

ID: 432846
Cookbook: browseurl.jbs
Time: 20:51:06
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://sites.google.com/view/tribridgeresidential/home 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 4
Signature Overview 4
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 10
Static File Info 40
No static file info 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 40
UDP Packets 41
DNS Queries 41
DNS Answers 41
HTTPS Packets 42
Code Manipulations 45
Statistics 45
Behavior 45
System Behavior 45
Analysis Process: iexplore.exe PID: 6784 Parent PID: 800 45
General 45
File Activities 45
Registry Activities 45
Analysis Process: iexplore.exe PID: 6888 Parent PID: 6784 45
General 45
File Activities 46
Registry Activities 46
Disassembly 46

Copyright Joe Security LLC 2021

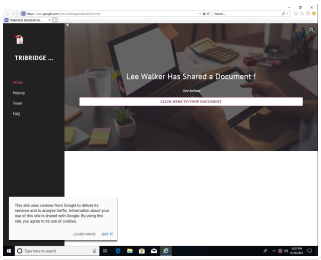
Analysis Report https://sites.google.com/view/tribridger…

Overview

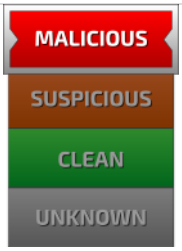
General Information

Sample URL:	http://https://sites.google.com/view/tribridgeresidential/home
Analysis ID:	432846
Infos:	

Most interesting Screenshot:



Detection



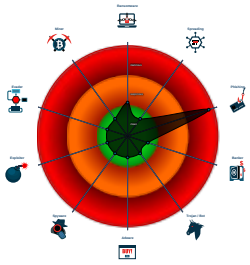
HTMLPhisher

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish20
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6784 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6888 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6784 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\index[1].htm	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	0x10a5:$x1: 78 34 4E 7A 52 63 65 44 63 77 58 48 67 0x10b5:$x1: 78 34 4E 7A 52 63 65 44 51 79 58 48 67 0x10c5:$x1: 78 34 4E 6A 5A 63 65 44 59 32 58 48 67 0x10e9:$x1: 78 34 4E 6D 52 63 65 44 63 77 58 48 67 0x110d:$x1: 78 34 4E 6A 46 63 65 44 5A 6A 58 48 67 0x1121:$x1: 78 34 4E 6A 6C 63 65 44 5A 6C 58 48 67 0x1131:$x1: 78 34 4E 6A 46 63 65 44 5A 6A 58 48 67 0x1141:$x1: 78 34 4E 6A 52 63 65 44 49 77 58 48 67 0x1151:$x1: 78 34 4E 6D 5A 63 65 44 5A 6B 58 48 67 0x1161:$x1: 78 34 4E 7A 4A 63 65 44 59 31 58 48 67 0x1171:$x1: 78 34 4E 7A 4E 63 65 44 59 35 58 48 67 0x1181:$x1: 78 34 4E 6D 56 63 65 44 49 77 58 48 67 0x1191:$x1: 78 34 4E 6A 56 63 65 44 63 30 58 48 67 0x11b5:$x1: 78 34 4E 7A 4A 63 65 44 5A 6D 58 48 67 0x11c5:$x1: 78 34 4E 6D 5A 63 65 44 63 30 58 48 67 0x11e9:$x1: 78 34 4E 6A 56 63 65 44 5A 6C 58 48 67 0x1221:$x1: 78 34 4E 6A 56 63 65 44 59 7A 58 48 67 0x1231:$x1: 78 34 4E 6D 52 63 65 44 63 77 58 48 67 0x1241:$x1: 78 34 4E 6A 56 63 65 44 63 7A 58 48 67 0x1255:$x1: 78 34 4E 6D 46 63 65 44 5A 6D 58 48 67 0x1279:$x1: 78 34 4E 6A 6C 63 65 44 59 32 58 48 67

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\2WF3MMUU\home[1].htm	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\2WF3MMUU\home[1].htm	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Phishing:



Phishing site detected (based on shot template match)

Yara detected HtmlPhish10

Yara detected HtmlPhish20

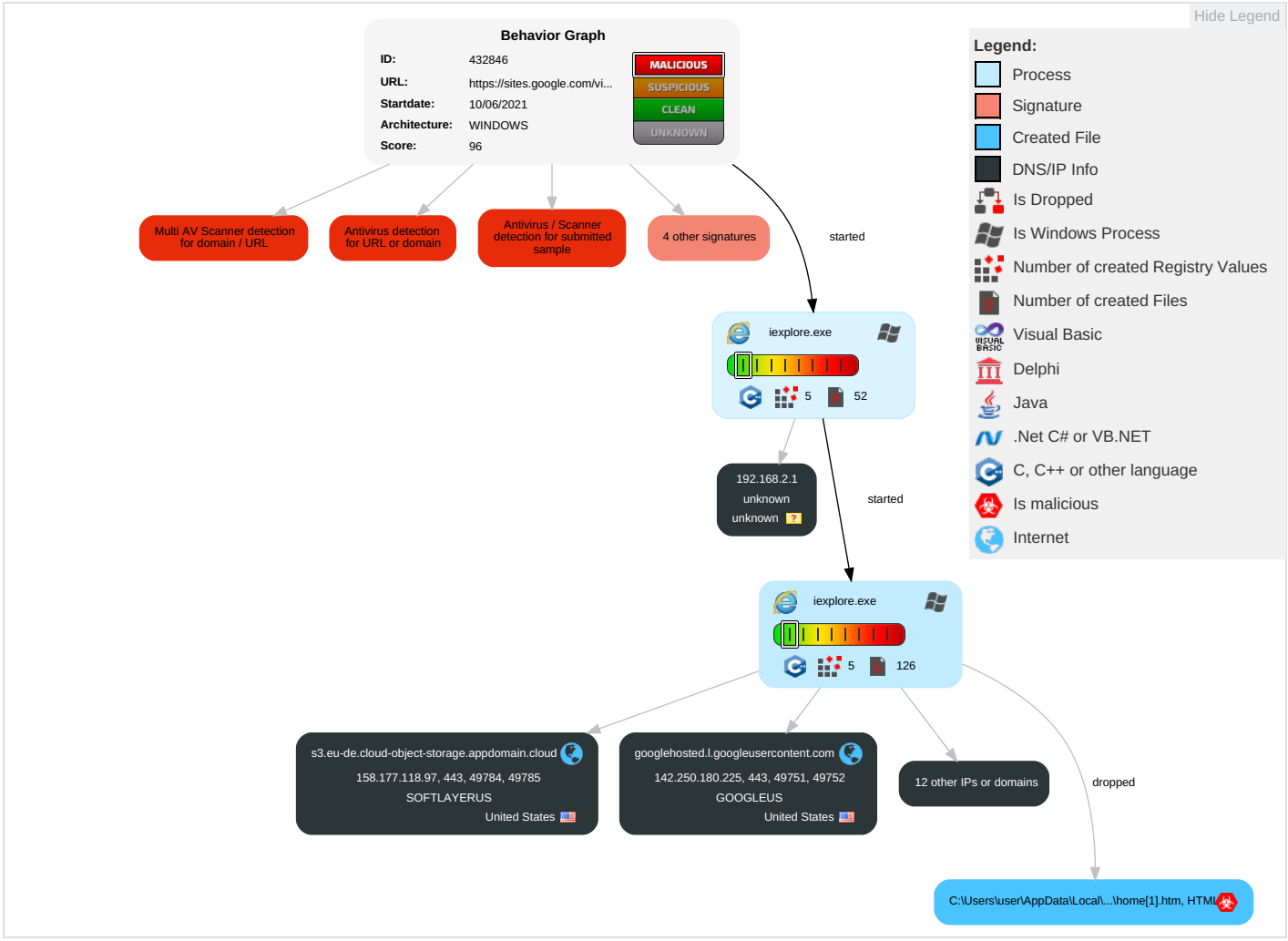
Yara detected HtmlPhish7

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	Impac
Valid Accounts	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	Modif Syste Partiti
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	Devic Lockc
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	Delet Devic Data

Behavior Graph

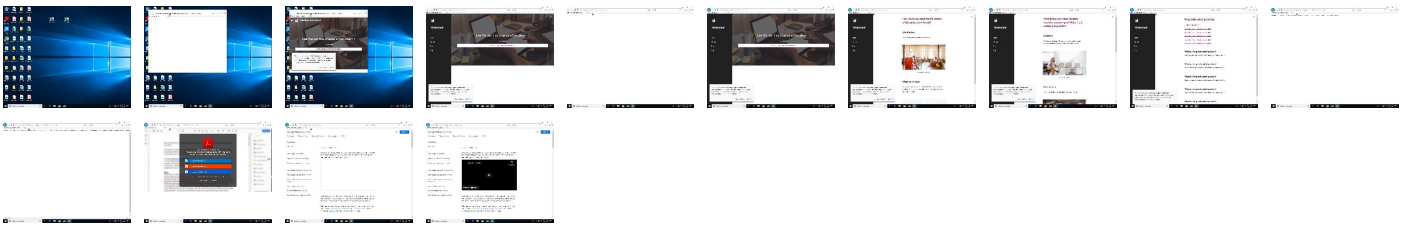
Copyright Joe Security LLC 2021

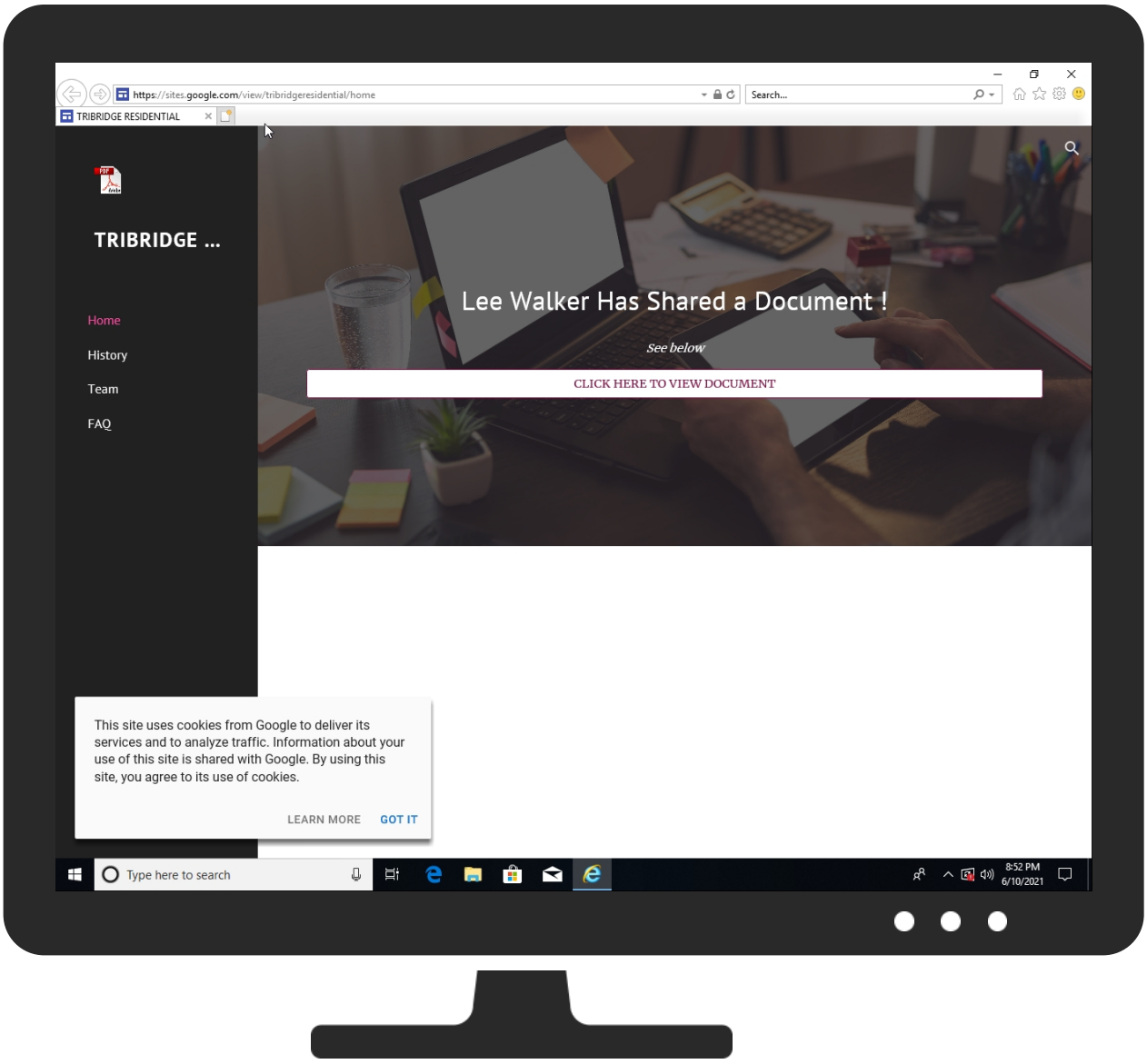


Screenshots

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://sites.google.com/view/tribridgeresidential/home	1%	Virustotal		Browse
http://https://sites.google.com/view/tribridgeresidential/home	0%	Avira URL Cloud	safe	
http://https://sites.google.com/view/tribridgeresidential/home	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://sites.goo/home	0%	Avira URL Cloud	safe	
http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html$Share	0%	Avira URL Cloud	safe	
http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html	6%	Virustotal		Browse
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://kanaan.s3.eu-de.cloud-object-storage.appdomain.clouRoot	0%	Avira URL Cloud	safe	
http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.htmlpdomain.cloud%2Farc	0%	Avira URL Cloud	safe	
http://https://sites.gooRoot	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/css/hover.css	0%	Avira URL Cloud	safe	
http://https://sites.gooe.cloud-object-storage.appdomain.cloud/archaizes/index.htmlpdomain.cloud%2Farchaize	0%	Avira URL Cloud	safe	
http://https://sites.gooPH0	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/gmail.png	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/8.jpg	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://sites.google.c	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/outlook1.png	0%	Avira URL Cloud	safe	
http://https://sites.goo/policies/technologies/cookies/.cloud/archaizes/index.htmlpdomain.cloud%2Farchaizes	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/aol.png	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/outlook.png	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/office3651.png	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/other1.png	0%	Avira URL Cloud	safe	
http://ianlunn.github.io/Hover/)	0%	Avira URL Cloud	safe	
http://https://redux.js.org/api/store#subscribelistener	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://smtpro101.com/email-list/mnb/images/othermail.ico	0%	Avira URL Cloud	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://sites.gooom/view/tribridgeresidential/faqryRoot	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/onedrive25/finish.php	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://sites.gooom/view/tribridgeresidential/homeRoot	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/adobe.jpg	0%	Avira URL Cloud	safe	
http://https://smtpro101.com/email-list/mnb/images/office365.png	0%	Avira URL Cloud	safe	
http://https://sites.gooom/view/tribridgeresidential/teamryRoot	0%	Avira URL Cloud	safe	
http://https://sites.gooom/view/tribridgeresidential/historyRoot	0%	Avira URL Cloud	safe	
http://https://kanaan.s3.eu-d	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	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://smtpro101.com/email-list/mnb/images/yahoo.png	0%	Avira URL Cloud	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://https://sites.goo/url?q=https%3A%2F%2Fkanaan.s3.eu-de.cloud-object-storage.appdomain.cloud%2Farchaiz	0%	Avira URL Cloud	safe	
http://https://sites.gooe.com/technologies/cookieses/.cloud/archaizes/index.htmlpdomain.cloud%2Farchaizes%2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtpro101.com	172.67.194.129	true	false		unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
s3.eu-de.cloud-object-storage.appdomain.cloud	158.177.118.97	true	false		unknown
lh5.googleusercontent.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
lh6.googleusercontent.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown
lh3.googleusercontent.com	unknown	unknown	false		high
lh4.googleusercontent.com	unknown	unknown	false		high
www.youtube-nocookie.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html	true	• 6%, Virustotal, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
158.177.118.97	s3.eu-de.cloud-object-storage.appdomain.cloud	United States		36351	SOFTLAYERUS	false
172.67.194.129	smtpro101.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432846
Start date:	10.06.2021
Start time:	20:51:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Copyright Joe Security LLC 2021

Sample URL:	http://https://sites.google.com/view/tribridgeresidential/home
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.phis.win@3/92@12/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://sites.google.com/view/tribridgeresidential/home • Browsing link: https://sites.google.com/view/tribridgeresidential/history • Browsing link: https://sites.google.com/view/tribridgeresidential/team • Browsing link: https://sites.google.com/view/tribridgeresidential/faq • Browsing link: https://www.google.com/url?q=https%3A%2F%2Fkanaan.s3.eu-de.cloud-object-storage.appdomain.cloud%2Farchaizes%2Findex.html&sa=D&sntz=1&usg=AFQjCNFtCAAkiNvTTHSVzB-bKWDyK7FRUA • Browsing link: https://www.google.com/policies/technologies/cookies/
Warnings:	Show All

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

Copyright Joe Security LLC 2021

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.youtube-nocookie[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):	64031
Entropy (8bit):	4.9852506902309415
Encrypted:	false
SSDEEP:	192:XXaXQX4X0XCXQXWXiXWXYXevvFAvWvaaU:XKgoEyAGSGIb
MD5:	4828DF95C8291EE6EF4FB33F19DF1933
SHA1:	B07DEE925FA79CDB2C8F1E6FD3E8CF6820AC15DB
SHA-256:	DC5C66CE45B310EBAEE20EC8C5F9961ECC2EC0BC078F0ED9C226EF33FBCC98F6
SHA-512:	4016C7B73742AC95508E5B7B03E43D927495980CB8D8FF81C56271B91B28159A97E4A0D089E65A972F90892CC19142E1B44EED67BC260529914ADCCA6932DBB2
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="__sak" value="1" ltime="3376850944" htime="30891561" /></root><root></root><root><item name="__sak" value="1" ltime="3474360944" htime="30891561" /></root><root></root><root><item name="yt.innertube::nextId" value="{"data":2,"expiration":1623437569245,"creation":1623351169262}" ltime="3475360944" htime="30891561" /></root><root><item name="yt.innertube::nextId" value="{"data":2,"expiration":1623437569245,"creation":1623351169262}" ltime="3475360944" htime="30891561" /><item name="yt.innertube::requests" value="{"data":{"1":{"method":"log_event","request":{"context":{"client":{"hl":"en","gl":"CH","clientName":56,"clientVersion":"1.20210607.1.1","configInfo":{"appInstallData":"CPK+iYYGENO4rQU="}}},"events":[{

