ID: 830975
Sample Name:
ATT9873645.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 21:58:26
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

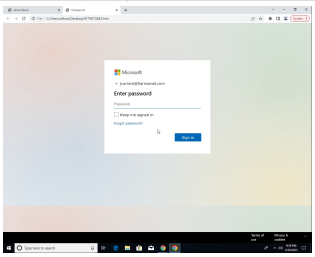
Windows Analysis Report

ATT9873645.htm

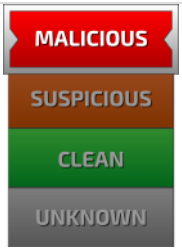
Overview

General Information

Sample Name:	ATT9873645.htm
Analysis ID:	830975
MD5:	cb5be4c57629…
SHA1:	b5b617201b0e…
SHA256:	7b98b775c966…
Infos:	



Detection



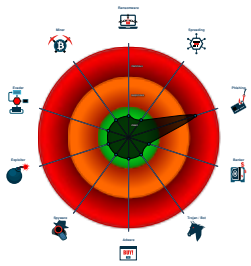
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Multi AV Scanner detection for subm…
- HTML document with suspicious title
- Phishing site detected (based on im…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2868 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5996 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=1976 --field-trial-handle=1788,i,11665051936163555835,8866798666326847203,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6324 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\ATT9873645.htm MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ATT9873645.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
37648.0.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

