ID: 882709
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 17:20:05
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

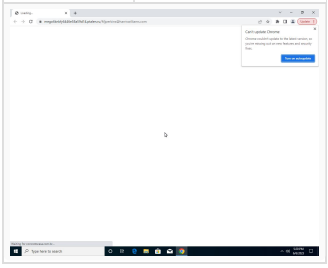
Windows Analysis Report

https://t.email.currys.co.uk/r/?id=h7aa4a341,8b3374d,743904&p1=concretocasa.com.br%2Fhtml%2F...

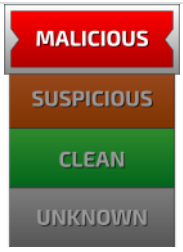
Overview

General Information

Sample URL:	https://t.email.currys.co.uk/r/?id=h7aa4a341,8b3374d,743904&p1=concretocasa...cretocasa.com.br%2Fhtml%2Fssl%2Ffyvqcw/anBlcmtpbnNAaGFycmlzd2lsbGlhbXMuY29t
Analysis ID:	882709
Infos:	YARA



Detection



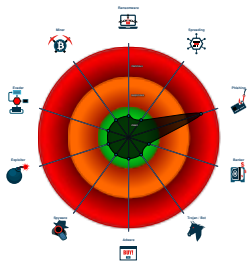
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on sh…
- Phishing site detected (based on im…
- HTML page contains hidden URLs o…
- Yara signature match
- Invalid 'forgot password' link found
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6592 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://t.email.currys.co.uk/r/?id=h7aa4a341,8b3374d,743904&p1=concretocasa.com.br%2Fhtml%2Fssl%2Ffyvqcw/anBlcmtpbnNAaGFycmlzd2lsbGlhbXMuY29t MD5: C817D9E0D995276EC89E4C89AFC19694)
  - chrome.exe (PID: 3752 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2200 --field-trial-handle=1760,i,5014297833913630884,728955890353194336,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: C817D9E0D995276EC89E4C89AFC19694)
- **cleanup**

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
dropped/chromecache_151	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x482:$c8: while(!![]) • 0x4a1:$d1: parseInt(_0x48d4ad(0x1c1))/0x1+parseInt(_0x48d4ad(0x1c6))/0x2+parseInt(_0x48d4ad(0x1b2))/0x3+parseInt(_0x48d4ad(0x1bf))/0x4+parseInt(_0x48d4ad(0x1d0))/0x5*(parseInt(_0x48d4ad(0x1aa))/0x6)+ • 0x4c0:$d1: parseInt(_0x48d4ad(0x1c6))/0x2+parseInt(_0x48d4ad(0x1b2))/0x3+parseInt(_0x48d4ad(0x1bf))/0x4+parseInt(_0x48d4ad(0x1d0))/0x5*(parseInt(_0x48d4ad(0x1aa))/0x6)+parseInt(_0x48d4ad(0x1b3))/0x7+- • 0x4df:$d1: parseInt(_0x48d4ad(0x1b2))/0x3+parseInt(_0x48d4ad(0x1bf))/0x4+parseInt(_0x48d4ad(0x1d0))/0x5*(parseInt(_0x48d4ad(0x1aa))/0x6)+parseInt(_0x48d4ad(0x1b3))/0x7+-parseInt(_0x48d4ad(0x1ba))/0x8*(

HTML

Source	Rule	Description	Author	Strings
3.6.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on shot match)

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

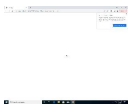
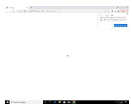
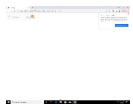
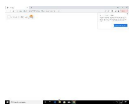
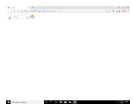
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading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