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{ECC508A0-CA1C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8547046990362086
Encrypted:	false
SSDEEP:	192:rQNZeUZER2DeWjntDifkE2zMG+BG4D9sfVE3jX:rK/9xpkVpFQq
MD5:	04F39B4D1BBF5D7B3054C38F8B14F677
SHA1:	4CF030287F5C9DA470B13522AB1AD8EBD7623A30
SHA-256:	E9D729F44FBF0523CA39583AB6BF86C5895FCA61544732646FB0032D7946BC2A
SHA-512:	7938D08E4F2EB13715BC4075EC7FDD5BE9B65BC41ADF02DFC0030D54FBC70E7DCAA2AFCA6C47C7BE8F7C0ED436F42E0812B361AFFB897436E7313D89FF971 37
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\{ECC508A2-CA1C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	185340
Entropy (8bit):	3.0442219594120887
Encrypted:	false
SSDEEP:	768:4vwmXzhf3hzPzaEAJUzmKAeCm67KLZrjHuiwUzmKAeCm67KLZrjHuif:1tj4mtj4f
MD5:	BE155C2BC8B2EA179874F0325FB4F8B2
SHA1:	5A680E4F885F50C459667789591D66DCFFF21681
SHA-256:	FA4E4E1C8F27B6CE09D57EB19B642F7932BB1A58B5D14BFDF6A769FB6654DE8B
SHA-512:	B40EAAB82DDDEC08C277F6DE09B0C2DB53988155252DAF4ADAC25BA453E8F7BBB10F6F8D2927820889145A018230B6A7B8DD288D98841C5BEB51D36A6C50B3 91
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\{F2CF8151-CA1C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5647069612888698
Encrypted:	false
SSDEEP:	48:IwgGcprhGwpaoG4pQUGrapbSCGQpK/oG7HpRvTGIpG:rEZ7Q46iBSKA7TNA
MD5:	ED8F2601CCFFDE54EEDAEE2606B83317
SHA1:	C14FDF1F3DCF7C66E3A6364D458EBF682C246CD7
SHA-256:	D9FFAE7A4D07C725D2DDE2FC0477AB57AC56FCCD44A7BB10F88ECBDF1B20236F
SHA-512:	B4FCE3A63951BF224D8271CB7FB9A5567A8507F0E86076AB8FB35D49E8DB605E4317A59FEE2EC3F04AA38550F6A8CEA37038CBD2E2CE12AB8C44E932CF7BE64A
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12634
Entropy (8bit):	3.8610775491303264
Encrypted:	false
SSDEEP:	96:ALvIJct+cP47v+rcqlBPG9fIJct+U47v+rcqlBPG9C:8vI6ttPqWceBPG9I6tjqWceBPGg
MD5:	0CB95DC09C89FA3D1C937071878C759E
SHA1:	A42D1FA77360847364890E341CD6CDA44A823A0F
SHA-256:	DB2467F687C142737169E329E7D8FF4F13868F4D1E8B1D3902ACEE3FE75A3D0C
SHA-512:	48811ECB3DE2116F97307A1A152AD76A6617B19A121C08BC89FFD74154A2ED06ABBA5F5CA3507AD2A5E48314E0DE38C2DD3BC49693163E42BC459172B04D1955
Malicious:	false
Reputation:	low
Preview:	7.h.t.t.p.s.:./.s.s.l...g.s.t.a.t.i.c...c.o.m./.a.t.a.r.i./.i.m.a.g.e.s./.p.u.b.l.i.c./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....P>..P>..P>..P>..P>..P>..P>..P>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3
Category:	downloaded
Size (bytes):	161118
Entropy (8bit):	7.5594351594508185
Encrypted:	false
SSDEEP:	3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ
MD5:	F17B5B1163EFB6D2D47DE6BAE6D3A9CD
SHA1:	6D6964B34BC44C6D2B106ADE1AE675985B96D012
SHA-256:	7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30
SHA-512:	7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/8.jpg
Preview:	......Exif..MM.*.....(.....1....".....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\adobe[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	30925
Entropy (8bit):	7.75667128400845
Encrypted:	false
SSDEEP:	768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL
MD5:	BE5274AF7D8BD25B8148A190FF515399
SHA1:	B8D0850FD92EE935287E17988B89E53607808C8C
SHA-256:	26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/adobe.jpg
Preview:	.....JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q.. ~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<.....T~g.....3$.=._.. IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1676769
Entropy (8bit):	5.581481887370015
Encrypted:	false
SSDEEP:	12288:aXm9FsvxMjQvcw1yzDBzem2mPMVBFxR7DwVQ0wud3Uql3rz:Ym9GvxMjQHCzem288BF37DwFwuVfl3rz
MD5:	F6DB6997C14E9815C1CCC0C5511BB765
SHA1:	C6F8BAE2B4976B468CA046608B949DC43BCE9119
SHA-256:	BE46404DF6D8F40E8787D034657072984F9F8DA178C033667BA21D23C179218C
SHA-512:	A5A3573401FE4EA6FD339870E2AA655059B9CCBFEDDF59C9B8725C59BAAFA6CC0039FD5ABFB8D582BA13FAA19735CD83915E49266D6F4EB38A52B4E9EB1902 A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube-nocookie.com/s/player/1fe59655/player_ias.vflset/en_US/base.js
Preview:	var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var ba,da,Gaa,ha,ia,ka,pa, qa,ra,ta,ua,va,wa,xa,Haa,Iaa,ya,Aa,Oaa,Ba,Ca,Da,Ea,Fa,Ja,Ka,Qaa,Raa,Ta,Ua,Va,Saa,Taa,Wa,Uaa,Xa,$a,Vaa,Waa,bb,ib,Xaa,pb,qb,Yaa,vb,sb,Zaa,tb,$aa,aba,bba ,Db,Fb,Gb,Hb,Kb,Mb,Nb,Qb,Wb,Yb,ac,bc,ec,gc,hc,eba,ic,jc,lc,uc,vc,xc,Cc,Ic,Jc,Nc,Lc,iba,lba,mba,nba,Rc,Sc,Uc,Tc,$c,cd,oba,pba,bd,qba,hd,id,jd,kd,ld,od,pd,qd,rd,t ba,sd,td,xd,yd,zd,Ad,Bd,Cd,Dd,Ed,Gd,Id,Jd,Ld,Md,Nd,vba,Od,Qd,wba,Sd,Td,Wd,Xd,Yd,Zd,ge,ie,le,pe,qe,ve,we,Ae,xe,Ce,Fe,Ee,De,Bba,ne,Ve,Pe,Qe,Xe,We,me,Ye, Dba,.bf,df,af,ff,gf,hf,jf,kf,lf,nf,of,pf,qf,Eba,wf,rf,yf,Bf,Cf,Fba,Ef,If,Hf,Jf,Kf,Lf,Mf,Nf,Of,Pf,Qf,Rf,Tf,Sf,Uf,Vf,Iba,Kba,Lba,Nba,Yf,Zf,$f,bg,cg,dg,fg,hg,ng,og,rg,Oba,ug,tg,vg,Pba ,Dg,Eg,Fg,Qba,Hg,Ig,Jg,Kg,Lg,Mg,Ng,Rba,Og,Pg,Qg,Sba,Tba,Rg,Tg,Sg,Vg,Wg,Zg,Xg,Vba,Yg,$g,ah,ch,bh,Xba,Wba,dh,Zba,Yba,$ba,gh,aca,ih,jh,kh,hh,lh,bca,mh,cc a,dca,oh,hca,ph,qh,rh,ica,th,vh,yh,Fh,Hh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[1].js	
Category:	downloaded
Size (bytes):	311448
Entropy (8bit):	5.529508875650321
Encrypted:	false
SSDEEP:	6144:xy6OfHp1RkzVclge9naBnzzcSgHYPQCLcOPvBfzuD:xyDxsVcf+g1O6
MD5:	96DBF8E527CB14D82E294328ABCDA48B
SHA1:	1D10004482E6834A72716425F26D0C43C427A35D
SHA-256:	7BEF45A2D66E62100D6A4DAD1B713DDE1DEF59A7B963618E1D96C56593BE00EC
SHA-512:	915867AA98685F359253A11F28A90E6C69FD0F9BEDE89B52ECC6510775ED7E43625A34C9AA5973125EAE8BE4147FC770CDF34ABDA3030B96820A3005A2DEA95
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_US.p7L79FLXQCw.O/m=client/rt=j/sv=1/d=1/ed=1/am=AQ/rs=AGLTcCO6hl1EejjzC-wrWbDdgTxPi0Gs8g/cb=gapi.loaded_0
Preview:	gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,na,pa,wa,Aa,Da,Oa;_.ha=function(a){return function(){return _.ca[a].apply(this,arguments)}};_.ca=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.na=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");};pa=na(this);wa=function(a,b){if(b)a:{var c=pa;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ka(c,a,{configurable:!0,writable:!0,value:b})}};.wa("Symbol",function(a){if(a)return a;var b=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\client[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12537
Entropy (8bit):	5.463657559601543
Encrypted:	false
SSDEEP:	192:8iApwYKUa9uVvQcJJBA1lgi7Cwm5Mi0+SczI+J:83pw9dIVJO1lEwmR0+Scx+J
MD5:	CADBEC618439D646834E3C71301A49F0
SHA1:	9CAC182E930D49C0DBCEEE7045D1295D716C525C
SHA-256:	DA1A63A10B52159D228C2E42EA36B941811F9F33B2F8367F32369E51ED59B75E
SHA-512:	5D82B05B9B4FFE460EB91FCD6B1EB694E85F3F58B0C85EDA62489D18DDF66E9DA581831C557C73EE6A96CF41E44C41377B24E93A8678A6B79361C90A20384FDB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/client.js?onload=gapiLoaded
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\2WF3MMUU\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	2.3710475547263856
Encrypted:	false
SSDEEP:	6:RlMRQ8W828W828W828W828S8eftXfc/lk:Ry3X3X3X3XjeVUk
MD5:	EA69A3F95DD5484853D128186DB7E13D
SHA1:	5FDB5FE05108FD6E5386BBDA06778AF4B446DC6A
SHA-256:	8179E80BCFEF62154D1FF7371A1C60BD2C6C1E71C3DA2F4A8B1DB518A1900EC2
SHA-512:	2169D31065059C3677D025F27A5650C1E35BF83B6D6B3D80842B0809FF67E85388CB00213A4BD3FA76F71909A21298C824B39299A3980BA3B11C0297DB472610
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/atari/images/public/favicon.ico
Preview:	..... .h.....(..... ....@.....P>..P>..P>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[2].ico	
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\2WF3MMUU\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-nocookie.com/s/player/1fe59655/fetch-polyfill.vflset/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 files (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or sell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the 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, WHETHER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gmail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	66743
Entropy (8bit):	7.712342056984168
Encrypted:	false
SSDEEP:	1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:FsK2qezl0zoYxEuKo7CYrOb+Rb
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/gmail.png
Preview:	.PNG.....IHDR.....sBIT....|.d.....pHYs...../....tEXtSoftware.www.inkscape.org..<... .IDATx...{x.u.....I.sS..9Q(..J.L&.$..V\|.....#..''...Zw.eEQv.Q..U.A]9Vh..I8...H2)`....i.....).....f.y....L.pu...{n.....@Is..... mj=...X<65....U.l.b.t.U...mR...e..P.i.$.i2U..@N1.f...i.s...cf...../....2ev.`..%.|.o...s..j..l.B....V&..s;b..Pfg.....!...:..5....$.@...I0.=.IY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....P.....^".HL.M...@.p..;04....9.&.(i....9.sK..=&.'$m.....f..1..'...f2.Uww.....PH....@..xq....k.2..l.Luf..s5..`.|