AV Detection

Multi AV Scanner detection for submitted file

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

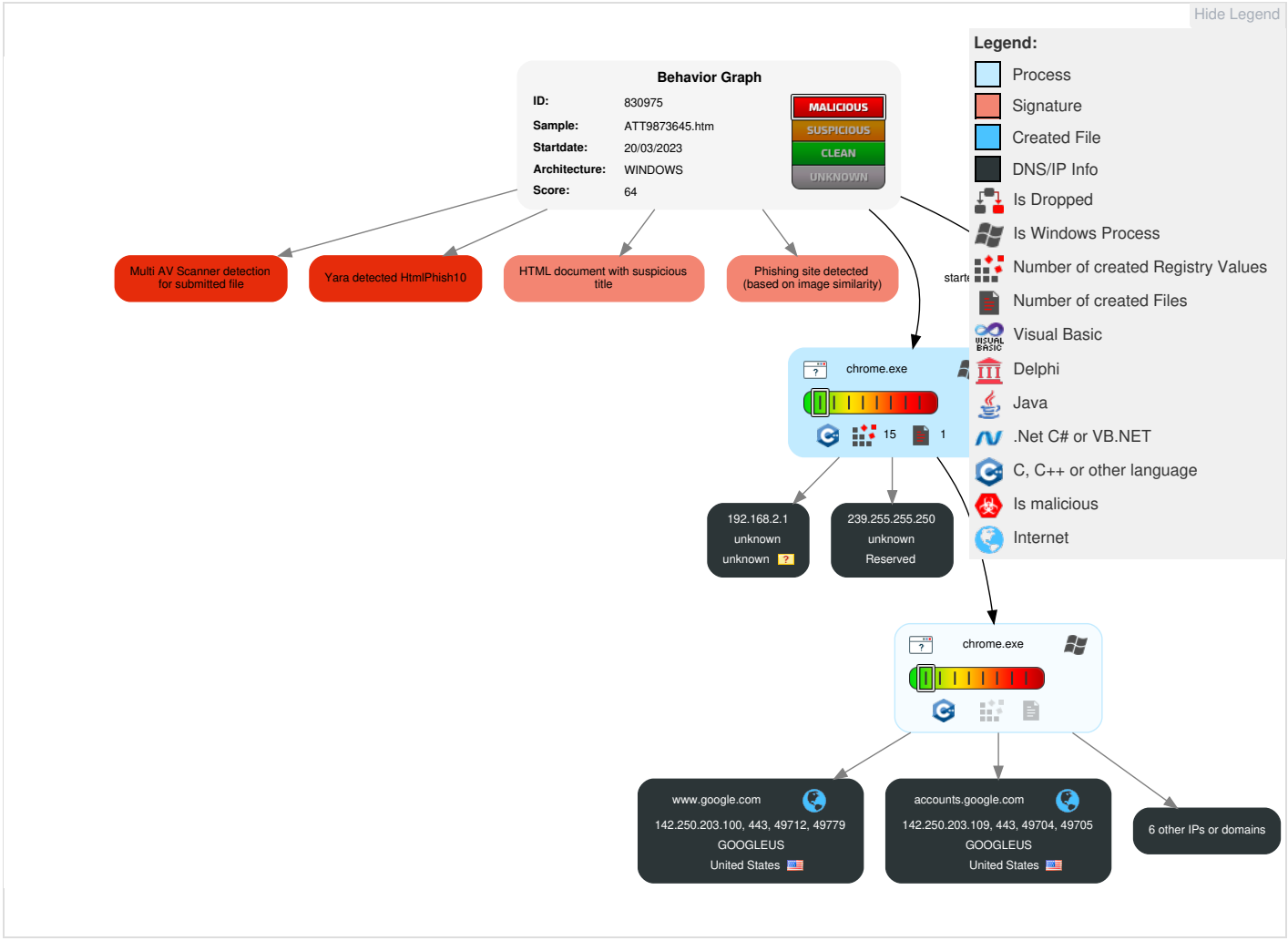
System Summary

HTML document with suspicious title

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

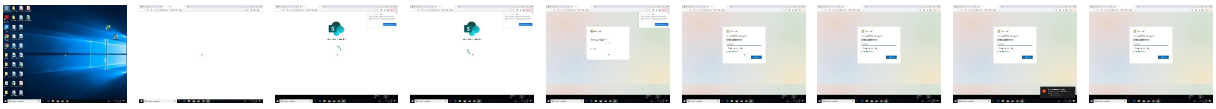
Behavior Graph

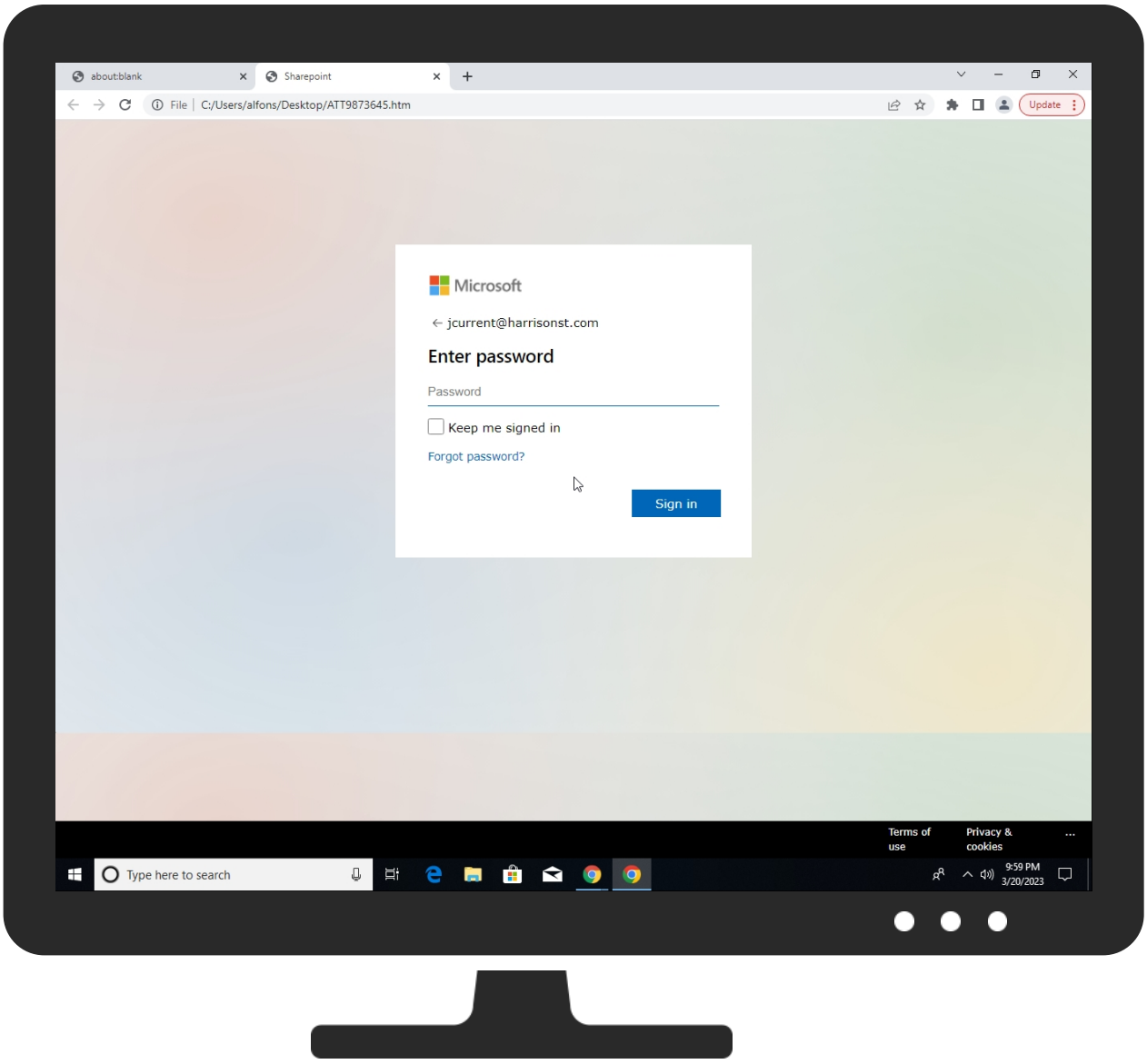


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ATT9873645.htm	17%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

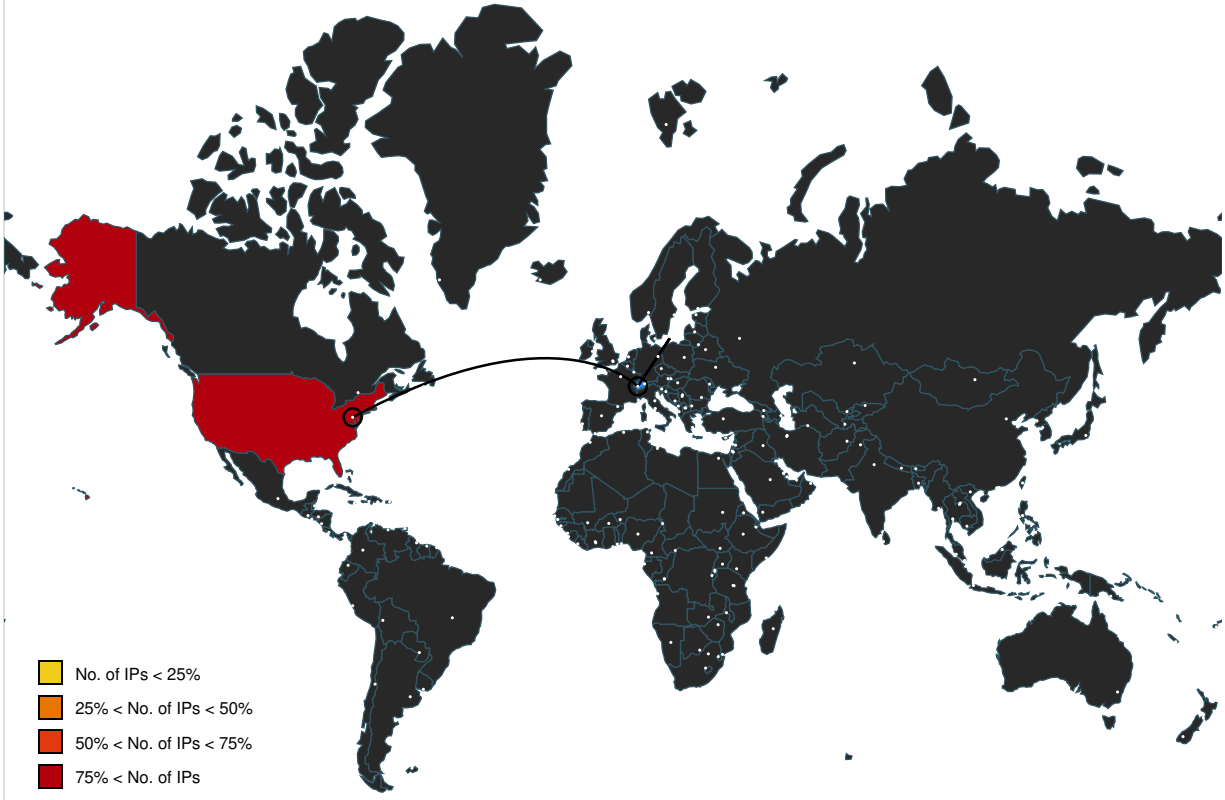
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
cs837.wac.edgecastcdn.net	192.229.133.221	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
www.w3schools.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
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
file:///C:/Users/user/Desktop/ATT9873645.htm	true		low
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.w3schools.com/w3css/4/w3.css	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	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
192.229.133.221	cs837.wac.edgecastcdn.net	United States		15133	EDGECASTUS	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:	830975
Start date and time:	2023-03-20 21:58:26 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
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:	6
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:	ATT9873645.htm
Detection:	MAL
Classification:	mal64.phis.winHTM@29/5@6/8
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, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, edgedl.me.gvt1.com, lgincdn.trafficmanager.net, lgincdnvzeuno.ec.azureedge.net, update.googleapis.com, clientservices.googleapis.com, lgincdnvzeuno.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: 136