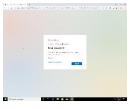
Screenshots

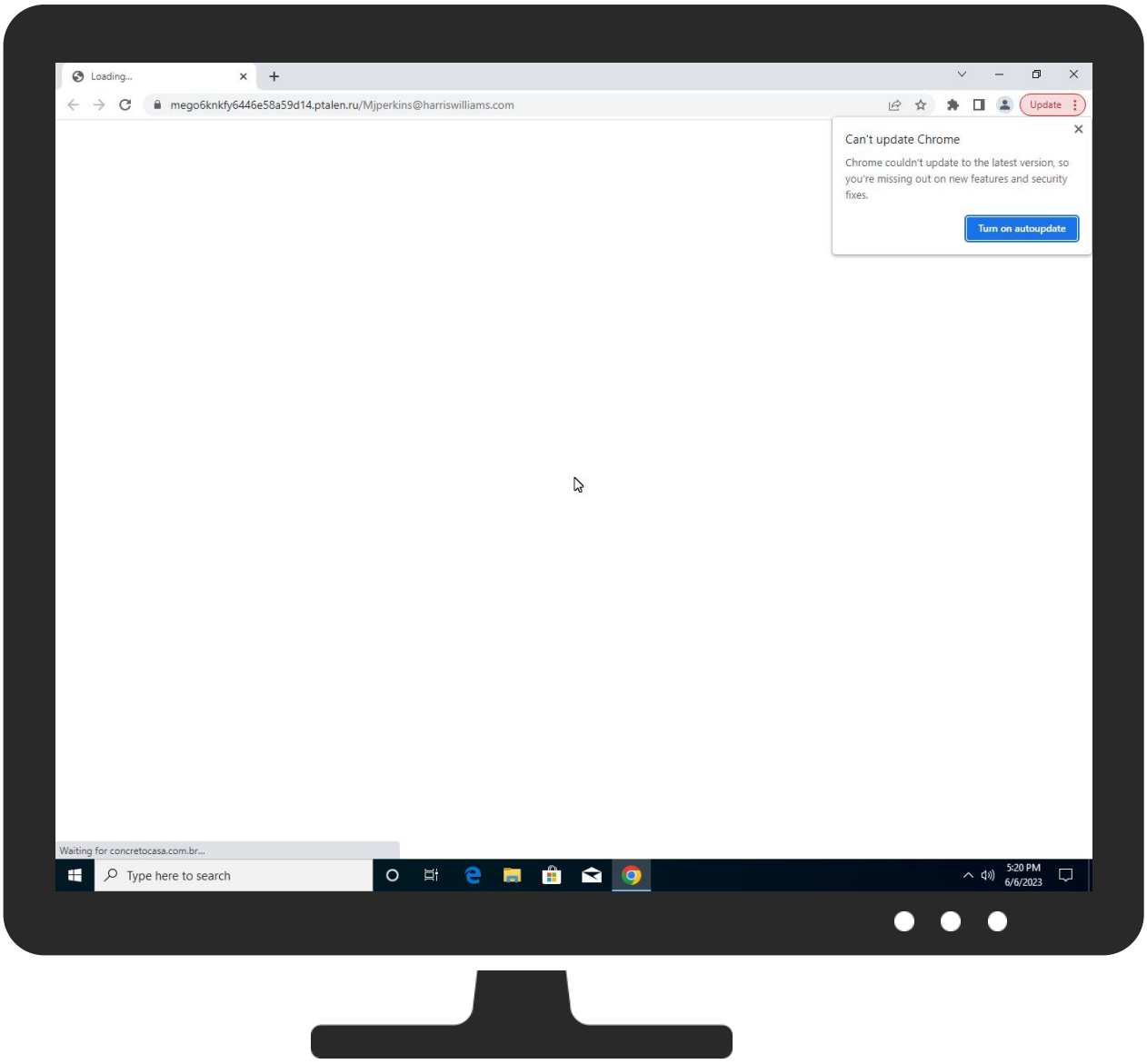
Thumbnails

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
https://t.email.currys.co.uk/r/?id=h7aa4a341,8b3374d,743904&p1=concretocasa.com.br%2Fhtml%2Fssl%2Ffyvqcw/anBlcmtpbnNAaGFycmlzd2lsbGlhbXMuY29t	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