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home[1].htm	
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	47716
Entropy (8bit):	5.774327712487098
Encrypted:	false
SSDEEP:	384:WCGYulh009w/PoLdy2i5D/E8+5qz+lhkD+DHq+Viv/+hhOWqWwSTdG+ng+qHPl1M:OYulK1JZ8jqAkoHRNOW/M+ngLM
MD5:	8692F7FE31E2925412EC2D58B1092D38
SHA1:	D2393D77D79A6CEA705B0F93034A33B880B259A0
SHA-256:	CD73A35207554B3854228C7220694C113CDFF53CB5C87C43F5F8DE8F4A54E773
SHA-512:	41891089F0095EE12A1D33F706581CE224A9AECB35DD5421409F4DF78AEE17378B43DD14B500843AED69758A3AF7BD3C186987E6253D38D7C2D9D86AC278AB8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_20, Description: Yara detected HtmlPhish_20, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_20, Description: Yara detected HtmlPhish_20, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="Hk7/OPglwkknAggOkCku1A">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="Hk7/OPglwkknAggOkCku1A">function _DumpException(e) {throw e;}</script><script nonce="Hk7/OPglwkknAggOkCku1A">_docs_flag_initialData={"atari-eiicg":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","ilcm":{"eui":"AHKXmL3SDWuqLQ11D51Nh-LdWogGxCQITxJKt-oGqmwgDjy4x-K8t_7KFTRV_a4Avl0ietDYjAKb","je":1,"sstu":1623351117377000,"si":"CMbhyZXejfECFWPBcwQdgn0NAg","gsc":null,"ei":[5720925,5720060,5703022,5703839,14101046,5704621,5734691,5713207,5713049,5711850,5714628,5721004,14101462,14101530,14100834,5722370,5712373,5732942,5719651,14101502,14101510,5735806,5706836,5706832,5713211,5709892,5711808,14101534,5712211,5729072,14101550,5707711,5734571,5727317,5708870,5714550],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\hover[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C378E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/css/hover.css
Preview:	/*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLunn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jizfRExUiTo99u79B_mh0O6tKw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 57524, version 1.1
Category:	downloaded
Size (bytes):	57524
Entropy (8bit):	7.989808002224364
Encrypted:	false
SSDEEP:	768:6k0bKY/R1FBhOX05AH6HINWEm370/gsvMtnPtKJiydtmih0V1r0TmJI3nOlKjj1j:6kKKYrFBhOE5AH6zrUEPtxNreO+j1j
MD5:	09D43F89EE9F28893C5D175F5EFF5045
SHA1:	27DF60E5879AA568876F747F3CFACF28564F9B09
SHA-256:	A1F431E4973D434EAD97B86815B31BB4553A7A3588FCD6D60D863C6150918F64
SHA-512:	AE41480C180523BC5E73A661B238E3E097DD63F02403A54C6015AA45E3D999726D7863AE35F51BDC13C2ED80D6866AD20D3B7D7F9E4AB67E49468D1C84FBF60C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ptsans/v12/jizfRExUiTo99u79B_mh0O6tKw.woff
Preview:	wOFF.....`.....GPOS.....^;.8.GSUB...X.....H{..OS/2.....X...`kx0.cmap...p.....cvt .....,...,.7.Rfpgm...(.....H.ogasp...8.....glyf...H.....>....hdmx.....,H5.Z.head.....6...6..(.hhea...0.....$.!..hmtx...P..".....cloca...t.....iR.}maxp...L... ... .name...l.....!r=0post...L.....r...prep.....#a.#x.l...d9..O..m.momac.m....jzl.g.J.....t...OZ1I...^S._+..S.....Fy.g.....b...+.E...*.;...~..|n.....UR.X%.A:.{,V..e./`Y.O.2...fl...D.M.U\%u...#zLO.i=...^....T_...Q;.W.uT'uQO..xM.DM....J.j5J?...B.L}=B..H..F.....u;..d.w.F.*.....W5.4.....I^..N.L.f{...q..v.m1..i.....E...j..i.....LQ?...{..7.q..oj....%.....C.\..s....;A....4...i.:.F....>DM.....4..3..K.3M.a.Wq...|.'B..(..r*.+ .)..U....=.|.>..1.....n.e}...G.U..<.<....[.B..i9...C....d~..O.3..C`(...0...x...a.L.y@6. ....+..^...'.....K.1~....9|._....>u.....>4...G.%...a...A0.F.(..ca*L..0...V.!.r.z*_..sh.F.j.....y..... ..A.dg..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jizfRExUiTo99u79B_mh0O6tKw[1].woff	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this, function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.c all(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,t oArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=Ae65rd,CuaHnc,sy1i,uY3Nvd,syj,syl,HYv29e,mxS5xe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	13557
Entropy (8bit):	5.44504001611651
Encrypted:	false
SSDEEP:	192:9Zrj87MVgromiAS/o7shcUspPudEI9A8p8XnRsHlTZeEeeh4N:9S7Mms/AS/o7shcUsWE8qXRsHlTD9h4N
MD5:	F51591533C2C7EF5C0321BA51E4D1867
SHA1:	CF9507BE04BE037FF200C05C6E1F54698C5D314D
SHA-256:	9917D466647F9DCA6E681F1C143433143O7AF9ADCBA065D759056C7BEDF5C991
SHA-512:	098E4AEA5AAE7A7F00F49D54E28AB8F6A47002FEF5C8302FEBE22E5404B66088EAE400A6C4062D9D156ED9BC8DEFC492BCA73A43976BE8F69F3EA81F3C743B AE
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("Ae65rd");.var tob=_.Ll("Ae65rd");.var n$=function(a){_.Mn.call(this,a.va);this.B= !1};_.G(n$,_.Mn);n$.ja=_.Mn.ja;_.g=n$.prototype;_.g.UG=function(){var a=this.O("haAclf").el();this.B="none"===_.Nm(a,"pointerEvents")};_.g.To=function(a){var b=this.aa(), c=this.O("haAclf").el();c="none"!==_.Nm(c,"display")&&null===_.vn(a.targetElement,".Znu9nd").el();var d=this.B&&c&&!_.wn(b,"CJIdie");c&&(b.Ma("CJIdie"),_.wc(thi s.O("haAclf"),"a").focus());d&&a.event.preventDefault();this.B=!1;return!0};_.g.Tr=function(){this.aa().Ka("CJIdie")};._.g.R7=function(){_.wc(this.aa(),".Znu9nd").Ma("eB4 8Hf")};_.g.Q7=function(){_.wc(this.aa(),".Znu9nd").Ka("eB48Hf")};_.g.j8=function(){this.aa().Ma("CJIdie")};_.g.A7=function(){this.aa().Ka("CJIdie")};_.O(n$.prototype,"SzA CGe",function(){return this.A7});_.O(n$.prototype,"jbFSOd",function(){return this.j8});_.O(n$.prototype,"dq0hvd",function(){return this.Q7});_.O(n$.prototype,"y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=FqLSBc,krBSJd,uiNkee,wmlPKb,lavLJc[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2933
Entropy (8bit):	5.32123751073728
Encrypted:	false
SSDEEP:	48:tyLTwf2wKSV3b9QrGIkVIMTMLG6AeamqS4MkxdVKO00PXDyQ/yrG:tyLsfxKmLyaJq0TrmqGAiy6OG
MD5:	2461C150BC64E235DE1902310E33655F
SHA1:	52FAE2F3D637ABA3FE8ACBFC731CAD1A4BD8322E
SHA-256:	C4E77B70ED382ECEFFF9F9232AE28C346DAF3E6C5F28F5002C1A4CB808C3386D
SHA-512:	E2F4E9E155C2D603862A532EF8F0E07AD5179BACB02AC85B1348FB80982A4636100BFA1B071CBC2CACCEF960317831905F7AE9201993B15A73A47002E49EC0F/
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=FqLSBc,krBSJd,uiNkee,wmlPKb,lavLJc[1].js	
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{._.n("sy7u");.._.t();.._.n("FqLSBc");.var F5=function(a){_.U.call(this,a.Aa);this.i=null};_.y(F5,_.U);F5.T=function(){return{}};F5.prototype.sl=function(a){a:{a=a.data;var b=this.v().H().getElementsByClassName("bCzwPe");b=_.v(b);for(var c=b.next();!c.done;c=b.next()){var d=c=c.value;if(d.href&&_.me(d.href,"#"+a)){a=c;break a}}a=null}a&&a!==this.i&&(this.i&&_.wj(this.i,"YySNWc"),(this.i=a)&&_.vj(this.i,"YySNWc"))};_.V(F5.prototype,"C1eaHb",function(){return this.sl});_.OI(_.jca,F5);.._.t();.._.n("krBSJd");.var B5=function(a){_.U.call(this,a.Aa)};_.y(B5,_.U);B5.T=function(){return{}};B5.prototype.bM=function(){var a=this.Ha("O1htCb").H().value;if(a){var b=new _.fu(this.getWindow().location);_.gu(b);b.Gd.set("hl",a);_.$e(this.getWindow().location,b.toString())}};_.V(B5.prototype,"msyOCf",function(){return this.bM});_.OI(_.ica,B5);.._.t();.._.n("wmlPKb");.var v4=function(a){_.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=sy1i,uY3Nvd,syj,syl,HYv29e[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10291
Entropy (8bit):	5.461521293037746
Encrypted:	false
SSDEEP:	192:37MVgromiAS/o7shcUspPudEI9A8p8XnRsHlTZeEe7:37Mms/AS/o7shcUsWE8qXRsHlTDQ
MD5:	FF48D9DB9AAC7EB98F95AFE49CC68C1D
SHA1:	838A667229554BA2165FCDAD753B5F1FC382EF02
SHA-256:	EA1E4218EC448407E6063F856790E79460DE2DDB805DA376BC7FF9C24B369060
SHA-512:	93D7E051253F9AB0F7704AF3A23D9F5E0163D0674DCAD24EA3C7DE762DB4791FF62A2F352F72BBFA3BA63726433342EBC509B2C83BB54C6A4B7CE56C5BA3F8E
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("sy1i");._.zF=function(a){this.F=a;this.H=this.D=this.C=null;this.B="NVegqd"};_.g=_.zF.prototype;_.g.kz=function(a){"NVegqd"==this.B&&(this.B="KWEn1",this.F.Rn(a.B,a))};_.g.lz=function(a){"KWEn1"==this.B&&(this.F.xq(a.B,_.Zm(a.event,a.B.el())),this.B="c9UNub",_.pl(function(){this.B="NVegqd"},10,this))};_.g.Gr=function(a){"NVegqd"==this.B&&(this.B="ysyYT",this.H=a,this.D=this.C=_.Zm(a.event,a.B.el()),_.pl(this.kZ,100,this))};_.g.Fr=function(a){return"NVegqd"!=this.B&&(this.C=this.C,this.D=_.Zm(a.event,a.B.el()),7<=_.Dh(this.D,this.C))?(this.B="NVegqd",!0):!1};_.g.Er=function(a){if("ysyYT"==this.B||"VML6Kd"==this.B||"KWEn1"==this.B)this.D=_.Zm(a.event,a.B.el()),"ysyYT"==this.B&&this.F.Rn(a.B),this.F.xq(a.B),this.B="c9UNub",_.pl(function(){this.B="NVegqd"},10,this)};_.g.kZ=function(){"ysyYT"==this.B&&this.D&&this.C&&(7>_.Dh(this.D,this.C)?(this.F.Rn(this.H.B,this.H),this.B="VML6Kd"):this.B="NVegqd")};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AA2YrTs7Zb87CqdFxEjh5qFvninf3C7moQ[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	101291
Entropy (8bit):	5.5497872842642035
Encrypted:	false
SSDEEP:	1536:8RDd/GTF32rgCwPJDOob5dtmH/P0RoDGjGOnxcWF3:q/GxGFoRmHF6jDxcY
MD5:	89908F7BA39B421A83B0BAAD77BED83E
SHA1:	53EC5B0578EF27E062AF9538A7C17316B723C8B8
SHA-256:	D231CD72051434824CCADD4CD4DF4556AD50296D738F4F0855A4275648E800EB
SHA-512:	36DE487E649408E5D82BF706945A60F629EE480B5814DEF8A6DD5208C101EF5EDB84ED38F1852DB46A7439039F0D6BFCFB905B041EF159BB8FC17EEF30A3882
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.*/.var Gj;_.Fj=function(a){this.j=a||{cookie:""}};_.h=_.Fj.prototype;_.h.set=function(a,b,c){var d=!1;if("object"===typeof c){var e=c.Tl;d=c.Ck||!1;var f=c.domain||void 0;var g=c.path||void 0;var k=c.hd}if(/[;=\s]/.test(a))throw Error("S`"+a);if(/[;\r\n]/.test(b))throw Error("T`"+b);void 0===k&&(k=-1);this.j.cookie=a+"="+b+(f?";domain="+f:"")+(g?";path="+g:"")+(0>k?"":0==k?";expires="+(new Date(1970,1,1)).toUTCString():";expires="+(new Date(Date.now()+1E3*k)).toUTCString())+(d?";secure":"")+(null!=e?";samesite="+e:"")};_.h.get=function(a,b){for(var c=a+"=",d=(this.j.cookie||"").split(";"),e=0,f;e<d.length;e++){f=(0,_.Wa)(d[e]);if(0==f.lastIndexOf(c,0))return f.substr(c.length);if(f==a)return""}return b};_.h.remove=function(a,b,c){var d=void 0!==this.get(a);this.set(a,"",{hd:0,path:b,domain:c});return d};_.h.lb=function(){return Gj(this).keys};_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AA2YrTtcf0OfTPFS7mDiDHvSrB_YVEoYtg[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):	5.192037061010406
Encrypted:	false
SSDEEP:	6:EZwTcqcA2n6gt9VvKcZWbnRVIM6RoeSjIUVY2rPs8QYMzY/:EZfqcA26gAcZWfp6SVYkUY/
MD5:	1B72E69FDEF1E3682A3EAFE2F5D81BDE
SHA1:	D4F2DAA025C2CF92332E5F5A2E692C6AC1C0512C
SHA-256:	296B72791199FCA038A621E32B7C6AD4EF056FE5C361BCA2797A06D6A0CC0AAA
SHA-512:	47677946F58903C4A903C4A1E8807E388A2470207A43F9FF55A3E9123FF20365D60652FA38AEB3EA5922A701900849AE401C75DE78A3935BFD308810E6474A84
Malicious:	false
Reputation:	low
Preview:	.gb_Qe{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_Hc .gb_Cc{overflow:hidden}.gb_Hc .gb_Cc:hover{overflow-y:auto}sentinel{}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AA2YrTtcf0OfTPFS7mDiDHvSrB_YVEoYtg[1].css	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\www-embed-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	197263
Entropy (8bit):	5.596066732874722
Encrypted:	false
SSDEEP:	3072:sIXX8qk/hze+DzkpASIy2QI82gEjlsk0pIIUrQaxc:qpze+DzkpASvPI82gEv0pl2
MD5:	43889017AAA093BD462EF758C267519A
SHA1:	ED2500E2E319B4C1C96CD8E14AA50B072CE5368F
SHA-256:	2DB1731278FEA4DC5E8BC660CCE5FB2E2DB61306A9F661C81547CF9D9F6593E7
SHA-512:	0A7F796EEC413B7EE6E3FB6703EE3E7D646241C28F5C2B852F3B47D45E96FE2F7DBE54B83641F21DEEBB73E8F77349BDD1D6FC8C9777B44159467BDBABBE78E3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube-nocookie.com/s/player/1fe59655/www-embed-player.vflset/www-embed-player.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var m;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 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");}.var da=ca(this);function r(a,b){if(b)a:{var c=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&&ba(c,a,{configurable:!0,writable:!0,value:b})}}.r("Symbol",function(a){function b(f){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c(d+(f||"")+"_"+e+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26180, version 1.1
Category:	downloaded
Size (bytes):	26180
Entropy (8bit):	7.9847487601205405
Encrypted:	false
SSDEEP:	768:axmLo3N7711ZHlB8N6yt/DvXjXjmDNzv6:bLodN78li7jKJv6
MD5:	4F2E00FBE567FA5C5BE4AB02089AE5F7
SHA1:	5EB9054972461D93427ECAB39FA13AE59A2A19D5
SHA-256:	1F75065DFB36706BA3DC0019397FCA1A3A435C9A0437DB038DAAADD3459335D7
SHA-512:	775404B50D295DBD9ABC85EDBD43AED4057EF3CF6DFCCA50734B8C4FA2FD05B85CF9E5D6DEB01D0D1F4F1053D80D4200CBCB8247C8B24ACD60DEBF3D739A4CF0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF.....fD.....GDEF.....\.....QGPOS.....#..+...QGSUB.....y.....m.OS/2...|...U...`h...cmap.....~n...cvt .....y.....fpgm.....uo..gasp.....glyf.....=...m...5head..Z....6...6..'.hhea..Z.... ...$.0.5hmtx..[.....).loca..].....y.....K.6maxp..`H... ... .=..name..`h.....r.i6Ppost..a.....i]\prep..d....p..... ..x.U....Q.F..=#.0ZD.@@<.....''...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.....x..Z..+..=Z...~.....0.8....r.\...=s&oG....q.Fg...Y...:Wc..>..p..p....).....{.aX..}.?.k... .....N.=.c.Do.....~2.=.i$....0..>..!.'v.....q.....>>.....o....30..0.w..|hR&mrf....,.Y.....%<..0.#.~...._a.c.....K.z...H1..u.2.Y_..0.9..`.,.:.=(.N~..*.a.<.D=....*.V....\..>./.B.`iE..A9.S.|?.g).Rj..8Q...h.y.G.^.kx.o.....(...#....9...,4I8...7..o.I|@x..1.>'...H.m..$.yp..f..%..F$0.0.I.1...WR...E..8?a..|''.....A.(...ZJ.q.K|...S.1..ht.ck....e...T.Zs,W..0..%.i.R...Ku.K.y.....j.RD..~..dpsh.fc.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Preview:	wOFF.....g.....GDEF.....q.....GPOS.....%..+...RGSUB.....y.....m.OS/2.....U...`i`..cmap.....~n...cvt .....fpgm...@.....uo..gasp..... ..glyf.....>F..m>Q..head..[\...6...6..'.hhea..[.... ...$...3hmtx..[.....<'3loca..^l...{....._{.maxp..`.... ... ....name..a.....V..4.post..a.....i]\prep..et.....^....x.D...Q...3..IX=D.@ @....@.....".}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....g...x.....6.E..8.....affff.0.B..&.L...B.Nzy..n.T.t~w&..%[.dYzzz.Oe" ..lE.....m..7[s}...[l..)..)... (H.A.@q.57..S.@.._..].*.j.-^N.R...'...]v.0..2n.6...~....X..xN.DN.T..b..*Q5.E.).,Ql.....M....6.P."..|..*.tl5.....t..r.(...{M..T}..@.kbNP.I*.9-...=E.U'.{.....p|.t..qJE.9...'...*...z...L./.....r nXQ.6.|.....n.V.....K.?.G...<..<..Q.....C..K(s.PR.x\(..P@.P..z.DL.1.$*../.8A.8Q.r.Pr[e.Rt+~.}9.)E.'.U..z.G..G..OH/H...L.../..{S...EP.%.....o.....uN...'.}%..9.F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UabrENHsxJlGDuGo1OIlLV154tzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26164, version 1.1
Category:	downloaded
Size (bytes):	26164
Entropy (8bit):	7.983292364847896
Encrypted:	false
SSDEEP:	768:L9QwjnXN11zY7+dePzz5Othh7STtySTygbOg9zp:L9pjz1kCePzQthJSYgbRp
MD5:	CCDA7B53E281A638F36ED62514815268
SHA1:	CF6D39BAB2A012D008EC9EDF95F4F4BDACF93770
SHA-256:	673F112749C21E5BE0D1338E1709A1D981053E239E98CE09D0BB849BB34FCD98
SHA-512:	20645A09B2FF157E50C71D862AA4FE6729FFD8BE18FB3D390B3714DEEC4F4FFF49FAC16EC509F8D620E476DC1942C67C95A95ABF14A06585F5B504FB4BE89F5 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UabrENHsxJlGDuGo1OIlLV154tzCwA.woff
Preview:	wOFF.....f4.....|.....GDEF.....q.....~GPOS.....#..+...UGSUB.....y.....m.OS/2.....U...`j(..cmap.....~n...cvt .....(...fpgm...`.....uo..gasp...(.....glyf...4 ..=...k....head..Z<...6...6.x'.hhea..Zt... ...$....hmtx..Z.....%.loca..] ...y.....%.maxp..._.... ... .name..._.....Z.L3.post..`d.....i]\prep..d$.....t...x.E.....E.}&$a.....A.. ...,....`..}. ...q....+o...9 ....B.J..WS..w2.{...o.D~!X.D:..Muq...[1 ..[.I...]..#-..0...x....+..E.pg....bfffffffff.0.+ef.5..N.0..K..r....Y...@..V.t.~.....[q....h+..y...1s.#.>.%....CX.,@.F..t.H..t..{.q.c.>..\?..J. ".J.+.M.L...!%..I\....<......_....M..-....7.BP.J.d2*.T..,G...*E?.Z.p..].w..=z....9.p{..<._O+*..r._...]U.]..?.r.JoQi..k..P...*.....=.X.:U.....\.....h.....r....L....J..Sn..<9..V..=.x=:x..x..yCr.#e.._. .o.>...s.<!M.....!..o....!....j.#$.:A..Bn.2.$.,..E...{...G_.....L.....jw..P.]!..wE.R..a..rK4...k.._.W24^...cuh..fTIH.Z.TJ....&.x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\EmbeddedImage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=3, description=Mockup image of male hands using a laptop computer and holing a smart phone both with blank whi, soft ware=Picasa], baseline, precision 8, 5472x3648, frames 3
Category:	downloaded
Size (bytes):	992111
Entropy (8bit):	7.925987674564042
Encrypted:	false
SSDEEP:	24576:BOVTzsogpJyZ30N9I1l+zOXC9Cr7fh74aaopUZmwJ:BNoIYEScuC9C3Zd/6
MD5:	087A6238EC6F45E5DDF220A02D97B01D
SHA1:	14762F8D4BF4A168812FC425914BA41AC16CCA58
SHA-256:	35823A90041E7E13F75C535AA7EAED0EA89EAFA9530B51556FBEA532727C5988
SHA-512:	19684C0B7B981A3892A3AA954F091AB0CA7D8E76F4E06B9302696FBF9C1EEA33528549C113791175DA9B48B81C7B24555B63EF1CD03CCFDB839298B4F459C41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh5.googleusercontent.com/NeL4dqnq9o5qsxTds1ViMOrR7QHEjqg59HxUNLbq_rcgDoWEOsnQ8VNmAgQCPmD8gc1O4tuNdzNMMdAM6EJPPvc=w16383
Preview:	.....JFIF.....Exif..II*.....2...1.....;.....Mockup image of male hands using a laptop computer and holing a smart phone both with blank white screens. Foc us on the index finger.Picasa.vladans.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" photoshop:Credit="Getty Images/iStockphoto"> <dc:description> <rdf:Alt> <rdf:li xml:lang="x-default">Mockup image of male hands using a laptop computer and holing a smart phone both with blank white screens. Focus on the index finger</rdf:li> </rdf:Alt> </dc:description> <dc:creator> <rdf:Seq> <rdf:li>vladans</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>...@ICC_PROFILE.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\EmbeddedImage[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=3, description=Mockup image of male hands using a laptop computer and holing a smart phone both with blank whi, soft ware=Picasa], baseline, precision 8, 5472x3648, frames 3
Category:	downloaded
Size (bytes):	992111
Entropy (8bit):	7.925987674564042
Encrypted:	false
SSDEEP:	24576:BOVTzsogpJyZ30N9I1l+zOXC9Cr7fh74aaopUZmwJ:BNoIYEScuC9C3Zd/6
MD5:	087A6238EC6F45E5DDF220A02D97B01D
SHA1:	14762F8D4BF4A168812FC425914BA41AC16CCA58
SHA-256:	35823A90041E7E13F75C535AA7EAED0EA89EAFA9530B51556FBEA532727C5988
SHA-512:	19684C0B7B981A3892A3AA954F091AB0CA7D8E76F4E06B9302696FBF9C1EEA33528549C113791175DA9B48B81C7B24555B63EF1CD03CCFDB839298B4F459C41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh5.googleusercontent.com/tK9WLr9doesqnl7t8y3sD70_snmPE15bl2VQ2aR8KfLCAS9cH921B3l7KOI6Goc1G7LtUO9jgqD6NVEUgLBpUPE=w16383