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:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 7F
Malicious:	false
Reputation:	moderate, very likely benign file
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>

Chrome Cache Entry: 137

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1555
Entropy (8bit):	3.9986369032270845
Encrypted:	false
SSDEEP:	48:fnPtRGMZvaYm+dN/fltkn9mU6X/pU2Ka1xZXM:XtQlvXHlinn6X/GKm
MD5:	BCB4D1DC4EAE64F0B2B2538209D8435A
SHA1:	4F10568BC1B70BC98D5297B85812C33B3E636766
SHA-256:	A76C08E9CDC3BB87BFB57627AD8F6B46F0E5EF826CC7F046DFBAF25D7B7958EA
SHA-512:	DB41DE25233B7000DD841D244CA2A7504E4B1443A7CF41AA88136764EEB3002B3B99D0E8B31A828AFE4749F454ADCF5D2E4F9F72D645F0A6E66918B5E5A8A7E 1
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M8,0a7.876,7.876,0,0,1,2.126.285,8.011,8.011,0,0,1,5.589,5.589,8.072,8.072,0,0,1,0,4.252,8.011,8.011,0,0,1-5.589,5.589,8.072,8.072,0,0,1-4.252,0A8.011,8.011,0,0,1,.285,10.126a8.072,8.072,0,0,1,0-4.252A8.011,8.011,0,0,1,5.874.285,7.876,7.876,0,0,1,8,0M8,15a6.863,6.863,0,0,0,1.858-.251,7.076,7.076,0,0,0,1.673-.707,6.994,6.994,0,0,0,2.507-2.507,7.076,7.076,0,0,0,.707-1.673,7,7,0,0,0,0-3.716,7.076,7.076,0,0,0,0-.707-1.673,6.994,6.994,0,0,0-2.507-2.507,7.076,7.076,0,0,0-1.673-.707,7,7,0,0,0-3.716,0,7.076,7.076,0,0,0-1.673.707A6.994,6.994,0,0,0,1.962,4.469a7.076,7.076,0,0,0-.707,1.673,7,7,0,0,0,0,3.716,7.076,7.076,0,0,0,.707,1.673,6.994,6.994,0,0,0,2.507,2.507,7.076,7.076,0,0,0,1.673.707A6.863,6.863,0,0,0,8,15m-.536-3.247H8.536V12.82H7.464V11.749M8,3.715a2.558,2.558,0,0,1,1.038.214,2.737,2.737,0,0,1,1.426,1.427,2.533,2.533,0,0,1,.214,1.037,2.215,2.215,0,0,1-.159.875,2.921,2.921,0,0,1-1.426,1.426,2.533,2.533,0,0,1-1.037.214,2.215,2.215,0,0,1-.875-.159,2.921,2.921,0,0,1-1.426-1.426,2.533,2.533,0,0,1-.214-1.037,2.215,2.215,0,0,1,.159-.875,2.921,2.921,0,0,1,1.426-1.426A2.533,2.533,0,0,1,8,3.715" fill="#404040"/></svg>

