170" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#e8eaed"/>. <stop offset="0.124" stop-color="#e8eaed" stop-opacity="0.835"/>. <stop offset="0.364" stop-color="#e8eaed" stop-opacity="0.542"/>. <stop offset="0.58" stop-color="#e8eaed" stop-opacity="0.309"/>. <stop offset="0.764" stop-color="#e8eaed" stop-opacity="0.141"/>. <stop offset="0.91" stop-color="#e8eaed" stop-opacity="0.038"/>. <stop offset="1" stop-color="#e8eaed" stop-opacity="0"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="32" y1="165" x2="108" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\acad335ad7ba163209d8c3e671b2c445[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	9346
Entropy (8bit):	4.909678911846309
Encrypted:	false
SSDEEP:	96:+12aGkB/pvtjRn5EC9QeOgyCVWV3h4yx2WFt1PMXdDWCkgiQAJ9FnPDbs/A2i:6jt9nGCG4SxMhkyAJfnPD4ti
MD5:	ACAD335AD7BA163209D8C3E671B2C445
SHA1:	6FFD6741AE59ED5B7AAA33505EF2F57F86A1D082
SHA-256:	BBD9E8EDDB8A9888E40E0CF19EA2E0898D7C2FA534B4E70F3922B7A1A20A584D
SHA-512:	C96EAF974A77B8D17723F02F84A4C28DC9B9A34C7DB0867CE7674C51A5772667152EE9057C137EA639DAA1728C23C22917DB05758BE7A56588D10D744A52C99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/acad335ad7ba163209d8c3e671b2c445.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="119" y1="165" x2="147" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="67" y1="165" x2="115" y2="165" xlink:href="#linear-gradient"/>. <linearGradient id="linear-gradient-3" x1="107.557" y1="61.557" x2="119.557" y2="49.5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\accounts[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.573637583125686
Encrypted:	false
SSDEEP:	6:wRkrQWR0iYBtqWkT2apKHu5BLCRiRtcRujcVRhHalZDDe86kToP:ekrY1t6Ks9CRi+ugV/IZDDesi
MD5:	AA1E0806D2F06EDAC8C89FC0C759FD2F
SHA1:	FD8BB6917025024BAD7CB5849EA42275AC8CCEC5
SHA-256:	1AE8A2F9CFA5394C2DD7596D217AF44D6FA58F14B05543DC91703758D0CAFF62
SHA-512:	DFB70EE28A712EBF984603198A7B163318D1142A1F922A7DC3119584E3C61F4646AF6F326578217D8A5368319FD8F006FB6A178EAD25761A27D14CA06661C22A
Malicious:	false
Reputation:	low
Preview:	<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>302 Moved</TITLE></HEAD><BODY>.<H1>302 Moved</H1>.The document has moved.<A HREF="https://support.google.com/accounts/answer/2917834?visit_id=637422629137283870-597027064&p=signin_privatebrowsing&hl=en-GB&rd=1">here</A>...</BODY></HTML>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bscframe[1].htm	
Reputation:	low
Preview:	<!DOCTYPE html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	63719
Entropy (8bit):	5.5792036933703235
Encrypted:	false
SSDEEP:	1536:pIjKdByen4KOw9McPis5wfmYWG7UIaJtTY2O26q02p:pxByen4mG7UIavY2Okp
MD5:	A25830D61E3A5E9C0EE1247711B1A2A6
SHA1:	CEB58B5369DBC7CE426C3856BBEC7E99332BE07C
SHA-256:	1320C729BB178D835E39CD1BF83F8C64EA0F8973BBCF69E27F9FAD8D7E2456F7
SHA-512:	9C2009AFA9F59F1077067CCD7D1FD4125DEF8DF44D4B0F4F42072CD9E7709F7622529326B234591A31CFCFA9253049AA136AAE942542BC311F744DB1ECD8DED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.uhBKOtz6fOw.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8GZHNTtpcfighnqAH0uUZTALLzrw/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 ja,na,ta,xa,Ba,Da,Ia,Ra;_.ea=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ja=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};na="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};.ta=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");};xa=ta(this);Ba=function(a,b){if(b)a:{var c=xa;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&&na(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
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...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\NUEPGTR9\favicon[2].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:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.google.com/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[2].ico	
Preview:	..... .h...&... ....(..... ....0.....v.].X.:.X.:r.Y..... .....q.X.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\NUEPGTR9\ggoJFaE71W8[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):	43221
Entropy (8bit):	5.918688130879337
Encrypted:	false
SSDEEP:	768:xCD/uR6oVfOHXsKtcpcsHuaCHT9WwsXXH/YJ6BrkAvTK:6tpMjXHXpH2
MD5:	595F4E99F73C44604681937723941690
SHA1:	5AB516584EC8090B561A79B88C72C3E4FAF9C4A7
SHA-256:	0D8D35C6316C69AF29BCCEE271FEB2C66A935FCF8E773003B8DB28F48492978D
SHA-512:	E2343EDF47AAF713894952D400C7256726ADB4721C82196D5A9F6FAFE1F4B7128821163DDAA6D568CF53E65E918D7DF80FBC8DEB62AAB83EA5852A8F9A6EE0E 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/embed/ggoJFaE71W8?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pref=en-GB&cc_load_policy=1&enablejsapi=1