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\EmbeddedImage[2].jpg	
Preview:	......JFIF.....Exif..II*.....2...1.....;.....Mockup image of male hands using a laptop computer and holing a smart phone both with blank white screens. Focus on the index finger.Picasa.vladans.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" photoshop:Credit="Getty Images/iStockphoto"> <dc:description> <rdf:Alt> <rdf:li xml:lang="x-default">Mockup image of male hands using a laptop computer and holing a smart phone both with blank white screens. Focus on the index finger</rdf:li> </rdf:Alt> </dc:description> <dc:creator> <rdf:Seq> <rdf:li>vladans</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>...@ICC_PROFILE.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf..L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4.\name..M.....\|..9.post..N..... .m.dprep..N.....:z/.Wx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,....<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	842
Entropy (8bit):	5.166015224651512
Encrypted:	false
SSDEEP:	24:570OY7aTr70OYN0aTF7QMczOY7asMoczOYN0asMS:h0OEaTv0OpaTi/OEasMjOpasMS
MD5:	271F7F08583B0FF51B875073985EEF7A
SHA1:	F0CF1FFCD071B020D761C8B3B19FA27A811CB694
SHA-256:	CD2AB98D26494918A67D4D439CD43BFAC5040D52A2EA9995624AB9358EEE4513
SHA-512:	3E41C843F7B9724B76077BE24A6D26D0F0BD64010BCE42832E8DD0BE353665B45199BB436ABACA958CEC9155926DF8E8BCDD9C80867C40236D1E5EAA225448A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=PT%20Sans%3A400%2C700%7CMerriweather%3A400%2C700&display=swap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Preview:	@font-face {. font-family: 'Merriweather';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/merriweather/v22/u-440qyriQwlOrhSvowK_l5-fCZK.woff) format('woff');.}.@font-face {. font-family: 'Merriweather';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/merriweather/v22/u-4n0qyriQwlOrhSvowK_l52xwNZWMf8.woff) format('woff');.}.@font-face {. font-family: 'PT Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiTo99u79D0KEww.woff) format('woff');.}.@font-face {. font-family: 'PT Sans';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/ptsans/v12/jizfRExUiTo99u79B_mh0O6tKw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap
Preview:	@font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\faq[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):	62355
Entropy (8bit):	5.774316048490858
Encrypted:	false
SSDEEP:	1536:oTsWqAkoHR6lLs+QlrErnUBvEyW7Xt+TOY:oibLnQJErU9Ed7dzY
MD5:	61BD944BF3904654A75176D440CC4EED
SHA1:	AE4D4D96CFECCD9C090D9ECC279F662DEA6E5BB1
SHA-256:	48B722E0B0B28D5AC591E630B27F54954F81B668469C814DCBC03D43B65E9615
SHA-512:	5162E54E00731DE71218C11BDA9BA45138246F1943A0A03E07A6EA526B415FF3BBEF6954CE8A5D7CDD023E6695AE67D4B6A6E915B4C5AE3E85F8F3A1646FBBF6
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="sMyDtGSL4I0Ekr3d6hejfQ">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="sMyDtGSL4I0Ekr3d6hejfQ">function _DumpException(e) {throw e;}</script><script nonce="sMyDtGSL4I0Ekr3d6hejfQ">_docs_flag_initialData={"atari-eiicg":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","ilcm":{"eui":"AHKXmL2fMcr0xO3P03CS_5O5l6Eo02_tdJoRDt3S2tsr2mR_L7yA9OJefEpkQwsxrpT0BOev9iJ3","je":1,"sstu":1623351144566000,"si":"CMygxaLejfECFYTBHwod5eIEpA","gsc":null,"ei":[5711850,14101530,14101502,5713211,5735806,5703022,5732942,5706832,5719651,5734691,14101550,14101462,5709892,5703839,5721004,14101534,14100834,5734571,5707711,5720060,5706836,5729072,5708870,5714628,5711808,5722370,5720925,5714550,14101510,5712373,5712211,5713049,5713207,5727317,14101046,5704621],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	6DA56208801596342l3E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/policies/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].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\9026IKNJ\googlelogo_color_74x24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 74 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1622
Entropy (8bit):	7.861147443229629
Encrypted:	false
SSDEEP:	48:1iZ3jFWCXwymKs5AbKuyp/fvBheQdm+6QmWO:1iZ3ZWKZmKsCb0/fphH6QJO
MD5:	DE327BF69212B7255BBB0C8F40F52A3C
SHA1:	8C9E7517E6456E13F3F4640E39743B74F98B8F39
SHA-256:	0793CEFA320C6C622E8B143B35FAFB577BD7584C26796D3B5E1321463494FE76
SHA-512:	FDC82955CCBA3E9310CAC694197C43EB289CE9FFCB2A0784CCBAE0F3CEB5ADCF2F72D40C411290BDB6F3311E23321D13D3C2C6D20DC63E733A291A115E254 60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/images/branding/googlelogo/1x/googlelogo_color_74x24dp.png
Preview:	.PNG.....IHDR...J.....].k.....IDATx....t.h...Y.sww?../$p...../.'-....C...K..{?,m...73d.....\|z[..U..L./.....Zp.....<...D.....TZ.....^...a`.E.....}@'.i.3.s.\|&.....2nty...` .r.A._H..e.p.- ..`.'%.....a..31x>>..h....z.~.....(..6.....V^..P...@u.....;..y..FY....J.B>+.....p..R.r.X.....@..V...z.M....y..)..@v..Fe..O.-8.5u9..px.. \.k....@..r..[..Y.*-}.4E...B..l@..3.G6....j.. <.of...a{j..d.L.r....7..a.../.*@...Y.`.l.....9A....r..u..9.J..1ryC.....HOt.U....b.E..{3iC.-....&!X.,9.*.....d..!k6.....M4...I..#4.....*.&\|...c..?OS...*.\~..v.q.A.....*.....Q..2...@..G..P.x..@ .j....d..@....(.....'.....%....._..Y...k...n<wkE .Wk\.....P<...p.....\' d.@..X@...$.....z..N)?.....S., Q.T:...@..BMZ..Z...Y..@.J/X'.....:.P... ...'..X....`....6L?....3..)+...c.K..~)pF. .d..s....B0`).....si.#..J.-...cl...s<.....z$'.#./x.....%-...0.-.d.....x...+."."....N.b .....7....@EQ..W.ds....;.8J....^..9@.t.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\index[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:	downloaded
Size (bytes):	79854
Entropy (8bit):	5.593767947386851
Encrypted:	false
SSDEEP:	1536:5+X3iWGYjxXU5hvr4y/kLuOsNp+2Rjt2ZxVSQDZNUFaIQb88HYFpy7:2SWiYoQDZT88HYFpy
MD5:	C264B2395B1F9CF424E5A463BCD4D8F5
SHA1:	CC0FF42A956B3BB150431483B46EFCF0C3278EEA
SHA-256:	E1CC7F9DC3DF7A2C30B04C41B1C30B4A3462118EDFE9F82F3D4E465998EED645
SHA-512:	6917CE165B5039A4352AB96990D3C456B87278F96A98090A8AE5495C49AB5837138313CD48762114439 63A1A0E1169D43F1EFD16A784A77B831CF2049DC2D224
Malicious:	false
Yara Hits:	• Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\index[1].htm, Author: Florian Roth
Reputation:	low
IE Cache URL:	http://https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html
Preview:	<html><head></head><body><template id="b6f78523-5dab-43f3-96b8-cd7eafb7907a">eJzlW+ly2zgS/r9V+w4YJjWSJyGp27Zsecs57MSexIdyztb8gEiQhE0SDAHqyNY 80L7GPtk0QFIiKcrHZDI1rpVKF45Go9H9sQ/qn//Y/8FmllhEBHki8A+gQX4iH4fuSCOhploItuEToX1uxTQSiMfWSPOEiPjQNPEVnhsuY65PcES5YbFAtZk+nXDz6ktC4 oXZMTpGL/thBDQ0rrh2sG+m9DbTtphNjGyWpJt+1btGG545GTn7vvMlBZiLaCiIG1OxGGncw53+QO+csuvtN5OzxTxy33+YHl6br046V9Q9G38ed3By2jt3vk6C7eTVoDX SkBUzzlMXRqONByycBGwpLo1YO4HXUeX5EtCY2KjgAiMBHY50vV8gGqzPBxzIkZaIhx9Z7kz1RfigIy0KSWziMUCVmbAeghjZ9QW3sgmU2oRXf14CtuigmJf5xb2yaj9F HEvpuG1LpjuUDEKmaRdYO0ZY4KLGEfo+Xhc4MqHSSgmPkhHLHzCPUJgaS8mzkrGAZ5bdmhMchLyh5T1ssHsGS2jZVqcr9rU4UFL9QS6Oz39OOzDx/zLRRuzj 58On7T6O5efzufn7sBZ9F5/nL5767VedgbdT8GRdeKPD2f02D06/Gjah3Q8OPkUbD6V4q7Km3BAmryqxcDfvxwcUH8x+kx8n80Epv6PNuWRjxcjPsORtiacm7TxmgpDLoR nhLOAqDX6O/1Jq9/u9FN9vKs+CSp8cjAGfSHonIEM0VkI2yL7Ztqzeac8EFHM2q22Wp4EsCXdp1yYQThRZ+SxKYnTs1k7+YDYFANjvl9QIDUASQwZaYLMhaS SdmcDTDUitXJzBSYTZi9yRm06RZaPOR9pUrExbCXWHT+hdi7R8qCYzTSkyl60Cbau3Zgloa3TALtkiJLYbzbutGE1gZs7xlXkNrb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jizaRExUiTo99u79D0KEww[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55340, version 1.1
Category:	downloaded
Size (bytes):	55340
Entropy (8bit):	7.989968916631909
Encrypted:	false
SSDEEP:	1536:ue5xVbIMTbfPLQkpweWndVY7v1ceRxeAc2:u8zTIgwF+7vaMh
MD5:	7A9A412D3B5F0FCF44A43035EF5749EB
SHA1:	0515F781A37C8775C466577EC40AEF136CBCF3CB
SHA-256:	1EC30E5248358ADF73BA90108EB2978F9E3A4855EE52BB64BCF3FB1CEF68DE7C
SHA-512:	88D8F01D1A54CA65FDB45F3D83423A5115EE93C3604FF8E7ECDA525796347CD3A4B439716FE68CC48546476AC44B4118CF7F023149EC9C837C55BA9F124BDC(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jizaRExUiTo99u79D0KEww[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiTo99u79D0KEww.woff
Preview:	wOFF.....,.....|.....GPOS.....GSUB.....H{..OS/2.....Y...`jL..cmap...4.....cvt .....6...6...Lfpgm.....,.ogasp.....glyf.....4...hdmx...,.. .b..+\...,head.....6...6.(.hhea.....$....hmtx.....+.loca.....wp.maxp..... ... .name.....=5post.....\|.$R.prep...x..... x.....G.E.z.m...J.m.b.m....m[k.95 .Z.=u..uOcg.%Hj...F...{..j}.w..J.b..5{F..W.v.Z.=Kh..D.$.Lh.....%zKYZ..U.1.?./g.;....u...!:V..D.....U..U.B..{....Q.....~C?.}...e.H..<..\|.....F.CM.<.....e.....B..(t.h.....%....uE{.... ..3....mM.Bt..O^.....0w.....R.+t .. z\|.../A.{.....3..:....Bh....8..s.[.....G.<..(.Q0.....(5..Z...C.O.....].JW{.zx..{..y.....z..&.....Q.....v.....V.....}I....g...;....5.K...x.....qnP....x.,".>/$.]AW.[... .B6;.....K\...$.u..:.}..}.l2.W.2O%.*.4.Y....k.y;Z.[.5.?.=/RG!XVb...B.~N.0.Js.#T2.s..w..x..q.....j.T.D.Ce...AOV@)>...?.3..mtgKM.`.7..fo...s.k...co.-.v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=Ae65rd,CuaHnc,sy1i,uY3Nvd,kTx9td,syj,syl,HYv29e,mxS5xe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	14250
Entropy (8bit):	5.445303617225314
Encrypted:	false
SSDEEP:	384:9S7Mms/AS/o7shcUsWE8qXRsHlP2D9h4N:9SwX/AXYhEYp2D9h4N
MD5:	8FE1D19C55DACDA5606B58F79783E306
SHA1:	54BFB902C9EA61A7A5909D14D6085945A85E1BFD
SHA-256:	D5FD544BBA00FFC58C199DD00F90332EDF34DDAFD2FCD6E8A8125893E58AB14A
SHA-512:	EDE40CA422DF523D00A74C8386830B80564E682F944F618FE312CC48CB58E2B002CE9E24D3BA3234AB2D794BC49D64C74B47D8CA075E584BFBD2A21E0C5F497
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("Ae65rd");.var tob=_.Ll("Ae65rd");.var n$=function(a){_.Mn.call(this,a.va);this.B= !1};_.G(n$,_.Mn);n$.ja=_.Mn.ja;_.g=n$.prototype;_.g.UG=function(){var a=this.O("haAclf").el();this.B="none"===_.Nm(a,"pointerEvents")};_.g.To=function(a){var b=this.aa(), c=this.O("haAclf").el();c="none"!==_.Nm(c,"display")&&null===_.vn(a.targetElement,".Znu9nd").el();var d=this.B&&c&&!_.wn(b,"CJIdie");c&&(b.Ma("CJIdie"),_.wc(thi s.O("haAclf"),"a").focus());d&&a.event.preventDefault();this.B=!1;return!0};_.g.Tr=function(){this.aa().Ka("CJIdie")};_.g.R7=function(){_.wc(this.aa(),".Znu9nd").Ma("eB4 8Hf")};_.g.Q7=function(){_.wc(this.aa(),".Znu9nd").Ka("eB48Hf")};_.g.j8=function(){this.aa().Ma("CJIdie")};_.g.A7=function(){this.aa().Ka("CJIdie")};_.O(n$.prototype,"SzA CGe",function(){return this.A7});_.O(n$.prototype,"jbFSOd",function(){return this.j8});_.O(n$.prototype,"dq0hvd",function(){return this.Q7});_.O(n$.prototype,"y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\m=pB6Zqd,syw,IZT63,SF3gsd,vfuNJf,sys,syq,syx,O8k1Cd,sy17,siKnQd,syr,syv,sy11,YNjGDd,sy10,sy12,PrPYRd,xs1Gy,hc6Ubd,o02Jie,SpsfSb,sy19,sy18,syn,zbML3c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	26806
Entropy (8bit):	5.38658403444768
Encrypted:	false
SSDEEP:	768:FREVS6r0Q9dE+MlN9d70pxNHMOH7GUOB+oBF6PWLXW4laOfdCRmiOplJ5TurW5t4:Fked7g1BOB+oBF6PWLXWWfIs52
MD5:	20A9810E91DE0B5B482FAB4ED6F6CB1C
SHA1:	8C9EF3938F1D015CEE97601FCD9C543B52D5460D
SHA-256:	08CF1ADAED56E9342B958F5700C1A1BB7E1C47436DE346D58C088ABA5E798EE8
SHA-512:	F69B91180593B2C45C9AD8AE9338CB3BF3754DA114211942FD95F26A2870143FA76D36EC3A9502474A6DD3FA63363FA2A6D590D68A15F53383A44C5DFF1E1E9F
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("pB6Zqd");._.tk(_.Ow);.._.y();..}catch(e){_._DumpException(e)}.try{._.aD=function(a,b) {return(b=b.WIZ_global_data)&&a in b?b[a]:null};_.n("syw");.._.y();..}catch(e){_._DumpException(e)}.try{._.n("IZT63");._.bD=function(a){_.In.call(this,a.va)};_.G(_.bD ,_.In);_.bD.Ga=_.In.Ga;_.bD.ja=_.In.ja;_.bD.prototype.get=function(a){var b=_.aD("nQyAE",window)[a];return void 0!==b?new _.Bn("nQyAE."+a,b):null};_.bD.prototyp e.getAll=function(){return(new _.Bn("nQyAE",_.aD("nQyAE",window))).object()};_.bD.prototype.isEnabled=function(a){return this.get(a).wb()};_.Ln(_.Ipa,_.bD);.._.y();..}cat ch(e){_._DumpException(e)}.try{._.n("SF3gsd");._.tk(_.Rw);.._.y();..}catch(e){_._DumpException(e)}.try{._.n("vfuNJf");.var nD=function(a){_.In.call(this,a.va)};_.G(nD,_.I n);nD.Ga=_.In.Ga;nD.ja=_.In.ja;_.Ln(_.Qw,nD);.._.y();..}catch(e){_._DumpException(e)}.try{._.n("sys");.var XA=function(a,b){this.jb=a;this.B=b};XA.prototype.get