Chrome Cache Entry: 138	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	23427
Entropy (8bit):	5.112735417225198
Encrypted:	false
SSDEEP:	384:1HHLO7eS0F4bBY/fn6jZcy9/cGK1q8CarY64Cb+dOy:1HHCLYXfl1q8CarY64Cb+dl
MD5:	BA0537E9574725096AF97C27D7E54F76
SHA1:	BD46B47D74D344F435B5805114559D45979762D5
SHA-256:	4A7611BC677873A0F87FE21727BC3A2A43F57A5DED3B10CE33A0F371A2E6030F
SHA-512:	FC43F1A6B95E1CE005A8EFCDB0D38DF8CC12189BEAC18099FD97C278D254D5DA4C24556BD06515D9D6CA495DDB630A052AEFC0BB73D6ED15DEBC0FB1E8E08E7
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://www.w3schools.com/w3css/4/w3.css
Preview:	./* W3.CSS 4.15 December 2020 by Jan Egil and Borge Refsnes */.html{box-sizing:border-box}*,*:before,*:after{box-sizing:inherit}./* Extract from normalize.css by Nicolas Gallagher and Jonathan Neal git.io/normalize */.html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}.article,aside,details,figcaption,figure,footer,header,main,menu,nav,section{display:block}summary{display:list-item}.audio,canvas,progress,video{display:inline-block}progress{vertical-align:baseline}.audio:not([controls]){display:none;height:0}[hidden],template{display:none}.a{background-color:transparent}a:active,a:hover{outline-width:0}.abbr[title]{border-bottom:none;text-decoration:underline;text-decoration:underline dotted}.b,strong{font-weight:bolder}dfn{font-style:italic}mark{background:#ff0;color:#000}.small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}.sub{bottom:-0.25em}sup{top:-0.5em}figure{margin:1em 40px}img{border-style:none}.code,kbd,p

Chrome Cache Entry: 139	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD97F
Malicious:	false
URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
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-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" 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>

Chrome Cache Entry: 140	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1555
Entropy (8bit):	3.9986369032270845
Encrypted:	false
SSDEEP:	48:fnPtRGMZvaYm+dN/fltkn9mU6X/pU2Ka1xZXM:XtQIvXHlinn6X/GKm
MD5:	BCB4D1DC4EAE64F0B2B2538209D8435A
SHA1:	4F10568BC1B70BC98D5297B85812C33B3E636766
SHA-256:	A76C08E9CDC3BB87BFB57627AD8F6B46F0E5EF826CC7F046DFBAF25D7B7958EA
SHA-512:	DB41DE25233B7000DD841D244CA2A7504E4B1443A7CF41AA88136764EEB3002B3B99D0E8B31A828AFE4749F454ADCF5D2E4F9F72D645F0A6E66918B5E5A8A7E1

Malicious:	false
URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/documentation_bcb4d1dc4eae64f0b2b2538209d8435a.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M8,0a7.876,7.876,0,0,1,2.126.285,8.011,8.011,0,0,1,5.589,5.589,8.072,8.072,0,0,1,0,4.252,8.011,8.011,0,0,1-5.589,5.589,8.072,8.072,0,0,1-4.252,0A8.011,8.011,0,0,1,.285,10.126a8.072,8.072,0,0,1,0-4.252A8.011,8.011,0,0,1,5.874.285,7.876,7.876,0,0,1,8,0M8,15a6.863,6.863,0,0,0,1.858-.251,7.076,7.076,0,0,0,1.673-.707,6.994,6.994,0,0,0,2.507-2.507,7.076,7.076,0,0,0,.707-1.673,7,7,0,0,0,0-3.716,7.076,7.076,0,0,0-.707-1.673,6.994,6.994,0,0,0-2.507-2.507,7.076,7.076,0,0,0-1.673-.707,7,7,0,0,0-3.716,0,7.076,7.076,0,0,0-1.673.707A6.994,6.994,0,0,0,.962,4.469a7.076,7.076,0,0,0-.707,1.673,7,7,0,0,0,0,3.716,7.076,7.076,0,0,0,.707,1.673,6.994,6.994,0,0,0,2.507,2.507,7.076,7.076,0,0,0,1.673.707A6.863,6.863,0,0,0,8,15m-.536-3.247H8.536V12.82H7.464V11.749M8,3.715a2.558,2.558,0,0,1,1.038.214,2.737,2.737,0,0,1,1.426,1.427,2.533,2.533,0,0,1,.214,1.037,2.215,2.215,0,0,1-.159.875,2.921,2.921,0,0,1-.636.931,2.921,2.921,0,0,1-.931.636,2.215,2.215,0,0,1-.875.159,2.533,2.533,0,0,1-1.037-.214,2.737,2.737,0,0,1-1.426-1.426,2.533,2.533,0,0,1-.214-1.037,2.215,2.215,0,0,1,.159-.875,2.921,2.921,0,0,1,.636-.931,2.921,2.921,0,0,1,.931-.636A2.215,2.215,0,0,1,8,3.715" fill="#646464" /></svg>