Preview:	<!DOCTYPE html> <html lang="en-GB" dir="ltr" data-cast-api-enabled="true">.<head><meta name="viewport" content="width=device-width, initial-scale=1"><meta name ="robots" content="noindex"><style name="www-roboto" >@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:italic;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOjCnq Eu92Fr1Mu51S7ACc6CsI.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92 Fr1MmEU9fBBc-.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4m xM.woff)format('woff');}</style><script name="www-roboto" >if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "");document.fonts .load("500 10pt Roboto", "");}</script>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\keyboard_arrow_up_24px[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	147
Entropy (8bit):	4.9621270003690565
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMcBH8+hHiATcvXjXRHoNcHgDXFUVLUJRVFiAdFUvuIIb:tI9mc4slzXdhC/O4gSVLU9FRF0ulb
MD5:	1F5DC0C5F607EC3BF9E3089FEBD9C373
SHA1:	1D8D1276A56A42B3EA7393767A8674CD45C43439
SHA-256:	00D8F7123BB5EF3F7FAD786905F5407CC5FB8B4C55E1B0511803F6C8C01E3903
SHA-512:	98C5C969A12B196176ADDD9C7DD8234C9D81EC513DE453F116E766DFA32E5B99AD2AEB68609353B349A65F7B26E68166C42337668B2BF1C8513FF4C772002711
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/icons/material/system/svg/keyboard_arrow_up_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><path d="M7.41 15.41L12 10.83l4.59 4.58L18 14l-6-6-6 6z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lazy.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	52265
Entropy (8bit):	5.475708166987928
Encrypted:	false
SSDEEP:	768:VMQUKnvcw43ZVFsiweXJ1qzW4uDD2hqapZdEgbYivhQC4YIS22/qPwEf:qDKz4LXweXJ18tuDD7gE+nHb/vk
MD5:	10A0BB2665344444F0A2AAE19D49EB57
SHA1:	F0076F600A1EF09DAFB10F766AB6D8B894B40B52
SHA-256:	9C41876D134589C345A9515BF13DE8DEE71D41AEB56733DB32C7A949A5E192A0
SHA-512:	83DC93BEBB0F4E04D7F798F44E0A1AAD2FF827A85F73D749984123F55621CA6B2FCF2580DB6F97E549EC3BB2B2BF3D0DD725BB151B8F428C8694D9AA6D4D4B D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lazy.min[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n,aa=function(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}},ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.v alue;return a},ca=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("Cannot find global object")};.},q=ca(this),t=function(a,b){if(b)a:{var c=q;a=a.spli t(".");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&&ba(c,a,{configurable:!0,writable:!0,value:b})}};. t("Symbol",function(a){if(a)return a;var b=function(e,f){this.hb=e;ba(this,"description",{configurable:!0,writable:!0,value:f})};b.prototype.toString=function()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	35769
Entropy (8bit):	5.453370126475908
Encrypted:	false
SSDEEP:	768:D4Un7hNQ3LymCjcL4LYSNwivqWjURpLb1xi59hZZT4uFKyqIZ1:DBfYSNw+qWqpLb1CLZZ+I
MD5:	6E0E784A56B3BD60E33D6DB48FD88EA2
SHA1:	E1C1AE80B3EDE6851D01CB99501D2BEED5231F75
SHA-256:	144AE33EE5D0021A69CB04E6155125434EE42FE403DB23EBA82578D1877D18FD
SHA-512:	B43AAE270A75FBDA7B6559E7B951E800C653B6285DE58BE2A51200B1348424569F7FA7346554970F615C6A840638B0A0CC3785AA76A1A8370AA6539019CB04D9
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{._.m("sy4x");.._.n();.._.Ns=function(a,b){a.sort(b||_.za)};_.Os=f unction(a,b){return(b||document).getElementsByTagName(String(a))};_.m("syy");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var Vs,Xs,rea,Ys,nea,mea,qea,oea;_.Ps=function(a,b){this.j=this.ya=this.o="";this.S=null;this.s=this.i="";this.u=!1;var c;a instanceof _.Ps?(this.u=void 0!==b?b:a.u,_.Qs(this,a.o),this.ya=a.ya,this.j=a.j,_.Rs(this,a.S),this.i=a.i,_.Ss(this,Ts(a.g)),_.Us(this,a.s)):a&&(c=String(a).match(_.bk))?(this.u=!!b,_.Qs(this,c[1]||"",!0),this.ya=Vs(c[2]||""),this.j=V s(c[3]||"",!0),_.Rs(this,c[4]),this.i=Vs(c[5]||"",!0),_.Ss(this,c[6]||"",!0),_.Us(this,c[7]||"",!0)):(this.u=!!b,this.g=new _.Ws(null,this.u))};_.Ps.prototype.toString=function(){var a= [],b=this.o;b&&a.push(Xs(b,Ys,!0),":");var c=this.j;if(c||"file"==b)a.push("//"),(b=this.ya)&&a.push(Xs(b,Ys,!0),"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	5.201646455938175
Encrypted:	false
SSDEEP:	12:haxyErYfhVkrC9sAUhlHWEJU2XwPKhlHMJmWmM8ytrI:haJspVkO9svhl22PXwChleaSI
MD5:	CE9D90FFB3C12814C5C0F4950F5F6433
SHA1:	B07DA98E771A3B4BF8B73B5687FEDA880D5BB354
SHA-256:	6163C1A8B6D752F6CE86BCE4DEE223DA02FB9EBE1072ED6BFA0CD47D01912346
SHA-512:	B0CE3464A9A444C468C52C81DAEEEE36DEE812A59E8B04C3FA8C627DDDF977F3174CB75F8874286FE65656E5E574AB0F485E6BD5E6A315CC90639F7682AB67(2
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="ksOoktmg6iRjyP CeWDSZWQ" src='https://ssl.gstatic.com/accounts/o/2231879498-postmessagerelay.js'></script></head><body ><script nonce="ksOoktmg6iRjyPCeWDSZWQ" 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\NUEPGTR9\proxy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.327257778015455
Encrypted:	false
SSDEEP:	12:hYA0HqJmqG+779hLFBkAAqJmPm/esHbSU4Nbx4IQL:hYPcBDBvPz7F4NW
MD5:	CAF9B15D61F837D94E774198B9EAEE8A
SHA1:	E959E7F292E35B5C1C3E17427BED9AFE075BD8AF
SHA-256:	66E7522D7621E4AB273CAA2DF04960C81286BBD28E2B2A843C1321442C03158C