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\office3651[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18025
Entropy (8bit):	3.011161251318808
Encrypted:	false
SSDEEP:	96:2S+WvkiqJq6Uq7NXrNG+GHhsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SJkiOq6Uq75shDs1kFP
MD5:	FE22440D79FFA34950F512EF4A718B2A
SHA1:	0E147E59544EE6580D3095353D4420849FA5EB8A
SHA-256:	A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8
SHA-512:	64218ECD4140DC05E50EB7BA4C9813794B8B5A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/office3651.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\office3651[1].png	
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/outlook1.png
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. .. .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0...d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C.....".....U....7....G...'h.....1j1E..%t.....@..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r(...6;EP.T.....h.m".[f.U)|t..2.Q.....g.cP.W...D..[.O>..d;.yl.{/..#v.._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\pxiDypQkot1TnFhsFMOfGShVF9eI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 38064, version 1.1
Category:	downloaded
Size (bytes):	38064
Entropy (8bit):	7.985282250659124
Encrypted:	false
SSDEEP:	768:FmLfShvXTNLstzb6V8QZ3+ibkkftFHdur7Lh9JVIzdMIWRirfqiW5Pm9WmX:FmzSdXOhOOA5uDzHIz3WUrPYtmX
MD5:	E7BBF7E9E89975E144CBC167F2293FDE
SHA1:	0CB43D4E0ECF79C8AF6629CA1C386EA23FA02C02
SHA-256:	A87A298223B431522629F284F2D237773F8257B2DB427904CA95EC20DFC34CDD
SHA-512:	75AD4EF05603116A2C0D16E9C7F793D47602044611F369A83A6AED4D14279809064C43B6EA3BEA28F889F3CE65199DA67CF0685819A8F0C01F5DFC0C97969A7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/productsans/v9/pxiDypQkot1TnFhsFMOfGShVF9eI.woff
Preview:	wOFF.....G.....GPOS.....K...X....GSUB.....!?-.OS/2.....Y...`k..cmap...(... ....)9.8cvt ...H...g...l...wfpgm.....a.A..gasp.....!glyf.....TD...$...yhdmx..c...'m..Kha`98head...h...6...6..N{hhea..... ...$...Chmtx.....^...l}.*.loca... ...8...8...Pmaxp...X... ... .8..name...x..... P<.post...L...|...{#_.sprep.....oNx.d.%@E1....w*Vpw.....]z$S...HT.L&.L.g8.M.....ib....&.....]..${..i..<..A..Y.....+.... .[..x...pL.=L.]`.mv...+..x.J.1..G<.$.B&..r..5.zs.q..W..... ?./.1.i.....?...?..uk.&~.I..\YF.6...|<!.:..Jxg.|...0.bb..|..=.=.=G....&!&!CB...Y".....)ij.....*r.....ku.j.9q"....hs...D"._.....X.+02.{*>...";>.....3.([a.'y.L.&."..2.O....*....`..L~.l}....h>x .J...V.8u<..."..Wh.....FF"#.8.....=#Q.K.....!.S}...9.....bv..V.....W..."/...9U}.....5....g.{"..{.....Y.v...T..o..i.s.....|V.Hs..8d..N=..lg..g.HV...E.{;W.w6...R3&.mV..Q"%.<.3tlE.i.3yB62.....>K...l....s.(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\remote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100380
Entropy (8bit):	5.447170305187555
Encrypted:	false
SSDEEP:	3072:w6v7A7dK/PhqflUlDSNWVLWYM3SyJW1Qpll06H0FQ:Hv7A7dK/PMlUlDSNWVLWYM3SyJW1Qplp
MD5:	F4FDA7A202A3EF6F55E3D0001E3B556C
SHA1:	65CDE0A38E9A4DC0CA590EA45769B7F3ABFEF194
SHA-256:	BD2808457ADFD2D1016BEA1AD38EF08F55E4E69CDA8E0785D8808D3168BE636E
SHA-512:	3C39F7372F0CE10D204BA3776DE8B07BBB6E8D007EAB219A071A128A5FBB4C641AAB54955ED94A18607821AB1D7BEF90159D4FF22DEA8991117B9781D1AF3BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube-nocookie.com/s/player/1fe59655/player_ias.vflset/en_US/remote.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\remote[1].js	
Preview:	(function(g){var window=this;'use strict';var OKa=function(a,b){return g.Lb(a,b)},PKa=function(a){if(a instanceof g.Yi)return a;.if("function"==typeof a.xg)return a.xg(!1);if(g.La(a)){var b=0,c=new g.Yi;c.next=function(){for(;;){if(b>=a.length)throw g.Sm;if(b in a)return a[b++];b++}};.return c}throw Error("Not implemented");},QKa=function(a,b,c){if(g.La(a))try{g.zb(a,b,c)}catch(d){if(d!==g.Sm)throw d;.}else{a=PKa(a);try{for(;;)b.call(c,a.next(),void 0,a)}catch(d){if(d!==g.Sm)throw d;}}},R4=function(a,b,c){a.l.set(b,c)},S4=function(a){R4(a,"zx",Math.floor(2147483648*Math.random()).toString(36)+Math.abs(Math.floor(2147483648*Math.random())^g.Ra()).toString(36));.return a},T4=function(a,b,c){Array.isArray(c)||(c=[String(c)]);.g.hn(a.l,b,c)},RKa=function(a,b){var c=[];.QKa(b,function(d){try{var e=g.$n.prototype.l.call(this,d,!0)}catch(f){if("Storage: Invalid value was encountered"==f)return;throw f;}void 0===e?c.push(d):g.Zn(e)&&c.push(d)},a);.return c},SKa=function(a,b){b=RKa(a,b);.g.zb(b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182623714755422
Encrypted:	false
SSDEEP:	192:BgHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:WRCfhFzevnEZ/h81Q5l8OsE
MD5:	D8CA71772D1E86D5FB9D5E2F6CC1AE70
SHA1:	9B043E60997FE552D652E4474E16AFF923D7AA76
SHA-256:	7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE
SHA-512:	8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\EmbeddedImage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=2, software=Picasa], baseline, precision 8, 1280x740, frames 3
Category:	downloaded
Size (bytes):	179737
Entropy (8bit):	7.965898834079505
Encrypted:	false
SSDEEP:	3072:ras19l5H/tC7gUC9wdYMjvByFSt/0pBIROMdp4U4ytnNNiQfc+/71P:ras19lRlFUCeTvBK+MBIRO+p4cFiQk8h
MD5:	7163EA61402B5A78AF49CF9A35F47733
SHA1:	2E424471873B349280A62BCC964D6BC9D0F137DC
SHA-256:	3D8AFD9036E89FDC543B20D109314C9B282104465B640CCCED689C8A0E1D5BC4
SHA-512:	1E7618FF8F284E5B06B4019DD3594D18BB80BCFC0E8024F394D2FFA1D71B7349F68B4C3A2484BFB5C65B21AFF6866C41C54997C72EBF3D150FC626B20EA36C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh5.googleusercontent.com/f6-8EKBxp5ehlT53qtioVBOxiLVnsove4k696nJHLRIjzmxrZxj2DiQrCZTbIEOyW4aIfpx9oBsTV0Eu-AmNu9l6rc0NDPW9NlJRkytrwJq7RXnjr_stXuYoQ-gWk7BRvQ=w1280
Preview:	......JFIF.....DExif..II*.....1.....&...;.....-.....Picasa.martin barraud.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" photoshop:Credit="Getty Images/Caiaimage"> <dc:creator> <rdf:Seq> <rdf:li>Caiaimage/Martin Barraud</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>...@ICC_PROFILE.....0ADBE....mntrRGB XYZ .....acspAPPL....none.....-ADBE.....cprt.....2desc...0...kwtpt.....bkpt.....rTRC.....gTRC.....bTRC.....rXYZ.....gXYZ.....bXYZ.....text....Copyright 1999 Adobe Systems Incorporated...desc.....Adobe RGB (1998).....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf...x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./ 6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m..../.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._..T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RKK2G0P6.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	297477
Entropy (8bit):	5.610488270408067
Encrypted:	false
SSDEEP:	6144:HuMNNiAOpjZqEABMKxePa28051Rtmprw+ilgx:TNNMZABa805p+
MD5:	1ABE18A516BD0F2DCB7CF9F48E30311C
SHA1:	4AFFE4AA230BF6B713E9FDBB5A742C171C1014F8
SHA-256:	136E0FE2AFDA1DCC46608D80A1BBB8D1D86599779D2C9FAA2E3AAA1C97D7FEE2
SHA-512:	E5B340B20549653761C21832B8CD79085E59B0F82904F2B37F48F914029A18518765FF4D7A02EF97C4900E53B19EEA23FCC7B06DD8119521A40AFB17B5A6ABDC
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\CS6IXJW6\TBR-xtJVq7E[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):	50080
Entropy (8bit):	5.814420432826252
Encrypted:	false
SSDEEP:	768:7BKiDH4H8bLeqpFe/XSuBJgyzPSXkAKIkD9DRn80//wTnjEeIqX:BX0XSByGXfKrDFR0Tnx
MD5:	C1C87DC5F46FA8B090F53275E101E546
SHA1:	E2CCF3550AD168D5012CE1D11AB1156DF30C653A
SHA-256:	F270CC61DB9DF83937CF20CCA43A82ABAAB31F22438E2D24C8C6965BF30D25C5
SHA-512:	9A584CE4D5619AE69B477FA91BB0F5F0D630170D825DD07D0CF2C082CA8CFD4B32A55B4ACA3FFA2BB3D58CC23E9EF3AB87DE32B0E5CB9969112426A57FD5406
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\TBR-xtJVq7E[1].htm	
Preview:	<!DOCTYPE html><html lang="en" dir="ltr" data-cast-api-enabled="true"><head><meta name="viewport" content="width=device-width, initial-scale=1"><style name="www-roboto" nonce="6l6OKj11ZKL3+0NvZBAmXA">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}</style><script name="www-roboto" nonce="B/jTVDpobWjJ8tkOumfVkA">if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "E"); document.fonts.load("500 10pt Roboto", "E");}</script><link rel="stylesheet" href="/s/player/1fe59655/www-player.css" name="www-player" nonce="6l6OKj11ZKL3+0NvZBAmXA"><style nonce="6l6OKj11ZKL3+0NvZBAmXA">html {overflow: hidden;}body {font: 12px Roboto, Arial, sans-serif; background-color: #000; color: #fff; height: 100%; width: 100%; overflow: hidden; position: absolute; margin: 0; padding: 0;}#player {width: 100%; height: 100%;}h1 {text-align: center; color: #fff;}h3 {margin-top: 6px; margi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\adobe-pdf-icon-logo-png-transparent-285x300[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 285 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	34353
Entropy (8bit):	7.979805722823804
Encrypted:	false
SSDEEP:	768:N9xfTAXr2MJkBTCNmDcEKzOYEUtVD3KdvW95:lmrJMCDzIU3WdvQ
MD5:	2499C2758E9581401BDA79616C11BC23
SHA1:	3484F31C3E550A20BC52E9D124038E24869D3253
SHA-256:	3CF94D7F901B97A6697F2E7AC4B4688779B0C705F48939A2E09BC86D7C24E350
SHA-512:	BC9254D9D2B4E7FD407BF98F0E980AD0E89A91D0AB99AB8BD8F7E6EA0C7604D7FA7895646C1960C4AB458AE09998C1A231A51411954E0DEF0187477D1E6C864 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh6.googleusercontent.com/zpO9kHTvpLtyF0occuD5iEjTbotrMbK6h-VvR6YrxCosY8V3x5Cp6-iMKe6v8WpZW4TvnO-UbNJea3Y7HI4OMTA=w16383
Preview:	.PNG........IHDR.....,.....Lgs....sBIT....|.d... .IDATx..]y..E..V..g6...$.$.....>$.....|..$..>...Q.DPy..P.y..@..GB.....{..t.?.....$...lwW..W.....~U..T.JU.R..T.*U.JU.R..T.*Uic#2.. T.J.H.....U*#UA.@...J..9.#...+9.R.(9....r...^.M.d.....,.Je...tXCK>..s.677..R.PJ.[.*.....J)..<r.....3ox..W.Q..,6...j...6..U.....{..#..l..4pD)..p]..\....X.n...>...n..]x..'.]W..D.\....I.....M....-.~t .CQ.;..d.:...,BH..~.N:.;.....4..:.....L.k.9..N.@C___.o.@q..I.?.e.s1L....).r.'..B2;....>...O.>.@..c..@gs.?%Qb...$J.r.4.|...1b.v@.aRJA....|...O3.d.L.....!f.QJ.....G.}.....7o. .@C...r.U.....k...?..<..i...(Y.O.3./..e...8.....d..f.....n.....h..l.U.o.b.*Y..h.0...@=.a....g....c.2b.k..*kpd...Y<===p].6m...r..?.....S..V.a.r..1..j.....(#.j.....:.T..[Y2...,f.8..d2.T*.t:.T*...N. [..S.N.....H.m.[=.k.....!..].....c'..ZU.L..4lY}..p.....9s..kG...W%.UQ.#m=.FX..T..-.&>.m.x.N*.BMM.2..jjj.b..tuu...../....v.3..x....z2(X=U.P.t"....|..~...(Y6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	103384
Entropy (8bit):	5.526517404243879
Encrypted:	false
SSDEEP:	1536:ybQMyyvL/aJi9MmvzaPvcWU3XMLxEzGZUkxyCFNCwKYWnxcdf0iHY7:IyyvL/x3fzGeKFTWnxgMiHY7
MD5:	A611C6714CEED4239A9CD09EDC362466
SHA1:	217FBF4900783F474F611B0A01A0386D4E0CF473
SHA-256:	E778E381055F2780B7816AF2D8F319EEEC9A62E9F82CE320CDC3F561F22AAA63
SHA-512:	AA55E6CF29D082EF114611BA3EB7C4F3660C9CE7061F2AE0A174D63C158850393E3226F09DE44CDB9F4FE8E9373AECF47E7CE94D60D2EB18F3B0B43C9843FD 0
Malicious:	false
Reputation:	low
Preview:	gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,na,pa,wa,Aa,Da,Oa;_.ha= function(a){return function(){return _.ca[a].apply(this,arguments)}};_.ca=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}} ;ka="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.na=functi on(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");};pa=na(this);wa=function(a,b){if(b)a:{var c=pa;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ka(c,a,{configurable:!0,writable:!0,value:b})}};.wa("Symbol",function(a){if(a)return a;var b=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cookies[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):	1429
Entropy (8bit):	5.275903140202486
Encrypted:	false
SSDEEP:	24:hoyihMiCN24xtMkb57jCSXYwBwWHQUCKNUVqHUCJO1JenHpZpw4wVO1D141dJ1MB:SyiKiuv8kYSX/QZWqCZeUnK4KO9yxoI6
MD5:	9D515063CEB30849D780B77615BCC85F
SHA1:	BDA02BC86A65BAF0D9C4B9ED2B9E0FC42EE976CB
SHA-256:	51047D749CD38B4990D40DC6ED8E01B32007C5E225E2D504A48BC6179AFF35BA
SHA-512:	BBD93FDF57719C9D6C960280262364A7B1C60A3B32F3AF6AF1749EAFC6298A2DA720CB3E9057B850814F79804CF60ECD89B23E0E2F3ABCA915288B728218403
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cookies[1].htm	
Preview:	<!DOCTYPE html>.<title></title><noscript>.<meta content="0; URL=https://policies.google.com/technologies/cookies" http-equiv="refresh"></noscript>.https://policies.google.com/technologies/cookies .<script nonce="_2IIhDmHIsTaJ7LTMRbYhw">.var url="https://policies.google.com/technologies/cookies";.try{var curl=window.location.href;var match=curl.match(/\/intl\/([^\/]+)\/policies/);var locale=match&&match[1];var hl;var gl;if(locale){if(locale.indexOf("_")>0){var parts=locale.split("_");hl=parts[0];gl=parts[1]}else hl=locale;if(hl=="ALL")hl=null;if(gl=="ALL")gl=null}.if (URL&&(!hl||!gl)){ var cu=new URL(curl);hl=hl||cu.searchParams.get("hl");gl=gl||cu.searchParams.get("gl");}.if (URL&&curl.indexOf("authuser")!==-1){var cu=new URL(curl);var authuser=parseInt(cu.searchParams.get("authuser"),10);if(!isNaN(authuser))url=url.replace('.com/',',com/u/'+authuser+'/');}.if(!gl){var tld=location.hostname.split(".").pop().toLowe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\cookies[2].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):	197820
Entropy (8bit):	5.667511851270972
Encrypted:	false
SSDEEP:	1536:QP+ooaA4VRvufezbCDuWf1IBtnWS9MIBbvDgaYofi0G6nhrTy2Br7/SdSs671Ium:D8VmDyjgaYz0h9t/w5uc
MD5:	93588142DEAD26C1EBAB6C79E29D24C5
SHA1:	E5FB331C411C406D5EE53BC3C0908338A46DE076
SHA-256:	5E6F5492A1A39D47DFFF2CFF785A11DEDFF576CC40215BA29000BA39EF4B20DB
SHA-512:	E4770368DF7C280B40A29C4C35D8DB9328A7D61614222D53206D1FA81D1CF6EF6F3AA48337042C6BE498237A1480E8A85C37E4AD68FED98AD1B68CECD8926B(
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\CS6IXJW6\googlelogo_clr_74x24px[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1660
Entropy (8bit):	4.301517070642596
Encrypted:	false
SSDEEP:	48:A/S9VU5IDhYYmMqPLmumtrYW2DyZ/jTq9J:A2VUSDhYYmM5trYFw/jmD
MD5:	554640F465EB3ED903B543DAE0A1BCAC
SHA1:	E0E6E2C8939008217EB76A3B3282CA75F3DC401A
SHA-256:	99BF4AA403643A6D41C028E5DB29C79C17CBC815B3E10CD5C6B8F90567A03E52
SHA-512:	462198E2B69F72F1DC9743D0EA5EED7974A035F24600AA1C2DE0211D978FF0795370560CBF274CCC82C8AC97DC3706C753168D4B90B0B81AE84CC922C055CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/branding/googlelogo/svg/googlelogo_clr_74x24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="74" height="24" viewBox="0 0 74 24"><path fill="#4285F4" d="M9.24 8.19v2.46h5.88c-.18 1.38-.64 2.39-1.34 3.1-.86.86-2.2 1.8-4.54 1.8-3.62 0-6.45-2.92-6.45-6.54s2.83-6.54 6.45-6.54c1.95 0 3.38.77 4.43 1.76L15.4 2.5C13.94 1.08 11.98 0 9.24 0 4.28 0 .11 4.04.11 9s4.17 9 9.13 9c2.68 0 4.7-.88 6.28-2.52 1.62-1.62 2.13-3.91 2.13-5.75 0-.57-.04-1.1-.13-1.54H9.24z"/><path fill="#EA4335" d="M25 6.19c-3.21 0-5.83 2.44-5.83 5.81 0 3.34 2.62 5.81 5.83 5.81s5.83-2.46 5.83-5.81c0-3.37-2.62-5.81-5.83-5.81zm0 9.33c-1.76 0-3.28-1.45-3.28-3.52 0-2.09 1.52-3.52 3.28-3.52s3.28 1.43 3.28 3.52c0 2.07-1.52 3.52-3.28 3.52z"/><path fill="#4285F4" d="M53.58 7.49h-.09c-.57-.68-1.67-1.3-3.06-1.3C47.53 6.19 45 8.72 45 12c0 3.26 2.53 5.81 5.43 5.81 1.39 0 2.49-.62 3.06-1.32h.09v.81c0 2.22-1.19 3.41-3.1 3.41-1.56 0-2.53-1.12-2.93-2.07l-2.22.92c.64 1.54 2.33 3.43 5.15 3.43 2.99 0 5.52-1.76 5.52-6.05V6.49h-2.42v1zm-2.93 8.03c-1.76 0-3.1-1.5-3.1-3.52 0-2.05 1.34-3.52 3.1-3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\history[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):	57510
Entropy (8bit):	5.794069112727472
Encrypted:	false
SSDEEP:	768:dVulKRDF8jqAkoHRSLVkjfArtTTm4+njSs:dVLWqAkoHRSLVkjfArtTTm4+jSs
MD5:	C3BA4DAD0A4FDCC57398AEEE6A35B35D
SHA1:	FCD9BB4C8E77BE8A7B94A58ADA8D5A1386CB3D68
SHA-256:	1FA9CEE0CA6BB42094433C80DED74BED7EB7A5A5333E15130A9A757E9BE1C7F7
SHA-512:	6361DE1C732A57660825124FFA126E7CE777658CCFE625D72A106F99B377171C36D5C5DCBDA2306350E0A4EFD65A4E7776EA0A82CF47598838BBE14EFC059C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\history[1].htm	
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="LZYvU1KFZnRQskN+8OaVDg">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="LZYvU1KFZnRQskN+8OaVDg">function _DumpException(e) {throw e;}</script><script nonce="LZYvU1KFZnRQskN+8OaVDg">_docs_flag_initialData={"atari-eiicg":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","ilcm":{"eui":"AHKXmL38hffkys42Io8jeFzjNJSRnl3CXkYV8tBBj2GKERngc05wV7uqLRhjHBBwzSiOjsp7J9pm","je":1,"stu":1623351138727000,"si":"CI7w4J_ejfECFYGhHwodtUwDXg","gsc":null,"ei":[5720060,14101550,5714550,14101462,5732942,5735806,5703022,14101046,5712211,5729072,5719651,5713049,5712373,5720925,5708870,5734571,14101530,5714628,5711808,14101510,14100834,5709892,14101534,5711850,5734691,5703839,5707711,5721004,5727317,14101502,5722370,5713207,5706832,5706836,5704621,5713211],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector	(c) JS Foundation and other contributors	jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4	(c) jQuery Foundation	jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=Wt6vjf,_latency,FCpbqb,WhJNk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	modified
Size (bytes):	6515
Entropy (8bit):	5.526490849936006
Encrypted:	false
SSDEEP:	96:tyQWQXSMX1T/9b9oFrCglURthrJLUnn5PiATNx/PWvzWT6OImz4MDWyt9Kq5t9SN:tVWQ9JbtD45PnJxwzWWrcOWbM2w8KN
MD5:	C6E57C5ACB2449E3F87D5E5213AF1BAC
SHA1:	EAEB094AF290DBD20673F715FF2745F3365DF261
SHA-256:	16BB9266943940735BB4C8105F68F14B6272EDC7F2CA52F8AEACB22057C93819
SHA-512:	2ADECF8D0D3BE7F3D70A4E6C3F5042FF10589C28D0555530E13E2FA56BA40379E4C4C30466F73D2135B036810A87F9D1D08D3365B6D9F4B13242A9674A80601E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=Wt6vjf,_latency,FCpbqb,WhJNk[1].js	
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{._.n("sy4k");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.._.t();.._.n("Wt6vjf");.var eL=function(a){_.z(this,a,-1,null,null)};_.y(eL,_.u);eL.prototype.Wa=function(){return _.Oh(this,1)};eL.Zc="f.bo";.var fL=function(){_.Zi.call(this)};_.y(fL,_.Zi);fL.prototype.Gb=function(){this.fu=!1;gL(this);_.Zi.prototype.Gb.call(this)};fL.prototype.g=function(){hL(this);if(this.Hm)return iL(this),!1;if(!this.Pv)return jL(this),!0;this.dispatchEvent("q");if(!this.Wr)return jL(this),!0;this.uq?(this.dispatchEvent("s"),jL(this)):iL(this);return!1};.var kL=function(a){var b=new _.fu(a.XC);null!=a.Ns&&(a=a.Ns,_.gu(b),b.Gd.set("authuser",a));return b},iL=function(a){a.Hm=!0;var b=kL(a),c="rt=r&f_uid="+encodeURIComponent(String(a.Wr));_.Xr(b,(0,_.q)(a.i,a),"POST",c)};.fL.prototype.i=function(a){a=a.target;hL(this);if(_.ds(a)){this.Cp=0;if(this.uq)this.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	161734
Entropy (8bit):	5.463934426409893
Encrypted:	false
SSDEEP:	3072:Zalcdi3uze/iHqIfa4Fh0sEzKz0s5FJnI:ZxgpSqIfpESvI
MD5:	784A6AD1FDA9BD7EF23A403025EFD8C4
SHA1:	16DE704D66CEFD1D1B6FECBC5FA8110364830A5C
SHA-256:	D69D6ED2C077EB970E5B646A422BA904E477803D089BBEB52535DF7D45AA9E1D
SHA-512:	AB19339F54B83B3B7B451E9DDBE6C74DC3FC24935C9C9F097E0F9EB2274839E0E7AFA7E6E86B43B3611F291CB097209EC7DA3B4CD9D488E86CEC198DCCA47 1A
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{.var ja,aaa,cb,Gb,baa,caa,daa,eaa,faa,gaa,kc,iaa,jaa,la a,maa,tc,naa,oaa,wc,qaa,Bc,waa,uaa,xaa,aa,Xc,Yc,yaa,ad,bd,zaa,fd;_.ba=function(a){return function(){return aa[a].apply(this,arguments)}};_.ca=function(a,b){return aa[a]=b};_.da=function(a,b){if(Error.captureStackTrace)Error.captureStackTrace(this,_.da);else{var c=Error().stack;c&&(this.stack=c)}a&&(this.message=String(a));b&&(th is.Ts=b);this.g=!0};_.fa=function(a){_.l.setTimeout(function(){throw a;},0)};._.ha=function(a){a&&"function"==typeof a.Sc&&a.Sc()};ja=function(a){for(var b=0,c=arguments. length;b<c;++b){var d=arguments[b];_.ia(d)?ja.apply(null,d):_.ha(d)}};_.na=function(){!_.la&&_.ma&&(_.la=(0,_.ma)());return _.la};_.n=function(a){if(_.la){var b=_.la;b.j= b.ih(a)}};_.t=function(){if(_.la){var a=_.la;if(a.j){var b=a.j.getId();a.isDisposed()||(oa(a.i[b],(0,_.q)(a.Rz,a))&&pa(a,4),_.qa(a.u,b),_.qa(a.o,b),0==a.o.lengt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=byfTOb,lsjVmc,LEikZe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	37196
Entropy (8bit):	5.469946156602675
Encrypted:	false
SSDEEP:	768:p9MY0kt/B8SNWw7jYhGKWMRjYLHlOnkuiZOpQ+RNxMr66KEm8hpP:p9MbqYhzgOnkuBpXR0JP
MD5:	165862D91EB3F10FC4FBB5E1283D0B31
SHA1:	2EA1BC33C615763F2E674D9D77524BE00BBB35BD
SHA-256:	5CBE095F37504C210B4787D63E23E4BE3A0250DBFC86A04C03B6EC78110CBBB0
SHA-512:	75C14C2936679190962164CED96AC913C850645406C8E2A9126B77916C573B1B10CA9AFE5FAD5CDFD2675DD88F44C1220A60D468DFC66AC3A89179744B334C2
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_IdentityPoliciesUi=this.default_IdentityPoliciesUi||{};(function(_){var window=this;.try{._.cu=function(a,b){a.sort(b||_.Na)};._.du=function(a,b,c,d){a=d||a;b=b&&"*"!=b?String(b).toUpperCase():"";if(a.querySelectorAll&&a.querySelector&&(b||c))return a.querySelectorAll(b+(c?"."+c:""));if(c&&a.getElementsByClassName) {a=a.getElementsByClassName(c);if(b){d={};for(var e=0,f=0,g;g=a[f];f++)b==g.nodeName&&(d[e++]=g);d.length=e;return d}return a}a=a.getElementsByTagName(b||"*") ;if(c){d={};for(f=e=0;g=a[f];f++)b=g.className,"function"==typeof b.split&&_.ya(b.split(/\s+/),c)&&(d[e++]=g);d.length=e;return d}return a};_.eu=function(){return _.vb("I m6cmf").Ta()};._.n("sya");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var iu,ku,lfa,lu,Ffa,Efa,Hfa,Gfa,nu;._.fu=function(a,b){thi s.Lj=this.Gk=this.ij="";this.$l=null;this.Nj=this.fg="";this.dg=this.uJ=!1;if(a instanceof _.fu){this.dg=void 0!==b?b:a.dg;this.xm(a.ij);var c=a.Gk;_.gu(this);t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=sy1w,sy1q,sy27,sy29,sy2h,fuVYe,vVEdxc,sy22,CG0Qwb[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	28550
Entropy (8bit):	5.611471883712465
Encrypted:	false
SSDEEP:	768:xME6sJWLriliKxrTQAg3T/GElLGd72O86MirhNx8ZE:FHWLRrTL72O8wVNgE
MD5:	033D1C7F7670A2BC62FBCF3B7226DBB1
SHA1:	42B7A7AAAB142B9A669641CE02C713324AAE587D
SHA-256:	DB62CCE0C21DED784700D98A48AFB4107A1963A9C3634D8847293FA27F721022
SHA-512:	998DB55A913C323E3B3F2A01DC958695262A61248F7F03426640F33BF7D27509ECEB4B3CC94DF3B7C1DD58CEED35FCCB8E24B7136CCF4EA821FC5845419748
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=sy1w,sy1q,sy27,sy29,sy2h,fuVYe,vVEdxc,sy22,CG0Qwb[1].js	
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("sy1w");.._.y();..}catch(e){_._DumpException(e)}.try{._.CH=function(a,b,c,d,e,f,h,m,p,u,w,E,F,K,Q,X,ha,fa,Da,Ob,jb,Qc,kd,Za,Pd,lf,ui,dg,Jf,Id,Xc,gd,eg,Xd,fg,de,hj,Lh,Jg,vi){this.ua=a;this.C=c;this.da=b;this.D=d;this.B=e;this.H=f;this.rc=h;this.lc=m;this.hb=p;this.Nc=u;this.mf=w;this.bd=E;this.L=F;this.oa=K;this.I=Q;this.F=X;this.J=ha;this.ia=fa;this.Ib=Da;this.Kb=de;this.Ca=Ob;this.Ha=hj;this.W=jb;this.ke=Qc;this.Lc=kd;this.wc=Za;this.Bc=Pd;this.Bd=If;this.wa=ui;this.Pa=dg;this.ca=Jf;this.fd=Id;this.V=Xc;this.fb=gd;this.za=eg;this.Ya=Xd;this.$a=fg;this.R=.Lh;this.S=Jg;this.Wd=vi};_.G(_.CH,_.tg);_.n("sy1q");._.DH=function(){};_.G(_.DH,_.tg);_.EH=function(a,b){a.ua=b;return a};_.FH=function(a){a.C&&a.B&&_.Tf(a.B,4)};_.GH=function(a){a.C&&(a.B||(a.B=new _.qj),_.kg(a.B,4,a.C));return new _.CH(a.ua,a.da,a.D,a.F,a.B,a.ke,a.bd,a.rc,a.hb,a.fd,a.Lc,a.wc,a.I,a.oa,a.Wd,a.R,a.qf,a.ia,a.lc,a.Ca,a.V,a.Kb,a.Bc,a.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\m=view[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	497633
Entropy (8bit):	5.561954762420147
Encrypted:	false
SSDEEP:	6144:asvVpObgbNkyk1Y3xzp8SxpJg5ocCLYj0MKnb:as6yF3xq2Jbct0M0
MD5:	F9B0702763D41ABAFEA4577D1D6EC31D
SHA1:	DACA448ECA31FFF6F3BC5486798BAA343114CB00
SHA-256:	29CF633C2A06C572F229D89372D27455E92B38DA5E71E1CE18771F190C985327
SHA-512:	E8A78FC26C56191B2132DADF4C85948672893EAB8A1F24417C4DC6E996C169157169D742A68E43A3D9BA5C6FEC1A669AD3656E2BA997239ED625ED213BCDA4 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/atari/_/js/k=atari.vw.en_US.fT7Agarg7eM.O/d=1/rs=AGEqA5kqyhjAgP8EcVBOydHCqcMjdjogrQ/m=view
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{.var aaa,baa,eaa,lb,jaa,tb,sb,vb,kaa,laa,maa,Ab,naa,oaa,paa,raa,Rb,taa,uaa,Baa,vaa,Caa,Faa,Haa,nc,oc,Kaa,pc,Laa,Maa,sc,Naa,Paa,Vaa,Xaa,Yaa,$aa,gba,iba,kba,lba,pba,tba,uba,bd,vba,dd,wba,kc,xba,ed,jd,ld,Aba,pd,qd;_.aa=function(a,b){if(Error.captureStackTrace)Error.captureStackTrace(this,_.aa);else{var c=Error().stack;c&&(this.stack=c)}a&&(this.message=String(a));b&&(this.cause=b);this.B=!0};_.ba=function(a){return a[a.length-1]};._.ca=function(a,b,c){for(var d="string"===typeof a?a.split(""):a,e=a.length-1;0<=e;--e)e in d&&b.call(c,d[e],e,a)};_.ja=function(a,b,c){b=_.ea(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]};_.ea=function(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)if(f in e&&b.call(c,e[f],f,a))return f;return-1};_.la=function(a,b,c){for(var d="string"===typeof a?a.split(""):a,e=a.length-1;0<=e;e--)if(e in d&&b.call(c,d[e],e,a))return e;return-1};._.na=fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\other1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21882
Entropy (8bit):	4.268463452779894
Encrypted:	false
SSDEEP:	192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDlJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://smtpro101.com/email-list/mnb/images/other1.png
Preview:	.PNG.....IHDR.....$.... cHRM..z&.....u0...`..:....p..Q<....sRGB.....gAMA.....a.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\url[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	499
Entropy (8bit):	5.205557096528763
Encrypted:	false
SSDEEP:	12:4krY1trWPqfor9emX8dwr9emXVFTQrpMr9emXE:zs1TWp8d2pVFuUpE
MD5:	0B8C4E1352D9920E57C197A02458C655
SHA1:	3EAF6D42A3654594179A98B17224EB23E0E7E4B2
SHA-256:	B85DCABF97A9233CA849DBCC03F57DB21C481300F289494288F3E361636EC66D
SHA-512:	4536277FE8847D69C1CB8EB8EEAB6B25E7C1D402CCB0DC6177A0B05B9E3182B1AA56964635B857D4F3E223DE23B4578B5ABE09CDBD56492B526486EE790CBF B1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\url[1].htm	
IE Cache URL:	http://https://www.google.com/url?q=https%3A%2F%2Fkanaan.s3.eu-de.cloud-object-storage.appdomain.cloud%2Farchaizes%2Findex.html&sa=D&sntz=1&usg=AFQjCNFtCAAkiNvTTHSVzB-bKWDyK7FRUA
Preview:	<HTML><HEAD>.<meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>Redirecting</TITLE>.<META HTTP-EQUIV="refresh" content="1; url= https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html">.</HEAD>.<BODY onLoad="location.replace('https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html'+document.location.hash)">.Redirecting you to https://kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud/archaizes/index.html</BODY></HTML>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wRcAf4HBykrYGCiISWytwERk8zO7uq9J4sRwSdSz-hE[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):	37929
Entropy (8bit):	5.6567582296838514
Encrypted:	false
SSDEEP:	768:YbYWWE8ms6XRLCJSyedjfV1meEOop0Px8rcuHAB37c8/T:YbTW1ms2pCdmjfTEOoGcu37c2
MD5:	788F3CEB3EE01EF6C06ED0576C5A4CDE
SHA1:	CF4E646B0E7D5ED374D849C20D8C3B3FF03208B2
SHA-256:	C117007F81C1CA4AD8182888496CADC04464F333BBBAAF49E2C47049D4B3FA11
SHA-512:	CCDA1356743B7B08975CF75DD516A1259EEEA8D31A5542EBBE5487DDD3FB53D632D8C30AA79B1C24BE09B1F7F887975F1259EDB028795F1F03DD81CF927FB5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/th/wRcAf4HBykrYGCiISWytwERk8zO7uq9J4sRwSdSz-hE.js
Preview:	(function(){function X(Z){return Z}var R=function(Z){return X.call(this,Z)},q=function(Z,g,P,h,M){if((h=(M=P,a.trustedTypes),!h)||!h.createPolicy)return M;try{M=h.createPolicy(g,{createHTML:R,createScript:R,createScriptURL:R})}catch(Y){if(a.console)a.console[Z](Y.message)}return M},a=this||self;(0,eval)(function(Z,g){return(g=q("error","ad",null))&&1===Z.eval(g.createScript("1"))?function(P){return g.createScript(P)}:function(P){return""+P}}(a)(Array(7824*Math.random()|0).join("\n")+'(function(){var MM=function(g,Z,M,X,P,R,h,a){if(!((Z<<2)%15))if(M.classList)J(0,9,X,function(Y,q){M.classList?M.classList.add(Y):U(g,28,"",M,Y)||(q=t("string","",8,M),N(15,"string",M,q+(0<q.length?" "+Y:Y)))});else{for(P in J(0,(J(0,(h={},9),L("",M,23),function(Y){h[Y]=true}),61),X,function(Y){h[Y]=true}),R="",h)R+=0<R.length?" "+P:P;N(30,"string",M,R)}return((Z+g)%14||(this.type=M,this.currentTarget=this.target=X,this.defaultPrevented=this.g=false),1==(Z+1&21))&&(d.call(this),M||Z7||(Z7=new gD),this.We=nu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\www-player[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):	366277
Entropy (8bit):	5.243924779987934
Encrypted:	false
SSDEEP:	1536:BDQI0irpHrpj/fn8M0MA0jDrzltP3Su3EMFfy7OP5FRrDJciM/ByDE4x6D6S7eTz:K4Drzz1ngWyxjFLu
MD5:	C54DBC7C85EC7A79949AB4859FED425B
SHA1:	1FA028B61E520E8077F9B21359A5932B3FB8BB5F
SHA-256:	247B9E16EA3C98F31C71C6921191F1BC4D96F56564C3E38C7AAC5F46D82CFBCB
SHA-512:	46BFC6E0959BF870CD186EE62906EC7AF781E641312B648316BBCD3725715BB761310E3BF6D4D516B98FC3AE82D8E7528C23A52972EB5667D3F352AD50B254C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube-nocookie.com/s/player/1fe59655/www-player.css
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;text-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000}.ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);-webkit-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);transition:color .1s cubic-bezier(0.0,0.0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0.4,0.0,1,1);-webkit-transition:color .1s cubic-bezier(0.4,0.0,1,1);transition:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\EmbeddedImage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=3, software=Picasa], baseline, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	99928
Entropy (8bit):	7.972378899176074
Encrypted:	false
SSDEEP:	3072:vWN51hUtQorDuWch48iduvmhQJCxxrtBM+4jh6MiloY:vg5ktdGouvmiJCbtBM+4jh6UY
MD5:	22FA2342F9A5D8DB9C50302304C7298B
SHA1:	219B50CB469D088502875E57F51C4438F07B0C10
SHA-256:	9723C7ECCB08342641FDF7D40E8F35288BDCCDC40FE6314FC54CEFDF30803D2F
SHA-512:	6EF4743DF23D7C9B46288E5DA58EB6DC13336147F1F218D722E9661834843317A641673384D970ACA781C3056C0301B6194ED9F2E5C34AAF5E4C64A925E88DCD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\EmbeddedImage[1].jpg	
IE Cache URL:	http://https://lh4.googleusercontent.com/autuU0VoLolXQGzjWfa8b1aEY2RB-HW1rvMPEg6MyGqM3h4P4OhVOkmpdjKMOR8zhCZCz7kKrh88sYbYM_6CGUWbLdjcy_cx3o3uywwmYgjXLdh-sZDJfFkEw9JSwC2Ziw=w1280
Preview:	.....JFIF.....~Exif..II*.....1.....2...;.....9.....!...T.....Picasa.JGI/Tom Grill/Blend Images..JGI/Tom Grill/Blend Images LLC.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" photoshop:Credit="Getty Images/Tetra images RF"> <dc:rights> <rdf:Alt> <rdf:li xml:lang="x-default">.JGI/Tom Grill/Blend Images LLC</rdf:li> </rdf:Alt> </dc:rights> <dc:creator> <rdf:Seq> <rdf:li>JGI/Tom Grill</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>...@ICC_PROFILE.....0ADBE....mntrRGB XYZ ... .acspAPPL....none.....-ADBE.....cprt.....2desc...0...kwtpt.....bkpt.....rTR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\EmbeddedImage[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=3, software=Picasa], baseline, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	181013
Entropy (8bit):	7.9711870081584895
Encrypted:	false
SSDEEP:	3072:7LTqUPbDUWkhkjnb97oMGUmKlgaqLGBPpAkyeQjjcjZv9vdNsGP9B0sH2:7XqUHehkl7g/L6P/Uc19vdNTPH0sW
MD5:	0B7C67960E94094684E6AECEFC2E11C4
SHA1:	6D8376B0711E801B39499BF32F43982B161640A3
SHA-256:	5752B65F3EB5E4603C3665ECD2F5C71398FA61EBA9F0F8D71303C458347FCA2C
SHA-512:	7B3E8158AA3B54E7CFF2B0F1637B1B1DB5769124BAC91AEEC8A10732B95C2C76EE44C2E69C1974255A37D4E0120E948910D8190F5B3298B821CF3FDF9A975D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/jccs3BPe4rAcQSKaF2lA3az_GvZfqUs3UxinLPIEkd3NE9w6Z8Az9Kh6Og5tWKT_Okg4mU3aH318M93EmUiCHb4KtuTPNlpAEn_dhx-Hk-dhD_q0J9bfjacW_bX1qpfaCw=w1280
Preview:	.....JFIF.....\Exif..II*.....1.....2...;.....9.....J.....Picasa.Hero Images Inc..Copyright....lhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" photoshop:Credit="Getty Images/Hero Images"> <dc:rights> <rdf:Alt> <rdf:li xml:lang="x-default">Copyright</rdf:li> </rdf:Alt> </dc:rights> <dc:creator> <rdf:Seq> <rdf:li>Hero Images</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>...@ICC_PROFILE.....0ADBE....mntrRGB XYZ .....acspAPPL....none.....-ADBE.....cprt.....2desc...0...kwtpt.....bkpt.....rTRC.....gTRC.....bTRC.....rXYZ.....gXYZ.....bXYZ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\FUGK6LE5.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	76766
Entropy (8bit):	5.665045265444621
Encrypted:	false
SSDEEP:	1536:sPdZEr6EiFo5WuCebZfdGsvTN7lTTj976dTt0p/R:niGxV1odTqp/R
MD5:	F4016515D3D21FF446303A8B93F11AD6
SHA1:	2081A239030E307AE969F47CC3A3882B444CBA80
SHA-256:	A0F43F561A82479F0716D4BC0914783FF612325A50AF17B2D89E6B3246770877
SHA-512:	D6EF24F62C492CCB5D43B573D7E7A11E0E0F5E6B0F7BD94E4DD32E0B1E6226FFE933B76AD82FE286254A5F5D17D4A33D7BEC141FDC4896AAED3CA880B968464
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("MpJwZc");:._.y();..}catch(e){_._DumpException(e)}.try{._.n("n73qwf");:._.y();..}catch(e){_._DumpException(e)}.try{._.n("A4UTCb");:._.y();..}catch(e){_._DumpException(e)}.try{._.n("qAKInc");.var XF=function(a){_.Mn.call(this,a.va);this.B=this.getData("active").wb(!1);this.C=this.O("vyyg5");this.D=_.Mb(_.Nb(this).kc().Ua(function(){var b=this.aa();this.B?b.Ma("qs41qe"):b.Ma("sf4e6b");this.B&&this.C.hf(b.getData("loading message").string(""));this.B||setTimeout(this.st.bind(this),500)}))};_.G(XF,_.Mn);XF.ja=_.Mn.ja;XF.prototype.Hb=function(){return this.B};XF.prototype.setActive=function(a){_.xc(this.aa(),"data-active",a)};.XF.prototype.xk=function(a){var b=a.data.ev;switch(a.data.name){case "data-active":this.B="true"==b,this.D()}};XF.prototype.st=function(){var a=this;_.Mb(_.Nb(this).Ua(function(){var b=a.aa();_.wn(b,"sf4e6b")&&(b.Ka("sf4e6b"),a.B||b.Ka("qs41qe"),a.C.hf(""),a.Ba(_.El))}))()};_.O(XF.p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....N,.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....R...`t.#.cmap...4.....L....cvt .....\...\1..Kfpgm...@...2.....$.gasp...t.....glyf.. ....:..j.'..hdmx..G,...f.....head..G....6...6...rhhea..G.....$....hmtx..G....a.....MOloca..JP.....\v@zmaxp..L,... ... .name..LL.....:.post..M(..... .m.dprep..M<.....S...)x...1.. P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T].....K=..K2 S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw...9..e!.....Q....f.. ....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19916, version 1.1
Category:	downloaded
Size (bytes):	19916
Entropy (8bit):	7.96782347282656
Encrypted:	false
SSDEEP:	384:JiNCb8EbT1rG/3rjJmQ8uLc5ZiRE5HWSiPTI45tKVr6+F7gLLdz:k4zbM3rjEQ8uQPiRERWSGIWtKVrWJ
MD5:	A1471D1D6431C893582A5F6A250DB3F9
SHA1:	FF5673D89E6C2893D24C87BC9786C632290E150E
SHA-256:	3AB30E780C8B0BCC4998B838A5B30C3BFE28EDEAD312906DC3C12271FAE0699A
SHA-512:	37B9B97549FE24A9390BA540BE065D7E5985E0FBFBE1636E894B224880E64203CB0DDE1213AC72D44EBC65CDC4F78B80BD7B952FF9951A349F7704631B903C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`t.#.cmap.....L....cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L..:...j...w.hdmx..F....d.....head..GD...6...6.Y.ihhea..G|.....$...vhmtx..G....k.....\].loca..J.....g.L.maxp..K.... ... ...\name..L.....|..9.post..L..... .m.dprep..L.....: z/.Wx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;..).....;..EoDo....E.E.D.. .`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|..|..|..|..|....o....l%.4.L.SI.&C.6..l`...{...c..\.J.(.2.C....V.A..?.M<nG. .....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{..p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19888, version 1.1
Category:	downloaded
Size (bytes):	19888
Entropy (8bit):	7.96899630573477
Encrypted:	false
SSDEEP:	384:0c6bX9TSzYzCrQH+qXM6C0ouF0xcYye+5x/U3S0X5v+obEgm:0cCV8GuPVyzx/MS0X5v+ol/
MD5:	CF6613D1ADF490972C557A8E318E0868
SHA1:	B2198C3FC1C72646D372F63E135E70BA2C9FED8E
SHA-256:	468E579FE1210FA55525B1C470ED2D1958404512A2DD4FB972CAC5CE0FF00B1F
SHA-512:	1866D890987B1E56E1337EC1E975906EE8202FCC517620C30E9D3BE0A9E8EAF3105147B178DEB81FA0604745DFE3FB79B3B20D5F2FF2912B66856C38A28C07EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....P...`u.#.cmap...0.....L....cvt .....H...H+~..fpgm...(...3...._...gasp...\..... ....glyf...h..:q..i..+ Ohdmx..F....f.....head..GD...6...6...\hhea..G|.....$.&..hmtx..G....d.....E#loca..J.....\s@.maxp..K.... ... .name..K.....~..9.post..L..... .m.dprep..L.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T]. ....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw. ..9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19824, version 1.1
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	7.970306766642997
Encrypted:	false
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C773527542228478CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf...L..:+..j.....hdmx..Fx...g.....head..F....6...6.j.zhhea..G.....$....hmtx..G8...]....Vlloca..I.....?.#.maxp..Kt... ... .name..K.....t.U9.post..Ld..... .m.dprep..Lx.....I.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;..).....;..EoDo....E.E.D..`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\adobe-pdf-icon-logo-png-transparent-285x300[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 285 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	34353
Entropy (8bit):	7.979805722823804
Encrypted:	false
SSDEEP:	768:N9xfTAXr2MJkBTCNmDcEKzOYEUtVD3KdvW95:lmrJMCDzIU3WdvQ
MD5:	2499C2758E9581401BDA79616C11BC23
SHA1:	3484F31C3E550A20BC52E9D124038E24869D3253
SHA-256:	3CF94D7F901B97A6697F2E7AC4B4688779B0C705F48939A2E09BC86D7C24E350
SHA-512:	BC9254D9D2B4E7FD407BF98F0E980AD0E89A91D0AB99AB8BD8F7E6EA0C7604D7FA7895646C1960C4AB458AE09998C1A231A51411954E0DEF0187477D1E6C864 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh6.googleusercontent.com/MPisMsKgfWPH_wyQtxwiETVIZ7-3oktBmkawItaNgMz0NXMp-_nwwU28HJuThaptRJp6_Rl5ZlY8PTPJpFX_7uQ=w16383
Preview:	.PNG.....IHDR.....,.....Lgs....sBIT....|.d... .IDATx..]y..E..V..g6...$.$.....>$.....\|..$..>...Q.DPy..P.y..@..GB.....{..t.?.....$...lwW..W.....~U..T.JU.R..T.*U.JU.R..T.*Uic#2.. T.J.H.....U*#UA.@...J..9.#...+9.R.(9....r...^.M.d.....,.Je...tXCK>..s.677..R.PJ.[.*.....J)..<r.....3ox..W.Q..,6...j...6..U.....{..#..l..4pD)..p]..\....X.n...>...n..]x..'.]W..D.\....I.....M....-.~t .CQ.;..d.:...,BH..~.N:.;....4..:.....L.k.9..N.@C___.o.@q..I.?.e.s1L....).r.'..B2;....>...O.>.@..c..@gs.?%Qb...$J.r.4.|...1b.v@.aRJA....|...O3.d.L.....!f.QJ.....G.}.....7o. .@C...r.U.....k...?..<..i...(Y.O.3./..e...8.....d..f.....n.....h..l.U.o.b.*Y..h.0...@=.a....g....c.2b.k..*kpd...Y<===p].6m...r..?.....S..V.a.r..1..j.....(#.j.....:.T..[Y2...,f.8..d2.T*.t:.T*...N. [..S.N.....H.m.[=.k.....!..].....c'..ZU.L..4lY}..p.....9s..kG...W%.UQ.#m=.FX..T..-.&>.m.x.N*.BMM.2..jjj.b..tuu...../....v.3..x....z2(X=U.P.t"....|..~...(Y6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F 4
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 n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==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= {},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a. hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListene r(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;-- warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint- xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1749
Entropy (8bit):	5.23061720471129
Encrypted:	false
SSDEEP:	48:IOEaRqP/OXaRWO1aNROEaNKCOXaNbOpaNaOEa21Opa1U:IOEaeOXaYO1aNROEaNKCOXaNbOpaNaO1
MD5:	EB0CD88A60302BF95C95366E2C82FF29
SHA1:	47FF9E436F413113B215513E0EF08ED150AA3C2A
SHA-256:	1CDD30E7B0C4E941967839C5DD5671F1A95648EE30E61B554513B3692F8D1640
SHA-512:	D2EAF170280D1562C5DE8118278273BA8827A37712944B2ADD9159D50B351FDF1D1719DB56B9361180D7F00AEC07E4E958FD16F3BF79205302DF179C468D7050
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. src: u rl(https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font- weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.@font-face {. font-famil y: 'Roboto';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff ');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92F r1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. font-display: swap;. src