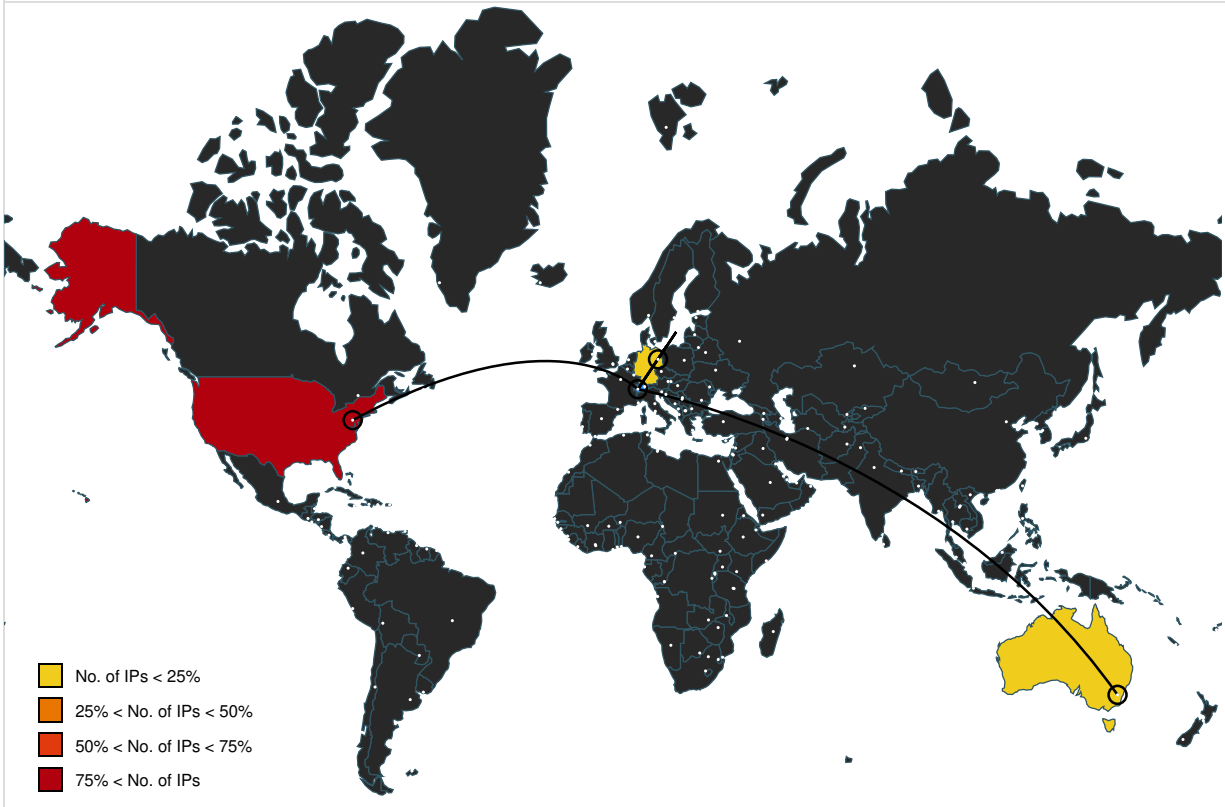
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mego6knkfy6446e58a59d14.ptalen.ru	172.67.173.146	true	false		unknown
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	142.250.186.77	true	false		high
challenges.cloudflare.com	104.18.7.185	true	false		high
concretocasa.com.br	185.201.10.27	true	false		unknown
www.google.com	142.250.185.164	true	false		high
clients.l.google.com	142.250.185.174	true	false		high
dixonsretail-mkt-prod1-ssl1-2796-396715988.eu-west-1.elb.amazonaws.com	52.31.211.174	true	false		high
unpkg.com	104.16.126.175	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
t.email.currys.co.uk	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://concretocasa.com.br/html/ssl/fyvqcw/anBlcmtpbnNAaGFycmlzd2lsbGlhbXMuY29t	false		unknown
https://mego6knkfy6446e58a59d14.ptalen.ru/e3b52af7f42b89943d3cf517518321e0647f4edf9d1ccPASe3b52af7f42b89943d3cf517518321e0647f4edf9d1ce	true		unknown
https://mego6knkfy6446e58a59d14.ptalen.ru/Mjperkins@harriswilliams.com	true		unknown
https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/turnstile/if/ov2/av0/rcv0/0/dp0qq/0x4AAAAAAADnPIDROrmt1Wwj/light/normal	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.35	unknown	United States		15169	GOOGLEUS	false
104.18.7.185	challenges.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
172.217.18.4	unknown	United States		15169	GOOGLEUS	false
52.31.211.174	dixonsretail-mkt-prod1-ssl1-2796-396715988.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.181.234	unknown	United States		15169	GOOGLEUS	false
185.201.10.27	concretocasa.com.br	Germany		47583	AS-HOSTINGERLT	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.174	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
142.250.184.227	unknown	United States		15169	GOOGLEUS	false
172.67.173.146	mego6knkfy6446e58a59d14.ptalen.ru	United States		13335	CLOUDFLARENETUS	false
142.250.186.77	accounts.google.com	United States		15169	GOOGLEUS	false
104.16.126.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.2
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882709
Start date and time:	2023-06-06 17:20:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://t.email.currys.co.uk/r/?id=h7aa4a341,8b3374d,743904&p1=concretocasa.com.br%2Fhtml%2Fssl%2Ffyvqcw/anBlcmtpbnNAaGFycmlzd2lsbGlhbXMuY29t
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	3
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@28/43@12/191