SHA-512:	4668C7918AE805983E845AF801143FDB09E5058765BC6792DAD33E770A98F8070E790ACC19B91C3CE68331C941FDDB0DEB6E193DDCF1031BD278A242E399E42
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script type="text/javascript" nonce="+cI2RUSqYc wOZPxJOokWiQ==">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script type="text/javascript". src="https://apis.google.com/js/googleap is.proxy.js?onload=startup" async. defer nonce="+cI2RUSqYcwOZPxJOokWiQ=="></script>.</head>.<body>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\proxy[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	436
Entropy (8bit):	5.2985960363719995
Encrypted:	false
SSDEEP:	12:hYA0HqJmqGj479hLFBkAAqJmPm/esHb3f4Nbx4IQL:hYPcBomBvPz73f4NW
MD5:	E8C2A75365E9CF0E4896E1CC7CF756D9
SHA1:	515CB0BA968D30F40FC0DC4F9ABC1C091E3361B6
SHA-256:	AEEC0EEAD1BC18D67DA15EDDCF6A94D36A2BC85AC646FDD06129ED8778398764
SHA-512:	52D67448BEE2AB748F57D602A5209581E682DE5D343D364BD3DCA2F928C13CA839F91719B1941EE27AEC802706D4F50A2EA8D06C0435775C8396B7F8F5CEC25
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scone-pa.clients6.google.com/static/proxy.html?usegapi=1&jsh=m%3B%2F_%2Fscs%2Fabc-static%2F_%2Fjs%2Fk%3Dgapi.gapi.en.uhBKOtz6fOw.O%2Fd%3D1%2Fct%3Dzgms%2Frs%3DAHpOoo8GZHNTtpcfighnqAH0uUZTALLzrw%2Fm%3D__features__
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script type="text/javascript" nonce="eliOnKEXFQIC2C+IkjVd1w==">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script type="text/javascript". src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async. defer nonce="eliOnKEXFQIC2C+IkjVd1w==">.</script>.</head>.<body>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\pxiDypQkot1TnFhsFMOfGShVF9eI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 40068, version 1.1
Category:	downloaded
Size (bytes):	40068
Entropy (8bit):	7.986363416256898
Encrypted:	false
SSDEEP:	768:SZjhV5AtCnIR51aT0aCfvoIypmLL5V+VQLwv0JR9D2juelmPrldaC+Qac7:S5r5KRnECf6aL5V+VQLtmk4QaC
MD5:	3ABA54A73723BD3E90CB74D603687CCD
SHA1:	2C3D597CD36CA5856587C8482557B07DD8633329
SHA-256:	A94234B7387BC4E9FA7B73DEDD34E5CC1189A28D526F4DADDECD1C9AB7B86840
SHA-512:	78F4E6514CD81CECC898D151B31B691122715D0239A47AB5D53ACA4F45FC1707DDD8464543D523E355DC1C19FF257C14DF4490D0938518D02BA35AECD72482E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/productsans/v12/pxiDypQkot1TnFhsFMOfGShVF9eI.woff
Preview:	wOFF.....`.....GPOS.....<.?..GSUB.....l..ROS/2.....V...`h...cmap...l...<....T.S$cvt .....g...l...wfpgm.....a.A..gasp.....!glyf.....Wm.....Nhdmx..i...(...O.....head...p...6...6..N{hhea..... ...$...Uhmtx.....x.....+.loca...@...\...\y"..maxp..... ... .J..name.....,+.l.post.....]/1.prep.....oNx.d..G.Q.....5.....n.....d..d..p..o.....Q.....o..y~.....<..0 ....h..'c..d8.;.N'....@...._.....LC.@.v.....:.<.....r~.c....i..&.C.!Gt.x.jF...r....K...R}H@G.la./i.#..C./Q....pl+..\..$..o.....Hm\.*.....Z..t.".S..-....p..W\...*9..a\IH...9..c.s,.<88dI...%&GD.4..DD$.w;.=..%.4N6N].R...V>..O...0q.D$.Ow.HP....7!..v..7.%#.#...;...&?a.W..\oS....P..t+T.....+.K...,.V..h.D.'t.....qW.....,.e1.n.....}.....G...q..b>.(.....#.....#Z./?0~FZ.5...O.".d4.'..|.ki..G...G.....Sv.w.@.qs`G@K.&.G..yk.....z.2.zB3.g....Mo.....E9..2lq...~H.B\.H..8...&..../.4.k..*6..]R.;.X..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	12566
Entropy (8bit):	5.46215752249084
Encrypted:	false
SSDEEP:	192:8iApwYKUa9u5vocJJBA1UwgZCwm5Mi0+Sozl/:83pw9dk9JO1UUwmR0+Sox/
MD5:	8BB17678DC8EDB536B2B8DEA5F6BFAE9
SHA1:	133E85FDDE914C9DB6C218DD63F9D413707AE1FE
SHA-256:	980641405328B10D2A139A08B58AA4F730D97B0E7D21DBCAA6BDEFC7443CD931
SHA-512:	264692E260404DB6762919333988259E981EEE15121197AC04429B6138D1845609327181954E9BF8A8FF71ED30232A1A1ED7946F3249AF4A9A0F8948034EF737
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\NUEPGTR9\unnamed[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 18 x 18, 8-bit gray+alpha, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\unnamed[1].png	
Size (bytes):	157
Entropy (8bit):	5.991001064175712
Encrypted:	false
SSDEEP:	3:yionv//thPlhl/ZiFtnW4t87t/F0kAtgnWhLNxKxLKsjamm0gMFaip8xoEmzO9Pz:6v/lhPi3WzW1UKsjrDgfAg2SVp
MD5:	8396B6E584F392180CDA492103C95602
SHA1:	AC67D383E68BFB641DDB2ADDD8F7CDBC53D6953A
SHA-256:	2E55B281F88F75BDB6B3F23F5F7D68CFF2F6988FDDBB7C0E9B9FB3751C49D440
SHA-512:	92FAE1AAFEDD97A4F71CC77B453315693BA7F04229EA2C00FB7B8293FC4E26C6BAC174B6C792BF374A44203F22F6A02EA652542C5AAA8C1E419CAE44E7FCFDE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/oLoRPrHJd7m46sWijX6zBWnEnfslP62AxJSwt5Nj0bNbpaYHz2pyscExleiofsH2kQ=w18-h18
Preview:	.PNG.....IHDR.....F.....sBIT..U.F....VIDAT(.c`.+`D....Oe`..=i#.(.."..&i&i..TQ.T...L.....P.....1.+aMb64.>..Y....XG....I6..@....^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\unnamed[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	288
Entropy (8bit):	6.7881820600030744
Encrypted:	false
SSDEEP:	6:6v/lhPW/CsDOsQSwS+pusToPVzqj0x9up:6v/7uzIu70jB
MD5:	E14A6794738FB4065E4B6A744206F223
SHA1:	AF6B63420BEBC1DE814AC0F7F1617AFFD3E411DC