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25226
Entropy (8bit):	5.511502397293664
Encrypted:	false
SSDEEP:	384:0YRgyq+e8mseA2yhaOP4h75d6oC9gd4gPYnE+shEhMer7VtMpOu8g5kQZgOL+WL0:g+1lewoL1qoCCechwKguddLa
MD5:	A5135971F228CB828E685A57AEAB4AE3
SHA1:	7D504C0F2E59B084D18CD4C8FE8688E99B92CB86
SHA-256:	174502AF11014B8EA0CFC43F0053BA6BF66C8C31448B622DA0957647DC63BC4C
SHA-512:	47350A7653281006C49C9CA1233F6D91B66E2C57C362B7E461791A9FA9919F07880805B264F07717E27A39A0E358C6C7F27097FED59D5CAA86B0F7D0E83DB18D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube-nocookie.com/s/player/1fe59655/player_ias.vflset/en_US/embed.js
Preview:	(function(g){var window=this;'use strict';var NJa=function(a,b){var c=(b-a.i)/(a.l-a.i);if(0>=c)return 0;if(1<=c)return 1;for(var d=0,e=1,f=0,h=0;8>h;h++){f=g.Mn(a,c);var l= (g.Mn(a,c+1E-6)-f)/1E-6;if(1E-6>Math.abs(f-b))return c;if(1E-6>Math.abs(l))break;else f<b?d=c:e=c,c-=(f-b)/l}for(h=0;1E-6<Math.abs(f-b)&&8>h;h++)f<b?(d=c,c=(c+e)/2):(e =c,c=(c+d)/2),f=g.Mn(a,c);return c},A3=function(){return{D:"svg",.V:{height:"100%",version:"1.1",viewBox:"0 0 110 26",width:"100%"},S:[{D:"path",Nb:!0,K:"ytp-svg-fill",V: {d:"M 16.68,.99 C 13.55,1.03 7.02,1.16 4.99,1.68 c -1.49,.4 -2.59,1.6 -2.99,3 -0.69,2.7 -0.68,8.31 -0.68,8.31 0,0 -0.01,5.61 .68,8.31 .39,1.5 1.59,2.6 2.99,3 2.69,.7 13.4 0,.68 13.40,.68 0,0 10.70,.01 13.40,-0.68 1.5,-0.4 2.59,-1.6 2.99,-3 .69,-2.7 .68,-8.31 .68,-8.31 0,0 .11,-5.61 -0.68,-8.31 -0.4,-1.5 -1.59,-2.6 -2.99,-3 C 29.11,.98 18.40,.99 18.40,.99 c 0,0 -0.67,-0.01 -1.71,0 z m 72.21,.90 0,21.28 2.78,0 .31,-1.37 .09,0 c .3,.5 .71,.88 1.21,1.18 .5,.3 1.08,.40 1.68,.40 1.1,0 1.99,-0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829823522211244
Encrypted:	false
SSDEEP:	192:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	8A99CE81EC2F89FBCA03F2C8CF1A3679
SHA1:	58F9EF32D12A5DA52CBAB7BD518BCC998FC59EF9
SHA-256:	362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF
SHA-512:	930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=585b051251