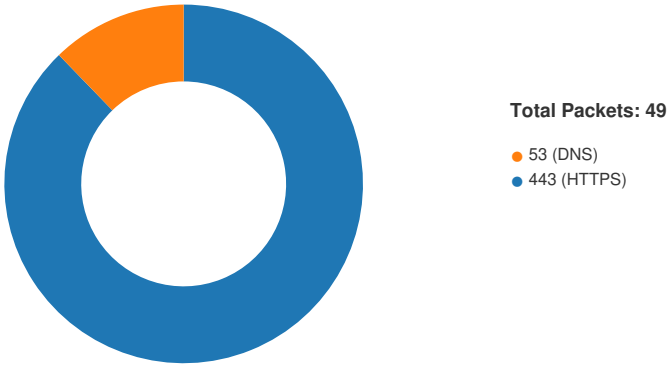
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (64487), with CRLF line terminators
Entropy (8bit):	6.063612367882672
TrID:	• HyperText Markup Language (15015/1) 20.56% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (11501/1) 15.75% • HyperText Markup Language (11501/1) 15.75%
File name:	ATT9873645.htm
File size:	1113680
MD5:	cb5be4c57629182364781024e6fd83d7
SHA1:	b5b617201b0e6992386a4854676903d96b1de0f7
SHA256:	7b98b775c96608b027154e518b723d3d6c8468d8c08925e393d58418f6d384d8
SHA512:	899d14a0048a61fddde01b8998a9831b52171de0eb81e203292da1719f502eb3c82011d74750c591de6bb70b99d709d9aa73575275951baa87e755a5452aef8c
SSDEEP:	24576:zNjx1VWZ9oMsB9U991Q/2qg1A8LGNSpzF+Y:RKsu9m/PF8qsZF3
TLSH:	1C3512F7E540EB7D1317C638197D4824D3A047629BC26B86BAECE8CB079DB27415E86C
File Content Preview:	<!DOCTYPE html>..<html id="mainAll" data-emailValue="jcurrent@harrisonst.com" data-fetch="" lang="en">....<head></head>....<body style="display: none;" id="allbody">.. <script>.. const _0x365e9f = _0x24fc;.. (function(_0x151353, _0x28df1e