SHA-256:	BDE575738A7B0EC443CC66157705EEB2A64938306E979F8693C12EDC9F6644A5
SHA-512:	C51AF36F020977F780473E1C2BFBEB6D4C49ED1A73CC64FC902956CB41219ADB2B2CB922C63AF07328EFB578FAC25D587824307DE1FA5716AF2B032FD878918
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/SaY5lqCwN7kppnS546l9ys-E2sZftTTIHjBrdV-WsGPIhGjaxcEXjfgdIfW_UNG7Sw0=h18
Preview:	.PNG.....IHDR.....V.W....sBIT....|.d.....IDAT8.c`....3....P]ww.H....n..H. &\.222Q,,,.....{---....C,,,..;..,.....?....\...%...B..c.q.e$.h.....LLL....[.....M..0.....b.....eaaq..... ..@..*..^.....4(??....."../.....S..Q.....>.g^.2....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\unnamed[3].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3279
Entropy (8bit):	7.715641786855708
Encrypted:	false
SSDEEP:	48:yqQvnLtkzdjmJJ3hAk+dJa9XrVmdGeNXCZ4o6w+Zv4lUWVV4c/952ql7mHiGJ4JU:7Q89mek+dJjnXno/++WSx1Vc/KWoxO/
MD5:	039E5B669C976EAA7569F9FA8ED813BE
SHA1:	1B5E33D16FC2A26B9318DFEAD0FEC938C5A0C98F
SHA-256:	265FE691B1687E0D18A34D33B5958C1A72E4CCB7D90BF3C70311B6DD4BAE13B6
SHA-512:	D9E8934419FC9E0A34CCDE0EEE3D8BC5435A95C4A72D50F9F8F1B3063C54AC6DB97E30B68ED8CD8CB37B5B73AD7400DC6585864E349B0893210B6152F084853
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh4.ggpht.com/WnIr0x3yhEpMTqI4DCrI_ZOc9vdK_yV0WPig_suRjHQCv4B-2CmQoQu3nE-Eo7_MZ-yZQbq30w=w72
Preview:	.PNG.....IHDR...H...H.....U.G....tEXtSoftware.Adobe ImageReadyq.e<...hiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:01801174072068118 22ABF5C578297F4" xmpMM:DocumentID="xmp.did:FAD30A79931D11E290ACA48D7B31C326" xmpMM:InstanceID="xmp.iid:FAD30A78931D11E290ACA48D7B31C326" xmp:CreatorTool="Adobe Photoshop CS6 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:01801174072068118 22ABF5C578297F4" stRef:documentID="xmp.did:01801174072068118 22ABF5C578297F4"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>*.P=....IDATx..[l....?J.....4.l'..Rb..f]..-.(Z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\13062c65605335a46d14656c46af3868[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	12178
Entropy (8bit):	5.047868477962458
Encrypted:	false
SSDEEP:	192:hC5CW/p5sraARO646QfW62lBHTKqB7BIh6k4o:cx/ptB9WLlBHVB7Btg
MD5:	13062C65605335A46D14656C46AF3868

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\13062c65605335a46d14656c46af3868[1].svg	
SHA1:	E9F0C2B7DDA37E448C75EDA6B6A57188ECC59F55
SHA-256:	70472A3B23DDA5B98B7A887D12AE8D7979EA8A53EC1955C237F62D6A86A14780
SHA-512:	B3340EE18D7C067D11B9806605CE214E1907CFDEFD3D2B5A3B6829A83D2859CAF35FDB884E033DA423C30A1FB4F7733464D9847E025F5929A67FF92A68109823
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/13062c65605335a46d14656c46af3868.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="30" y1="165" x2="56" y2="165" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="815.315" y1="-230.563" x2="857.315" y2="-230.563" gradientTransform="translate(-664.532 550.377) rotate(-15)" gradientUnits="userSpaceOnUse">. <stop

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\4165cd3aa643abb80fe1953668f67551[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	21529
Entropy (8bit):	5.054443624807617
Encrypted:	false
SSDEEP:	192:X60/6I3ppwx5qaqdT0TM2uTQOi4Rsd22Z1CrTqtqj3UGs8GsCv31Y9YUxzfmUY:/3ppwx5ncTBRsd22Z1CrT8u3M3unY
MD5:	4165CD3AA643ABB80FE1953668F67551
SHA1:	5CB99354ADCF5162232CF6947AEA1423426CF12F
SHA-256:	F3FF1A6BB6153FA3F31FC17B1A8E57F835BB0DA7A9EB6430CFF660A02DEE7E54
SHA-512:	070292AB655F2879879DF09306E5F57BFFCD075B7CBEA27156DD19D981B6E40F441C5DE05EF40DB0AFDB1D6294B4E02A0C304E5E67C4EC4F9011483C0FF7BD A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/policies/privacy/4165cd3aa643abb80fe1953668f67551.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="360" height="204" viewBox="0 0 360 204">. <defs>. <linearGradient id="linear-gradient" x1="240" y1="94" x2="316" y2="94" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#9aa0a6" stop-opacity="0"/>. <stop offset="0.15" stop-color="#9aa0a6" stop-opacity="0.025"/>. <stop offset="0.306" stop-color="#9aa0a6" stop-opacity="0.1"/>. <stop offset="0.464" stop-color="#9aa0a6" stop-opacity="0.225"/>. <stop offset="0.624" stop-color="#9aa0a6" stop-opacity="0.4"/>. <stop offset="0.786" stop-color="#9aa0a6" stop-opacity="0.626"/>. <stop offset="0.946" stop-color="#9aa0a6" stop-opacity="0.898"/>. <stop offset="1" stop-color="#9aa0a6"/>. </linearGradient>. <linearGradient id="linear-gradient-2" x1="272" y1="68" x2="272" y2="72" gradientUnits="userSpaceOnUse">. <stop offset="0" stop-color="#bdc1c6"/>. <stop offset="1" stop-color="#bdc1c6" st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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/v16/4UaGrENHsxJlGDuGo1OIlL3Owpg.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\PEJLKQA8\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].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

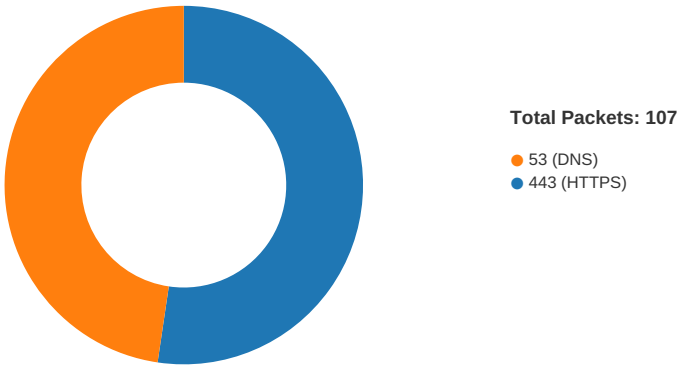
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