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe
- Excluded IPs from analysis (whitelisted): 142.250.186.35, 34.104.35.123, 178.79.242.128, 93.184.221.240, 95.101.54.113, 209.197.3.8
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, login.live.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, t.email.currys.co.uk.cname.campaign.adobe.com
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

Chrome Cache Entry: 144

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (31803)
Category:	downloaded
Size (bytes):	31842
Entropy (8bit):	5.341705273940054
Encrypted:	false
SSDEEP:	
MD5:	6470A918BA1FD4B8D0882DF0269DDB82
SHA1:	97814FDAB64AA7D1B30F082F9EB272D4B1CE18A2
SHA-256:	FD4CE12A87594281AFCEE9C73A40FE7ACC282BCC9E764FBB3AFA1481A96A091E
SHA-512:	B8CB57985DBC03601BFC924EDADFEF62195A6BFDDA8543A08F565FDBB339ACEA3CFFE7DC4D4547D3F134965EBC9E39A3ACBA8E0635CCDD5F4D88F14BE72C163D
Malicious:	false
Reputation:	low
URL:	https://unpkg.com/axios@1.4.0/dist/axios.min.js
Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e="undefined"!=typeof globalThis?globalThis:e||self).axios=t()}(this,(function(){"use strict";function e(t){return e="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e},e(t)}function t(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}function n(e,t){for(var n=0;n<t.length;n++){var r=t[n];r.enumerable=r.enumerable||!1,r.configurable=!0,"value"in r&&(r.writable=!0),Object.defineProperty(e,r.key,r)}}function r(e,t,r){return t&&n(e.prototype,t),r&&n(e,r),Object.defineProperty(e,"prototype",{writable:!1}),e}function o(e,t){return function(e){if(Array.isArray(e))return e}(e)||function(e,t){var n=null==e?null:"undefined"!=typeof Symbol&&e[Symbol.iterator]||e["@@iterator"];if(nul

Chrome Cache Entry: 145

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4C
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

Chrome Cache Entry: 146

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (19175)
Category:	downloaded
Size (bytes):	19176
Entropy (8bit):	5.333007695939954
Encrypted:	false
SSDEEP:	
MD5:	21A964474A4841C3E62893476CFEC550
SHA1:	AF06EB1E31D451FE557B7581E707CD88A3107491
SHA-256:	FB479D9C5DB685793FD57B4CACB188D2AA9AB40D660D54E1CF35D0F54B390C12
SHA-512:	E5F303A6E296A76FBC93DF3E9E6960C0CD8745DCA6050895DBE5AB9F00005C9A3DB74923E912FF3009D2A0960E53CC20F189A58E5CECE531117DA2227D19FAC
Malicious:	false
Reputation:	low
URL:	https://challenges.cloudflare.com/turnstile/v0/g/68662470/api.js?onload=_cf_chl_turnstile_l&render=explicit

Preview:	"use strict";(function(){function R(e,o){return o!=null&&typeof Symbol!="undefined"&&o[Symbol.hasInstance]?!!o[Symbol.hasInstance](e):R(e,o)}function Ie(e){if(Array.isArray(e))return e}function Ae(e,o){var n=e==null?null:typeof Symbol!="undefined"&&e[Symbol.iterator]||e["@@iterator"];if(n!=null){var s=[],d=!0,h=!1,f,M;try{for(n=n.call(e);!(d=(f=n.next()).done)&&(s.push(f.value),!(o&&s.length===o));d=!0);}catch(z){h=!0,M=z}finally{try{!d&&n.return!=null&&n.return()}finally{if(h)throw M}}return s}}function we(){throw new TypeError("Invalid attempt to destructure non-iterable instance.\nIn order to be iterable, non-array objects must have a [Symbol.iterator]() method.")}function ue(e,o){(o==null||o>e.length)&&(o=e.length);for(var n=0,s=new Array(o);n<o;n++)s[n]=e[n];return s}function Te(e,o){if(e){if(typeof e=="string")return ue(e,o);var n=Object.prototype.toString.call(e).slice(8,-1);if(n==="Object"&&e.constructor&&(n=e.constructor.name),n==="Map"||n==="Set")return Array.from(n);if(n===""

Chrome Cache Entry: 147	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/o/61f8e92fa388cdf9e29b4e7455e01865647f4ee25ce22
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-. .