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 21:59:32.819076061 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.819169998 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:32.819400072 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.819547892 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.819591045 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.819655895 CET	49704	443	192.168.2.5	142.250.203.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 21:59:32.820374966 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.820410967 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.820501089 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.821118116 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.821161985 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:32.821279049 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.822649956 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.822709084 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:32.823652983 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.823715925 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.823898077 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.823916912 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.824269056 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:32.824310064 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:32.950491905 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.962707996 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:32.962776899 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.965380907 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:32.965498924 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.057779074 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.059912920 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.069502115 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.109122992 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.160166025 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.160166025 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.160224915 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.160604000 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.160619974 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.160784006 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.160815001 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.161777973 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.161808968 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.161891937 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.162398100 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.162432909 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.162502050 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.164160967 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.164226055 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.164236069 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.164288044 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.164288044 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.164324045 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.164638042 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.164710999 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.164741039 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.208498955 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.261120081 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.261120081 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.606395960 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.606457949 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.606816053 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.607079029 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.607111931 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.607182026 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.607230902 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.607589006 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.607681036 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.615047932 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.615103006 CET	443	49706	142.250.203.110	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 21:59:33.615521908 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.617292881 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.617374897 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.617870092 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.617904902 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.653955936 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.654055119 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.654093981 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.654408932 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.654484987 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.660291910 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.660300016 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.660321951 CET	443	49704	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.672538042 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.673868895 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.673959017 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.705667973 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.705727100 CET	443	49706	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.728508949 CET	49705	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.728586912 CET	443	49705	142.250.203.109	192.168.2.5
Mar 20, 2023 21:59:33.729053020 CET	49703	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.729104042 CET	443	49703	142.250.203.110	192.168.2.5
Mar 20, 2023 21:59:33.763139963 CET	49704	443	192.168.2.5	142.250.203.109
Mar 20, 2023 21:59:33.808130026 CET	49706	443	192.168.2.5	142.250.203.110
Mar 20, 2023 21:59:33.820372105 CET	49708	443	192.168.2.5	192.229.221.185
Mar 20, 2023 21:59:33.820472002 CET	443	49708	192.229.221.185	192.168.2.5
Mar 20, 2023 21:59:33.820600033 CET	49708	443	192.168.2.5	192.229.221.185
Mar 20, 2023 21:59:33.820651054 CET	49709	443	192.168.2.5	192.229.221.185
Mar 20, 2023 21:59:33.820724964 CET	443	49709	192.229.221.185	192.168.2.5
Mar 20, 2023 21:59:33.820831060 CET	49709	443	192.168.2.5	192.229.221.185
Mar 20, 2023 21:59:33.821155071 CET	49710	443	192.168.2.5	192.229.133.221
Mar 20, 2023 21:59:33.821224928 CET	443	49710	192.229.133.221	192.168.2.5
Mar 20, 2023 21:59:33.821290016 CET	49710	443	192.168.2.5	192.229.133.221
Mar 20, 2023 21:59:33.821446896 CET	49708	443	192.168.2.5	192.229.221.185
Mar 20, 2023 21:59:33.821474075 CET	443	49708	192.229.221.185	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 21:59:31.526016951 CET	60649	53	192.168.2.5	8.8.8.8
Mar 20, 2023 21:59:31.526348114 CET	51441	53	192.168.2.5	8.8.8.8
Mar 20, 2023 21:59:31.545957088 CET	53	60649	8.8.8.8	192.168.2.5
Mar 20, 2023 21:59:31.546515942 CET	53	51441	8.8.8.8	192.168.2.5
Mar 20, 2023 21:59:33.609267950 CET	61452	53	192.168.2.5	8.8.8.8
Mar 20, 2023 21:59:33.638539076 CET	53	61452	8.8.8.8	192.168.2.5
Mar 20, 2023 21:59:34.847563982 CET	56751	53	192.168.2.5	8.8.8.8
Mar 20, 2023 21:59:34.865767956 CET	53	56751	8.8.8.8	192.168.2.5
Mar 20, 2023 22:00:34.913739920 CET	54585	53	192.168.2.5	8.8.8.8
Mar 20, 2023 22:00:34.934633970 CET	53	54585	8.8.8.8	192.168.2.5
Mar 20, 2023 22:01:34.979279041 CET	63938	53	192.168.2.5	8.8.8.8
Mar 20, 2023 22:01:34.999069929 CET	53	63938	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 21:59:31.526016951 CET	192.168.2.5	8.8.8.8	0x8e5	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:31.526348114 CET	192.168.2.5	8.8.8.8	0x1134	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 21:59:33.609267950 CET	192.168.2.5	8.8.8.8	0x6a73	Standard query (0)	www.w3schools.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:34.847563982 CET	192.168.2.5	8.8.8.8	0xa979	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:00:34.913739920 CET	192.168.2.5	8.8.8.8	0xe655	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:01:34.979279041 CET	192.168.2.5	8.8.8.8	0xa714	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