SHA1:	A33B906ECF28D62EFE4941521FDA567C2B417E4E
SHA-256:	F8F2046A2847F22383616CF8A53620E6CECDD29CF2B6044A72688C11370B2FF8
SHA-512:	ED9C3EEBE1807447529B7E45B4ACE3F0890C45695BA04CCCB8A83C3063C033B4B52FA62B0621C06EA781BBEA20BC004E83D82C42F04BB68FD6314945339DF2A
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

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 17:08:34.194210052 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.195074081 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.215495110 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.215665102 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.216223955 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.216315031 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.216917992 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.218683958 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.238046885 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.239434004 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.251301050 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.251365900 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.251415014 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.251440048 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.251457930 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.251486063 CET	49744	443	192.168.2.5	216.58.215.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 17:08:34.251494884 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.251518011 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.252156973 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.252202988 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.252233028 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.252240896 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.252254963 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.252281904 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.252290964 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.252331972 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.261540890 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.261929035 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.262151003 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.269376993 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.269809008 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.282598019 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.282630920 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.282658100 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.282707930 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.282730103 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.283231020 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.284077883 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.284113884 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.284141064 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.284184933 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.284210920 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.284214973 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.285598040 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.290684938 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.290728092 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.290766001 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.290786028 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.290808916 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.290836096 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.291413069 CET	49744	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:34.306693077 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:34.317727089 CET	443	49744	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.711570978 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.712450027 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.713519096 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.715490103 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.733196974 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.733222008 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.733239889 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.733293056 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.733328104 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.734008074 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.734216928 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.734240055 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.734287024 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.734313011 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.736632109 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.737261057 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.737294912 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.737343073 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.737369061 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.737833023 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.737895966 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.754726887 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.754751921 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:35.754803896 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.754848003 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:35.758431911 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.037748098 CET	49743	443	192.168.2.5	216.58.215.