Chrome Cache Entry: 148	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 92 x 11, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	61
Entropy (8bit):	4.035372245524405
Encrypted:	false
SSDEEP:	
MD5:	354F8CEA999B2705EC9EA3C705B3AE81
SHA1:	D78201EE68BC019A37E1647815820B951AB7AA84
SHA-256:	CA8CBB74C18E308E8DD105484B76EF87A042FF0327CD283529867EEFCA5E657E
SHA-512:	922CEEFDA7D2832B1EDEFC822745E30C54C6A6390D2D1C65BD835CFDC89F665B9B5634B71D666A2C96FFB9A10DC1FD6E96EA91E9D68802A148246897558371 8
Malicious:	false
Reputation:	low
URL:	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/img/7d31a3feec7e9159/1686064851305/uqo8D8Icolb3Bdi
Preview:	.PNG.....IHDR...\.....}.}@....IDAT.....$.....IEND.B`.

Chrome Cache Entry: 149	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (50758)
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD A
Malicious:	false
Reputation:	low

URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/boot/61f8e92fa388cdf9e29b4e7455e01865647f4edfc4936
Preview:	/*!. * Bootstrap v4.1.3 (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,h){"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 l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

Chrome Cache Entry: 151

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6149), with no line terminators
Category:	downloaded
Size (bytes):	6149
Entropy (8bit):	5.28332400916268
Encrypted:	false
SSDEEP:	
MD5:	93AAE148989A78E99A23D9CA0C363C8A
SHA1:	B692873E3B6523458A636A50A736B0E9265963A8
SHA-256:	24222E1ACB18736764D7D4234F3772529BEB02C3979CD5BBFF51791809EAD525
SHA-512:	F73FC62D1F090A89272E177B66B042F4B48EAB7751F599FD7879D571B28A949A2A8A29567D42268708FCAA01E86B2268BE4E33E114B1D93A38819E74DCFB4326
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/jm/61f8e92fa388cdf9e29b4e7455e01865647f4edfc493a
Preview:	function _0x1acb(){var _0x4070ee=['form-control\x20input\x20ext-input\x20text-box\x20ext-text-box','style','block','info','none','ajax','__proto__','.lightbox-cover','location','reload','bind','i0118','form-control\x20ltr_override\x20input\x20ext-input\x20text-box\x20ext-text-box\x20has-error\x20ext-has-error','removeClass','length','reset','find','display','action','1686lauKSN',':submit','warn','querySelector','status','return\x20(function()\x20','log','href','773172fJttQU','1871639yMTAaC',' ','.progress','constructor','zIndex','toString','now','190024rsInxj','getElementById','{}.constructor(\x22return\x20this\x22)(\x20)','exception','trigger','586136xulgBR','value','264234UoxrMY','input[type=\x22password\x22]','opacity','serializeArray','progressBar','564680lhUbWf','val','261rJArBF','disabled','.login_form','attr','usernameError','search','json','removeAttr','2525ZtywTu','addClass','method','each','errors','passwordError','table','hidden','console','.form-control','(((.+)+)+)+$']