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free-v4-shims.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728641238865369
Encrypted:	false
SSDEEP:	768:0Uh31lPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q
MD5:	390B4210E10C744C3C597500BCF0B31A
SHA1:	2600C7C2F25D7DBCBC668231601E426010DC6489
SHA-256:	C2819CA1F7AD1AF7BA53C4EDFDFD395C547BCB16D29892A234D7860C689ED929
SHA-512:	E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBBF13907D5901D76FFE127D92FDD7493853646F83F5985CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\home[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):	47716
Entropy (8bit):	5.7757889289910525
Encrypted:	false
SSDEEP:	384:8QGculh0YP9w/PoIYy2izD/E8+5qz+lhkD+DHq+ViTT+hhaWUWwSTdG+ng+qHPl6:AculKPpb8jqAkoHR9aWRM+ngLg
MD5:	1A6820BCEC81BE35FA6DCFD5D9952CC2
SHA1:	329C13B34D1B3C0CB5A75000404056648CC936ED
SHA-256:	075BA605CE66FDEA585D29826F5756397A54503F807270E0EAEF907D67E5B485
SHA-512:	47D626AF8C7E7223336E74464B8A1B198CD31B3F328EAB961093F64307ACB7E799E8C83750A4D013F8B4C7411D2171D264409ECEB96C1570170D6C98D68A143E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="ogObHoVzJ3rofL55GT/KFQ">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="ogObHoVzJ3rofL55GT/KFQ">function _DumpException(e) {throw e;}</script><script nonce="ogObHoVzJ3rofL55GT/KFQ">_docs_flag_initialData={"atari-eiicg":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","iIcm":{"eui":"AHKXmL0awsXsyZ7yEClPc-ibJXWgubPJDezipjeAjptC1SEWqu2ON525UZp5JhCXm1uPYIszVU1N","je":1,"sstu":1623351136102000,"si":"CLbQwJ7ejfECFReyHwodLkEPrw","gsc":null,"ei":[14101510,14101046,5713049,14101550,5706836,5703022,5732942,5714628,5720060,14101534,14100834,5727317,5721004,5734571,5719651,5703839,5707711,5711808,5729072,5722370,5711850,5713207,5734691,5708870,5714550,5712373,14101530,5713211,14101502,5712211,5709892,14101462,5720925,5735806,5704621,5706832],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\popper.min[1].js	
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\rs=AGEqA5lU6_p3Xs6-mgc-DsOLuNR8p1pPPg[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):	417394
Entropy (8bit):	5.733575489337279
Encrypted:	false
SSDEEP:	3072:nZy79lbL9hbYY88/K5RSoZJcPixSemtO+6byufSuDIT1:q9lbLLxlAN4ixSpf
MD5:	0BFE0410F4DD6AB56086A8CBA64C4D44
SHA1:	955A2AB0F81ED59B0EC9DEB3F47C4497903066CF
SHA-256:	26434455023C8B96A93DEA398EAD43B3F235658B87CBE33E7DE1F5E94E4118EB
SHA-512:	9D792F01616239983F9739CA8346163A29A310E362B64138CB43E0BD76720251993B02387637D2946671BDE2CFD50A00EC3CE91C48E1F6E6715E72DFAFB76F4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/atari/_/ss/k=atari.vw.H9gJArw3r2Q.L.I11.O/d=1/rs=AGEqA5lU6_p3Xs6-mgc-DsOLuNR8p1pPPg
Preview:	/*! normalize.css v2.1.1 | MIT License | git.io/normalize */article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,video{display:inline-block}audio:not([controls]){display:none;height:0}[hidden]{display:none}html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}a:focus{outline:thin dotted}a:active,a:hover{outline:0}h1{font-size:2em;margin:.67em 0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}hr{box-sizing:content-box;height:0}mark{background:#ff0;color:#000}code,kbd,pre,samp{font-family:monospace,serif;font-size:1em}pre{white-space:pre-wrap}q{quotes:"\201C" "\201D" "\2018" "\2019"}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:0}fieldset{border:1px solid silver;margin:0 2px;padding:.35em .625em .75em}legend{bo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	47570
Entropy (8bit):	5.730864923241311
Encrypted:	false
SSDEEP:	768:Lc/d9SvRuAWXM0FUBMVYY1tTrvqQPFJ/N4avO6yhw:8DM6qY1prvh1bvO6yhw
MD5:	CBEB6D1EB9CB3501AD133EEAD845037A
SHA1:	025C11A397BD5E53273CBD30500ABA32E94FB114
SHA-256:	B56E748865923BD6E079107FB5FFED2A5272E8EF734F7018DCF220392C21EAA0
SHA-512:	9E45F741CCDF4EB3BB803D31BF09B735B7CAF49B5EF00B67476D353E9816F2209ACFA9AE94671F4A662867F1C3081784DA4C937FDBD631DD02D329F02E3E648
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/app/so?bc=1&origin=https%3A%2F%2Fpolicies.google.com&cn=app&pid=269&spid=545&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="VQZhUhg3w/TqRv+z5grRQQ">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"4258451908995687362","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1623351155359563,178774235,771822610]\n","ZwjLXe":545,"cfb2h":"boq_onegooglehttpserver_20210607.07_p0","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333],"gGcLoe":false,"ikfjnc":["https://policies.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"OneGoogleWidg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\team[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):	70518
Entropy (8bit):	5.8069199689885265
Encrypted:	false
SSDEEP:	1536:RkWWqAkoHRik82eckj5y9dDD2x5Dtlnf+qdA:RXa8Jci5y7DD2x5jnfjA
MD5:	9E8E838E0570B3E0E6241B07F4982393
SHA1:	5B2EB15B6C3110E743ED1290D521F3E89027B1CF
SHA-256:	253DC2F9F7648EBBF4436922EC7C2EDBF9142494EF6AD09EE0C1ADCDE87F7D7C
SHA-512:	546C9316A157E7C3974BED6FC93AEF454D1450AF0768B54895CCAE381563C96CEAC19928073CA4BE8BA0E23B635B9C7D696740EF60CBC6C04104EF4B9A23D3A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\team[1].htm	
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="ta5Nnf75ak7AQzzwZEk7EA">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="ta5Nnf75ak7AQzzwZEk7EA">function _DumpException(e) {throw e;}</script><script nonce="ta5Nnf75ak7AQzzwZEk7EA">_docs_flag_initialData={"atari-eiicg":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","ilcm":{"eui":"AHKXmL2veDd2egqWfGxzOEC_TgNshvJjbkxYUcXDVd8u0B4LdrkSvjmJqp1R_TonbF-HzbaA7WxA","je":1,"sstu":1623351141659000,"si":"CJrlk6HejfECFRUaHwodyaQFRg","gsc":null,"ei":[5721004,5719651,5720925,5712211,14100834,5727317,5720060,14101534,5707711,5704621,5709892,5708870,5729072,5706832,5722370,5734691,5714550,5713207,5714628,5735806,5703839,14101462,14101502,5713049,5703022,5711850,14101530,5734571,5732942,5711808,14101510,14101046,5706836,5712373,5713211,14101550],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u-440qyriQwlOrhSvowK_l5-fCZK[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23600, version 1.1
Category:	downloaded
Size (bytes):	23600
Entropy (8bit):	7.973583674109776
Encrypted:	false
SSDEEP:	384:OMPViqjFD/7v1VG9bCaNwTTRz10p2dF5rnmaMfmF1tKlYFwWajBob/T670WyDLrx:hNdjhRV0bCaNwvRz10pAF5CaMfm8Iqjj
MD5:	69F09800F4F6479D06E44EBA837DF872
SHA1:	5C889B1BEE3D4E75A5FC0749617A15C0E6922072
SHA-256:	8E0F8D862D80DB8B358C03FCCD1FCEB993DEA6A22569620BCD0959806D3D1D12
SHA-512:	1EFFE91D2A3BC1C6442E9B8012EA6806AAB60FCCFB1947F011E281170FE8070FFA5B9E6096363B2B3908C8BCF0D49AF3DDD1BF004E87438B6F0C450FE968F105
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/merriweather/v22/u-440qyriQwlOrhSvowK_l5-fCZK.woff
Preview:	wOFF.....\0.....t.....GDEF.....S...p....GPOS..... ... DvLuGSUB.....s.e.OS/2.....O...`U.Kcmap.....j,.|cvt .....8.....~.lfpgm.....F...mA..|gasp...(.....glyf...0..F...y.e.a.head..S....6...6.).7hhea..SL... ...$....hmtx..Sl...c....VG(.loca..U.....b.C.maxp..W.... ... .g.pname..W.....r:.Q.post..Y....~.....yujprep..[.....Z.,.x.....'@T7H.....$ AJ...`f...<.....V.vy.QN.....>...Q.m..y.2...k.....DFLT.....x...n-Q...am.Fp}.k.m.m....A.2.de.d...~.lc.,..8.v.;F...O.Q}.....X^..NY(b.O....o>....[7.+e..#.O..|...../...[...M..T..pH$..*..D6.T..#....6.O...Sc..R..Z..F>..Q.....,E..O._..hy....V|.|x...*f..b.X+6?x~...:Z..1b..'z".+Z.-:.O.....`..a...l...I3V@....L.....Xj.U;.bG#1.t|.....Q.7....O.2.....J.....3<R....q..x...!.....K..o#&g.....UL.....}..d..#.L.u^..p..|....v.....S.s..C...k.3.^.6.....s+`..A.x.c`a..8.....).....B3.1.1...@)8`.b&.'8.Y.....(.....X4.....)..f..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u-4n0qyriQwlOrhSvowK_l52xwNZWMf8[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23260, version 1.1
Category:	downloaded
Size (bytes):	23260
Entropy (8bit):	7.976160585728166
Encrypted:	false
SSDEEP:	384:Bv0MPVryqjFD/7v15tcgxwkH5+WVPgq7FGj2mQf4MBpgt3Re+X8NM7v/9J9PJ3sN:tzNRjhRAG5f+2I2my4YmtMNNMrL9pssC
MD5:	BA56EA84B8084B7FF9677F50D3CD81BD
SHA1:	799C0C07912F6996B80459937AC097813B6B461C
SHA-256:	649C6472A611C5BCFEBB341109E5754F205EE57550F5614577C6B6CB963D17AE
SHA-512:	724487602C085EBA3D79D74A40BFF75A3123241CAE759A27D21430813C0ED6D90899E826A7BE49FBABCD8586DD08DB76D86BB9BE4C8FD9B284AB747727A0A29
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/merriweather/v22/u-4n0qyriQwlOrhSvowK_l52xwNZWMf8.woff
Preview:	wOFF.....Z.....p.....GDEF.....S...p....GPOS..... ... DvLuGSUB.....s.e.OS/2.....P...`W..8cmap.....j,.|cvt .....<.....fpgm.....F...mA..|gasp...,.....glyf...4..E...uD...head..Q....6...6.M.7hhea..Q.... ...$....hmtx..R...._...._B".loca..T|.....`..maxp..V.... ... .g.oname..V.....Z7.O.post..W....~.....yujprep..Z<.....Z.,.x.....'@T7H.....$ AJ...`f...<.....V.vy.QN.....>...Q.m..y.2...k.....DFLT.....x...n-Q...am.Fp}.k.m.m....A.2.de.d...~.lc.,..8.v.;F...O.Q}.....X^..NY(b.O....o>....[7.+e..#.O..|...../...[...M..T..pH$..*..D6.T..#....6.O...Sc..R..Z..F>..Q.....,E..O._..hy....V|.|x...*f..b.X+6?x~...:Z..1b..'z".+Z.-:.O.....`..a...l...I3V@....L.....Xj.U;.bG#1.t|.....Q.7....O.2.....J.....3<R....q..x...!.....K..o#&g.....UL.....}..d..#.L.u^..p..|....v.....S.s..C...k.3.^.6.....s+`..A.x.c`a.....).....B3.1.1.2.....1.....AI.....,.....ArL:L....3.