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 17:08:38.059952974 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.060023069 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.060111046 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:38.060157061 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:38.060264111 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.060328007 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.060332060 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:38.060396910 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:38.070589066 CET	49743	443	192.168.2.5	216.58.215.225
Nov 29, 2020 17:08:38.097201109 CET	443	49743	216.58.215.225	192.168.2.5
Nov 29, 2020 17:08:38.759720087 CET	49758	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.759932995 CET	49759	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.791430950 CET	443	49759	172.217.168.1	192.168.2.5
Nov 29, 2020 17:08:38.791476965 CET	443	49758	172.217.168.1	192.168.2.5
Nov 29, 2020 17:08:38.791580915 CET	49758	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.791630030 CET	49759	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.798542023 CET	49758	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.798574924 CET	49759	443	192.168.2.5	172.217.168.1
Nov 29, 2020 17:08:38.830050945 CET	443	49759	172.217.168.1	192.168.2.5
Nov 29, 2020 17:08:38.830280066 CET	443	49758	172.217.168.1	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 17:08:08.646522999 CET	65447	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:08.673852921 CET	53	65447	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:09.488183022 CET	52441	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:09.515202045 CET	53	52441	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:10.378953934 CET	62176	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:10.406229019 CET	53	62176	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:13.279988050 CET	59596	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:13.315804958 CET	53	59596	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:14.042866945 CET	65296	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:14.078752041 CET	53	65296	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:14.359980106 CET	63183	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:14.419034958 CET	53	63183	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:14.655994892 CET	60151	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:14.699290037 CET	53	60151	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:14.841598988 CET	56969	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:14.868813038 CET	53	56969	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:16.973553896 CET	55161	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:17.009171009 CET	53	55161	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:17.128654957 CET	54757	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:17.155821085 CET	53	54757	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:17.620886087 CET	49992	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:17.656656027 CET	53	49992	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:17.946502924 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:17.982332945 CET	55016	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:17.990112066 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:18.025902033 CET	53	55016	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:18.130084038 CET	64345	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:18.173713923 CET	53	64345	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:20.748404980 CET	57128	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:20.775429010 CET	53	57128	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:21.936532021 CET	54791	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:21.963494062 CET	53	54791	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:22.749875069 CET	50463	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:22.777086020 CET	53	50463	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:31.883946896 CET	50394	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:31.919445992 CET	53	50394	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:33.283711910 