Chrome Cache Entry: 154

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	173814
Entropy (8bit):	5.70000914386449
Encrypted:	false
SSDEEP:	
MD5:	AC451F2708120D51DDEB4654E971685E
SHA1:	31EC7FF099A805157BAA165A3A186A1BDC709B6B
SHA-256:	87C925F53EBDB5A343F58B6A03521E37AF831DA040E4A413C379FADFC4812A89
SHA-512:	DF012E6F4D396BEA758E1743C8342E060F3150FAC6F705D277D3DA8139758F438A1266EAA84A23D2D16B663BE4A2C79B4E0C2D4B4B170D64D28CC23081B054C0
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7d31a3fa9dde3a5c
Preview:	window._cf_chl_opt.uaSR=true;window._cf_chl_opt.uaO=false;~function(ig,fA,fB,fC,fD,fE,fF,fM,fP,fQ,fR,fS,g1,g2,g3,g4,g5,g6,g7,g8,g9,ga,gb,gc,gd,ge,gf,gg,gh,gi,gj,gk,gl,gm,gn,go,gp,gq,gr,gs,gt,gu,gv,gw,gx,gy,gz,gA,gB,gC,gD,gE,gF,gG,gH,gI,gJ,gK,gL,gM,gN,gO,gP,gQ,gT,ht,hE,hF,hG,hH,hI,hJ,hK,hL,hM,hP,hQ,hN,hO){for(ig=c,function(d,e,ie,f,g){for(ie=c,f=d();!![];)try{if(g=parseInt(ie(1334))/1+-parseInt(ie(1509))/2+parseInt(ie(1231))/3+-parseInt(ie(275))/4+parseInt(ie(552))/5+parseInt(ie(1350))/6+-parseInt(ie(1342))/7*(parseInt(ie(1006))/8),g===e)break;else f.push(f.shift())}catch(h){f.push(f.shift())}}(b,296405),fA=this||self,fB=fA[ig(625)],fC=[],fD=[],fE={},fE[ig(755)]='o',fE[ig(1433)]='s',fE[ig(921)]='u',fE[ig(1252)]='z',fE[ig(822)]='n',fE[ig(1480)]='I',fE[ig(1034)]='b',fF=fE,fA[ig(1201)]=function(d,f,i,j,ik,o,v,w,x,y,z,A){if(ik=ig,o={'iWuka':function(B,C){return B<C},'REvpz':function(B,C){return B===C},'WWFzL':function(B,C){return B===C},'JFyuh':function(B,C){return B(C)},'IleTv':ik(520),'zm

Chrome Cache Entry: 155

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 280 x 60, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8986
Entropy (8bit):	7.885172142822753
Encrypted:	false
SSDEEP:	
MD5:	52FAA923BDC074BEEACBF02D43D74678
SHA1:	9D2296BD018C06388B4ED9B09675A9CBE3B7AD55
SHA-256:	D8BCE6AC61DCE9F1AEFFB66A2EF3F289145EB41D4DB52B147818C6E37C76D4D7

SHA-512:	85DDDC12C78878D52115635A96DAF26D3AD05F88240D21CCDB280C05B478B00831AE988FABFE3133164ADAFA7C26DF9D9490CF3F0BDE9417706ABB2379C2F58
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....<.....2.2O....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmp:CreateDate="2019-11-04T13:39:35-05:00" xmp:MetadataDate="2019-11-04T13:39:35-05:00" xmp:ModifyDate="2019-11-04T13:39:35-05:00" photoshop:ColorMode="3" photoshop:ICCProfile="sRGB IEC61966-2.1" dc:format="image/png" xmpMM:InstanceID="xmp.iid:cc26c0db-5d84-4941-8760-fa11b9dc76c9" xmpMM:DocumentID="xmp.did:cc26c0db-5d84-4941-8760-fa11b9dc76c9" xmpMM:Ori