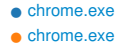
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 21:59:31.545957088 CET	8.8.8.8	192.168.2.5	0x8e5	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 21:59:31.545957088 CET	8.8.8.8	192.168.2.5	0x8e5	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:31.546515942 CET	8.8.8.8	192.168.2.5	0x1134	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:33.634310961 CET	8.8.8.8	192.168.2.5	0xe2a5	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:33.638539076 CET	8.8.8.8	192.168.2.5	0x6a73	No error (0)	www.w3schools.com	cs837.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 21:59:33.638539076 CET	8.8.8.8	192.168.2.5	0x6a73	No error (0)	cs837.wac.edgecastcdn.net		192.229.133.221	A (IP address)	IN (0x0001)	false
Mar 20, 2023 21:59:34.865767956 CET	8.8.8.8	192.168.2.5	0xa979	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:00:34.934633970 CET	8.8.8.8	192.168.2.5	0xe655	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:01:34.999069929 CET	8.8.8.8	192.168.2.5	0xa714	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

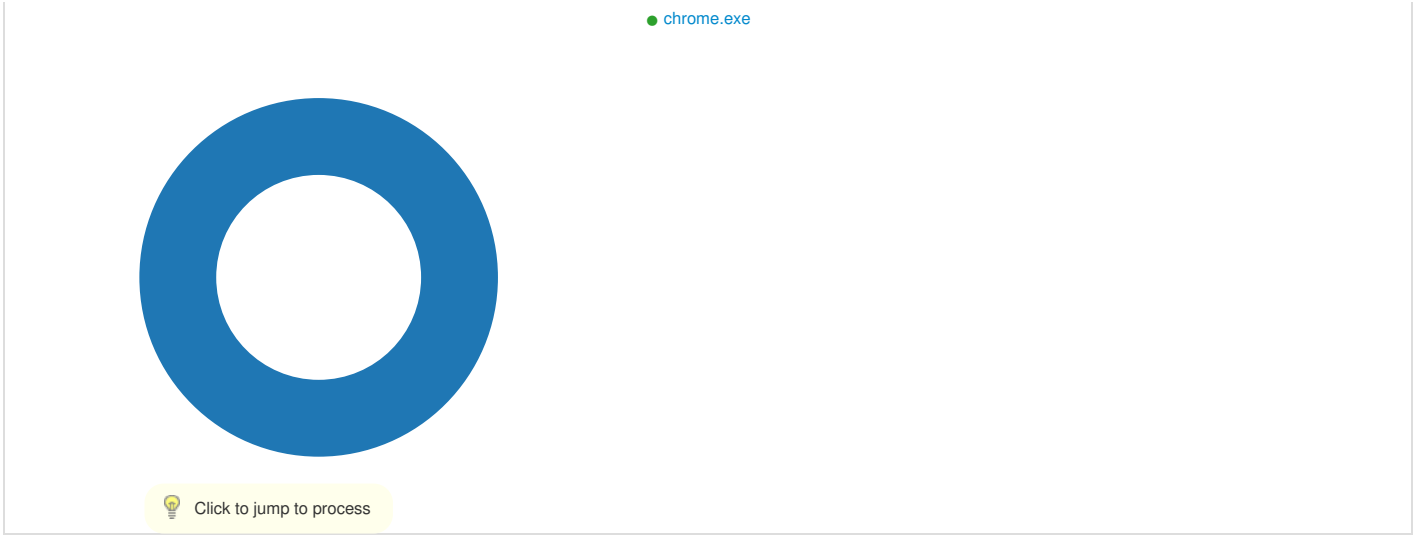
HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- logincdn.msauth.net
- www.w3schools.com

Statistics

Behavior





System Behavior

Analysis Process: chrome.exe PID: 2868, Parent PID: 4924

General

Target ID:	0
Start time:	21:59:28
Start date:	20/03/2023
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:	0x7ff7d31b0000
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: 5996, Parent PID: 2868

General

Target ID:	1
Start time:	21:59:29
Start date:	20/03/2023
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=1976 --field-trial-handle=1788,i,11665051936163555835,8866798666326847203,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
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

Analysis Process: chrome.exe PID: **6324**, Parent PID: **4924**

General

Target ID:	2
Start time:	21:59:30
Start date:	20/03/2023
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\ATT9873645.htm
Imagebase:	0x7ff7d31b0000
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