CET	58530	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:33.310842037 CET	53	58530	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:33.504304886 CET	53813	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:33.547818899 CET	53	53813	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 17:08:34.149035931 CET	63732	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:34.190063953 CET	57344	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:34.192687035 CET	53	63732	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:34.215620995 CET	54450	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:34.230051041 CET	53	57344	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:34.253119946 CET	53	54450	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:34.728281975 CET	59261	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:34.772332907 CET	53	59261	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:34.887789011 CET	57151	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:34.931246996 CET	53	57151	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:35.009238005 CET	59413	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:35.048738956 CET	53	59413	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:35.294655085 CET	60516	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:35.336653948 CET	51649	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:35.338124990 CET	53	60516	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:35.380402088 CET	53	51649	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:38.713103056 CET	65086	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:38.757160902 CET	53	65086	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:38.835452080 CET	56432	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:38.878964901 CET	53	56432	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:40.739065886 CET	52929	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:40.782344103 CET	53	52929	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:43.267889023 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:43.306114912 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:43.630779982 CET	61004	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:43.666173935 CET	53	61004	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:43.962599039 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:44.000076056 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:44.287682056 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:44.323275089 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:44.965490103 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:45.000961065 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:45.289972067 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:45.317209959 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:45.974076986 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:46.009759903 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:47.293706894 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:47.329061031 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:47.660515070 CET	62372	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:47.696392059 CET	53	62372	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:47.743899107 CET	61515	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:47.787527084 CET	53	61515	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:47.977827072 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:48.013782024 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:51.298146963 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:51.333715916 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:52.027869940 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:52.063153028 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:57.156059980 CET	56675	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:57.193587065 CET	53	56675	8.8.8.8	192.168.2.5
Nov 29, 2020 17:08:58.140034914 CET	57172	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:08:58.187412024 CET	53	57172	8.8.8.8	192.168.2.5
Nov 29, 2020 17:09:24.875837088 CET	55267	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:09:24.912924051 CET	53	55267	8.8.8.8	192.168.2.5
Nov 29, 2020 17:09:26.431653023 CET	50969	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:09:26.475311995 CET	53	50969	8.8.8.8	192.168.2.5
Nov 29, 2020 17:09:36.162564993 CET	64362	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:09:36.189755917 CET	53	64362	8.8.8.8	192.168.2.5
Nov 29, 2020 17:09:37.717152119 CET	54766	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:09:37.752620935 CET	53	54766	8.8.8.8	192.168.2.5
Nov 29, 2020 17:09:56.312675953 CET	61446	53	192.168.2.5	8.8.8.8