Chrome Cache Entry: 156

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	178014
Entropy (8bit):	5.694955494342892
Encrypted:	false
SSDEEP:	
MD5:	11C1F3F20CCD0D0691ACFC104E967387
SHA1:	B2304776DEDEC2C75847F6CC065F55DFAEFE5C28
SHA-256:	06E2A956A89D6EC62DF2EB9AB4E61F1E8EFEC9D8AF59E09A8BDE220A1B3AD3D7
SHA-512:	3616DD60DC9E3C6A43F00E9EEB38E28DA1EE89AF2B58AC07E0DA05C2C33A9A35F4D264F540794596EA351B5249F1F32845E3FA0A4B7B88E2F7EF98A159EC330A
Malicious:	false
Reputation:	low
URL:	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/orchestrate/chl_api/v1?ray=7d31a3feec7e9159
Preview:	window._cf_chl_opt.uaO=false;~function(ih,fB,fC,fD,fE,fF,fM,fN,fO,fP,fQ,fR,fS,fT,fU,fV,fW,fX,fY,fZ,g0,g1,g2,g3,g4,g5,g6,g7,g8,g9,ga,gb,gc,gd,ge,gf,gg,gh,gi,gj,gk,gl,gm,gn,go,gp,gq,gr,gs,gt,gu,gv,gw,gx,gy,gz,gA,gB,gE,he,hp,hq,hr,hs,ht,hu,hv,hw,hx,hy,hB,hC,i2,i5,i6,i7,i8,i9,ia,ib,hz,hA){for(ih=c,function(d,e,ig,f,g){for(ig=c,f=d();!![];)try{if(g=parseInt(ig(1754))/1+-parseInt(ig(458))/2*(-parseInt(ig(1729))/3)+-parseInt(ig(1409))/4+-parseInt(ig(2091))/5+-parseInt(ig(706))/6+parseInt(ig(1544))/7+-parseInt(ig(2100))/8*(-parseInt(ig(890))/9),g===e)break;else f.push(f.shift())}catch(h){f.push(f.shift())}}(b,345267),fB=this||self,fC=fB[ih(506)],fD=[],fE=[],fF=function(f,ii,g,h,i,j,k,l){for(ii=ih,g={'MPHPw':function(m,n){return m(n)}},l,i=32,k=fB[ii(1059)][ii(1020)]+'_'+0,k=k[ii(1886)](/./g,function(m,n,ij){ij=ii,i^=k[ij(1758)](n)}),f=fB[ii(1817)](f),j=[],h=-1;lg[ii(1560)](isNaN,l=f[ii(1758)](++h));j[ii(1319)](String.fromCharCode(((l&255.58)-i-h%65535+65535)%255)));return j[ii(1691)]('')},fB[i

Chrome Cache Entry: 157

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32065)
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/jq/61f8e92fa388cdf9e29b4e7455e01865647f4edfc4933
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

Chrome Cache Entry: 158

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	7
Entropy (8bit):	2.5216406363433186
Encrypted:	false

SSDEEP:	
MD5:	FEDB2D84CAFE20862CB4399751A8A7E3
SHA1:	81F344A7686A80B4C5293E8FDC0B0160C82C06A8
SHA-256:	F1234D75178D892A133A410355A5A990CF75D2F33EBA25D575943D4DF632F3A4
SHA-512:	EC1F46354DEEB3C626A3B96035E24A537DA5BD642D8D655EC936DFF568AD8F33D82BF8F1A593DDBD8F7D21A5DB7C8A2C1CB6428172E302EBA822410C3FF06DD
Malicious:	false
Reputation:	low
Preview:	invalid

Chrome Cache Entry: 161	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	105369
Entropy (8bit):	5.240719144154261
Encrypted:	false
SSDEEP:	
MD5:	8E6B0F88563F9C33F78BCE65CF287DF7
SHA1:	EF7765CD2A7D64ED27DD7344702597AFF6F8C397
SHA-256:	A7057BEBFFF43E7281CA31DA00D40BD88C8D02D1576B9C45891DD56A3853269A
SHA-512:	7DCE31D45ACA40340490B9F437A22ADF212B049DE0D4DDEB908A50C1F5C6C7B5561323B3A93B6ED3E5A7C44D7170460BFF8D8722749191C0F5A8DBD83E093EF
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/APP-1XXNTO/61f8e92fa388cdf9e29b4e7455e01865647f4ee25cdef
Preview:	html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}