C:\Users\user\AppData\Local\Temp\~DF22D972DD4D0EC9B9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	182270
Entropy (8bit):	2.117329604542338
Encrypted:	false
SSDEEP:	768:9KEmHZZy1AiCvUzmKAeCm67KLZrjHuiwUzmKAeCm67KLZrjHuiiUzkUz/Uz9:utj4mtj42
MD5:	F80D133C0BE7FF986E4996A697DBFAF5
SHA1:	4B5EEBBC61B1DCA0F7FBDB211E964ED07A1DF2C5
SHA-256:	B77F0950ABC25F315FF3B6A2FB0169518C6B18E9C63AE45DC56A19CB3B2235C6
SHA-512:	A055A504322ED2F425EF950F6A62A36EC847364AAB7AADD2ABFDCDFDFB227DB657886BC6BD85B78519E112A40E165298D414AB9450102F0B0BDF05509A9310E1
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF22D972DD4D0EC9B9.TMP	
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 20:51:57.544938087 CEST	192.168.2.4	8.8.8.8	0x896a	Standard query (0)	lh6.google usercontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:51:58.248922110 CEST	192.168.2.4	8.8.8.8	0xc3c4	Standard query (0)	lh5.google usercontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:22.377317905 CEST	192.168.2.4	8.8.8.8	0x1be3	Standard query (0)	lh4.google usercontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:22.381923914 CEST	192.168.2.4	8.8.8.8	0xde69	Standard query (0)	lh3.google usercontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:27.692681074 CEST	192.168.2.4	8.8.8.8	0xb84f	Standard query (0)	kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:30.356286049 CEST	192.168.2.4	8.8.8.8	0x4d18	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:30.856539965 CEST	192.168.2.4	8.8.8.8	0x4758	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.218533993 CEST	192.168.2.4	8.8.8.8	0x565c	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.482808113 CEST	192.168.2.4	8.8.8.8	0x29fb	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.489989042 CEST	192.168.2.4	8.8.8.8	0xc06e	Standard query (0)	smtpro101.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.871527910 CEST	192.168.2.4	8.8.8.8	0x58f1	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:33.890862942 CEST	192.168.2.4	8.8.8.8	0x17a0	Standard query (0)	www.youtube-nocookie.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 20:51:57.603457928 CEST	8.8.8.8	192.168.2.4	0x896a	No error (0)	lh6.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:51:57.603457928 CEST	8.8.8.8	192.168.2.4	0x896a	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 20:51:58.310225010 CEST	8.8.8.8	192.168.2.4	0xc3c4	No error (0)	lh5.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:51:58.310225010 CEST	8.8.8.8	192.168.2.4	0xc3c4	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:22.435889959 CEST	8.8.8.8	192.168.2.4	0x1be3	No error (0)	lh4.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:22.435889959 CEST	8.8.8.8	192.168.2.4	0x1be3	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:22.464764118 CEST	8.8.8.8	192.168.2.4	0xde69	No error (0)	lh3.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:22.464764118 CEST	8.8.8.8	192.168.2.4	0xde69	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:27.757920980 CEST	8.8.8.8	192.168.2.4	0xb84f	No error (0)	kanaan.s3.eu-de.cloud-object-storage.appdomain.cloud	s3.eu-de.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:27.757920980 CEST	8.8.8.8	192.168.2.4	0xb84f	No error (0)	s3.eu-de.cloud-object-storage.appdomain.cloud		158.177.118.97	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:30.409470081 CEST	8.8.8.8	192.168.2.4	0x4d18	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:30.916949034 CEST	8.8.8.8	192.168.2.4	0x4758	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 20:52:30.916949034 CEST	8.8.8.8	192.168.2.4	0x4758	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.282248020 CEST	8.8.8.8	192.168.2.4	0x565c	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:31.545521975 CEST	8.8.8.8	192.168.2.4	0x29fb	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 20:52:31.553793907 CEST	8.8.8.8	192.168.2.4	0xc06e	No error (0)	smtpro101.com		172.67.194.129	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.553793907 CEST	8.8.8.8	192.168.2.4	0xc06e	No error (0)	smtpro101.com		104.21.20.217	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.930829048 CEST	8.8.8.8	192.168.2.4	0x58f1	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:31.930829048 CEST	8.8.8.8	192.168.2.4	0x58f1	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 10, 2021 20:52:33.962543011 CEST	8.8.8.8	192.168.2.4	0x17a0	No error (0)	www.youtube-nocookie.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 20:51:57.748497963 CEST	142.250.180.225	443	192.168.2.4	49751	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:51:57.749181032 CEST	142.250.180.225	443	192.168.2.4	49752	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:51:58.460120916 CEST	142.250.180.225	443	192.168.2.4	49753	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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
Jun 10, 2021 20:51:58.461236954 CEST	142.250.180.225	443	192.168.2.4	49754	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:52:22.587821960 CEST	142.250.180.225	443	192.168.2.4	49779	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:52:22.594563007 CEST	142.250.180.225	443	192.168.2.4	49778	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:52:22.624337912 CEST	142.250.180.225	443	192.168.2.4	49781	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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		
Jun 10, 2021 20:52:22.629530907 CEST	142.250.180.225	443	192.168.2.4	49780	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	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 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
Jun 10, 2021 20:52:31.006505966 CEST	104.18.11.207	443	192.168.2.4	49791	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:52:31.008678913 CEST	104.18.11.207	443	192.168.2.4	49790	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:52:31.646434069 CEST	172.67.194.129	443	192.168.2.4	49797	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Apr 23 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Apr 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:52:31.651240110 CEST	172.67.194.129	443	192.168.2.4	49796	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Apr 23 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Apr 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 20:52:32.027069092 CEST	104.16.18.94	443	192.168.2.4	49799	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 20:52:32.028733015 CEST	104.16.18.94	443	192.168.2.4	49798	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6784 Parent PID: 800

General

Start time:	20:51:55
Start date:	10/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff690680000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6888 Parent PID: 6784

General

Start time:	20:51:55
Start date:	10/06/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6784 CREDAT:17410 /prefetch:2
Imagebase:	0xf80000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021