Nov 29, 2020 17:09:56.339838982 CET	53	61446	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 17:08:17.982332945 CET	192.168.2.5	8.8.8.8	0x3b1b	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:34.149035931 CET	192.168.2.5	8.8.8.8	0x4c95	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:38.713103056 CET	192.168.2.5	8.8.8.8	0x986c	Standard query (0)	lh4.ggpht.com	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:38.835452080 CET	192.168.2.5	8.8.8.8	0x9425	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:47.660515070 CET	192.168.2.5	8.8.8.8	0xc37b	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:47.743899107 CET	192.168.2.5	8.8.8.8	0x5069	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Nov 29, 2020 17:09:56.312675953 CET	192.168.2.5	8.8.8.8	0x49d7	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 17:08:18.025902033 CET	8.8.8.8	192.168.2.5	0x3b1b	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:08:34.192687035 CET	8.8.8.8	192.168.2.5	0x4c95	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:08:34.192687035 CET	8.8.8.8	192.168.2.5	0x4c95	No error (0)	googlehosted.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:38.757160902 CET	8.8.8.8	192.168.2.5	0x986c	No error (0)	lh4.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:08:38.757160902 CET	8.8.8.8	192.168.2.5	0x986c	No error (0)	photos-ugc.l.googleusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:38.878964901 CET	8.8.8.8	192.168.2.5	0x9425	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:08:47.696392059 CET	8.8.8.8	192.168.2.5	0xc37b	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:08:47.696392059 CET	8.8.8.8	192.168.2.5	0xc37b	No error (0)	pagead46.l.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Nov 29, 2020 17:08:47.787527084 CET	8.8.8.8	192.168.2.5	0x5069	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:09:56.339838982 CET	8.8.8.8	192.168.2.5	0x49d7	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 17:09:56.339838982 CET	8.8.8.8	192.168.2.5	0x49d7	No error (0)	stats.l.doubleclick.net		74.125.128.157	A (IP address)	IN (0x0001)
Nov 29, 2020 17:09:56.339838982 CET	8.8.8.8	192.168.2.5	0x49d7	No error (0)	stats.l.doubleclick.net		74.125.128.154	A (IP address)	IN (0x0001)
Nov 29, 2020 17:09:56.339838982 CET	8.8.8.8	192.168.2.5	0x49d7	No error (0)	stats.l.doubleclick.net		74.125.128.155	A (IP address)	IN (0x0001)
Nov 29, 2020 17:09:56.339838982 CET	8.8.8.8	192.168.2.5	0x49d7	No error (0)	stats.l.doubleclick.net		74.125.128.156	A (IP address)	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
Nov 29, 2020 17:08:34.251457930 CET	216.58.215.225	443	192.168.2.5	49744	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 Nov 03 08:37:44 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:37:44 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Nov 29, 2020 17:08:34.252281904 CET	216.58.215.225	443	192.168.2.5	49743	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 Nov 03 08:37:44 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:37:44 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		
Nov 29, 2020 17:08:38.842801094 CET	172.217.168.1	443	192.168.2.5	49759	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 Nov 03 08:37:44 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:37:44 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		
Nov 29, 2020 17:08:38.843624115 CET	172.217.168.1	443	192.168.2.5	49758	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 Nov 03 08:37:44 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:37:44 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		
Nov 29, 2020 17:08:47.775830984 CET	172.217.168.2	443	192.168.2.5	49766	CN=*.g.doubleclick.net, 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 Nov 03 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 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		
Nov 29, 2020 17:08:47.776972055 CET	172.217.168.2	443	192.168.2.5	49767	CN=*.g.doubleclick.net, 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 Nov 03 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 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
Nov 29, 2020 17:09:56.391330004 CET	74.125.128.157	443	192.168.2.5	49780	CN=*.g.doubleclick.net, 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 Nov 03 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 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		
Nov 29, 2020 17:09:56.392396927 CET	74.125.128.157	443	192.168.2.5	49781	CN=*.g.doubleclick.net, 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 Nov 03 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 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: 5776 Parent PID: 792

General

Start time:	17:08:12
Start date:	29/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff627780000
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: 244 Parent PID: 5776

General

Start time:	17:08:13
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5776 CREDAT:17410 /prefetch:2
Imagebase:	0x12f0000
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