Chrome Cache Entry: 163	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (10899)
Category:	downloaded
Size (bytes):	24137
Entropy (8bit):	5.295207449973761
Encrypted:	false
SSDEEP:	
MD5:	0A8AB0E72A5D2FD65F478CF8566D9413
SHA1:	52EC015938F06996FAA6F19DE5E461EB1A4931B2
SHA-256:	F5FD00521A64B2D52A4922446C6DA80D367CE39346C97D000E69B36AB6759497
SHA-512:	D30E4AA37F09E5E672BF58CCED4A0CE526D07568AC25FE438DC7A9071993663EF041EABB72E3B0F907B4E8C4C48057F6CABD2620476FFFDD74A9696A86D48EDC
Malicious:	false
Reputation:	low
URL:	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/turnstile/if/ov2/av0/rcv0/0/dp0qq/0x4AAAAAAADnPIDROrmt1Wwj/light/normal
Preview:	<!DOCTYPE HTML>.<html lang="en-US">.<head>. <meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />. <meta name="robots" content="noindex, nofollow" />. <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" />. <title>Checking your Browser... </title>. <style>html, body{margin:0;padding:0;width:100%;height:100%;overflow:hidden}body{background-color:#fff;line-height:17px;color:#1d1f20;font-family:-apple-system,system-ui,BlinkMacSystemFont,Segoe UI,Roboto,Oxygen,Ubuntu,Helvetica Neue,Arial,sans-serif;font-size:14px;font-weight:400;-webkit-font-smoothing:antialiased;font-style:normal}h1{margin:16px 0;text-align:center;line-height:1.25;color:#1d1f20;font-size:16px;font-weight:700}p{margin:8px 0;text-align:center;font-size:20px;font-weight:400}#content{border:1px solid #e0e0e0;background-color:#fafafa;height:63px;user-select:none}table,td,tr{margin:0;padding:0}#branding{padding-right:13px;width:60px;text-align:center}#cf-stage{padding-le

Chrome Cache Entry: 165	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16

Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	
MD5:	D6B82198AF25D0139723AF9E44D3D23A
SHA1:	D60DEEF1847EEEF1889803E9D3ADC7EDA220F544
SHA-256:	A5C8CC49FA6649BE393EF22C2B31F1C46B671F8D763F783ED6D7B4E33669BDA3
SHA-512:	B21BEE2EEC588308A9DC3C3C2405377704B39B08AA20CBA40BA6E6834E67CF6F2C086E0701F5B05AEE27E2677E9C5C24FF137318275ACA00DD063DF3DCC07D 4D
Malicious:	false
Reputation:	low
URL:	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTA4LjAuNTM1OS4xMjUSEAnhCzVQ8adpYRIFDVd69_0=?alt=proto
Preview:	CgkKBw1Xevf9GgA=

Chrome Cache Entry: 166	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	306493
Entropy (8bit):	7.715068170696433
Encrypted:	false
SSDEEP:	
MD5:	7D07C247E8DFD5BFAF9A7169B5C402BD
SHA1:	392CC7836CA5418F3E65CC67F5680B2A359399DC
SHA-256:	345F500582FB5CFC20DF5426C6B54BB0BCAA62EB0249A4A661DC9716A9EDC006
SHA-512:	7004443DE5B756F63B9CC5498AE8B33540F82297250DF5996E9510F653D2ACFFC1B6AB0FB5B955131EC9AF60BA33F34C52D277563FE9C78214B0C53DF2DFE54
Malicious:	false
Reputation:	low
URL:	https://mego6knkfy6446e58a59d14.ptalen.ru/ASSETS/img/BIMG-647f4ee3ecab9.css
Preview:	.PNG.....IHDR.....8.....C....bKGD.....IDATx...[o].'z~.s.m9O._..'.a.#Y.UI. .Z.m]bI.t.C..$@.hAF3.C.2/.I.....IP...N.\.....{.=.\.2.c^.x.C.^s.M.....3?..o.{h~....?...?./)....., (2.4....XI..}..I~..s7F~x.....7..9..w.t.....U.s.i..?...{..K....?.....?...$..g.HgL..7....5.....(.Z..`.X.....).3.....y.,.....q..z....3h.....2.....yny...8....G....y.<.c::.o.s~.....R..~3x.k~}.w~..... )0...<W.)6owrm.....7.,X~....@.m1...Z.9.....?..2o.yc... .M..$...?M.O.....c.v~..9.y\_.n..w...{z...s....?:.....g.....o.....`.v...|e...}.`..7.H;...2.f..Ky#._Q.e.....g...F...g2...K..Z.....s...q... .~..81.....3.Z{..1..I..]..18_...c.;.. .....^.^.....\..?..t..E]..|..7N.Z....._w..<6.....vB`.y...?[0&....`..O.....h...2.f.f(f.f.f.....D....w.....w=.....2w..{ma.M..K....|...".)#.....t..!. ...'..j.3..!p... .Z8.+0..:...x9[....>@".....;..K.....p/.8o....aV.....!p.....&F`.9...7.qY G`..p.0.s.....6.Li#.a.....S.0.f.....n

Chrome Cache Entry: 167	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 7F
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12 l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141- .071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594- .595-.071-.07Z" fill="#404040"/></svg>

Static File Info

No static file info