

ID: 756272
Sample Name: ATT16342.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 22:46:57
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ATT16342.html 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Initial Sample 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Phishing 4
Networking 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 8
General Information 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
Network Behavior 9
Network Port Distribution 9
TCP Packets 10
UDP Packets 12
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 13
Statistics 13
Behavior 13
System Behavior 14
Analysis Process: chrome.exePID: 2884, Parent PID: 2204 14
General 14
File Activities 14
Registry Activities 14
Analysis Process: chrome.exePID: 4844, Parent PID: 2884 14
General 14
File Activities 14
Analysis Process: chrome.exePID: 6356, Parent PID: 2204 15
General 15
Registry Activities 15
Disassembly 15

Copyright Joe Security LLC 2022

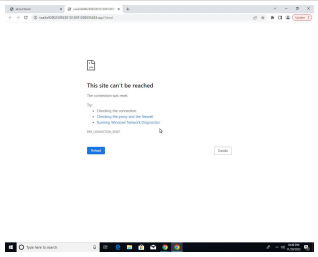
Windows Analysis Report

ATT16342.html

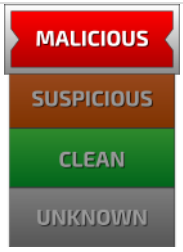
Overview

General Information

Sample Name:	ATT16342.html
Analysis ID:	756272
MD5:	9b3a5b0636ee04.
SHA1:	2aa758ad0ea7a1.
SHA256:	bc67d13fb61a85..
Infos:	



Detection



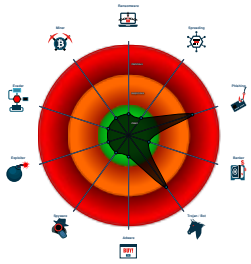
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish44
- Performs DNS queries to domains w…
- IP address seen in connection with …
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2884 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4844 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=1768 --field-trial-handle=1776,i,2414851685685751221,11507612187326661899,131072 --disable-features =OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6356 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\ATT16342.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ATT16342.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Yara detected HtmlPhish44

Networking

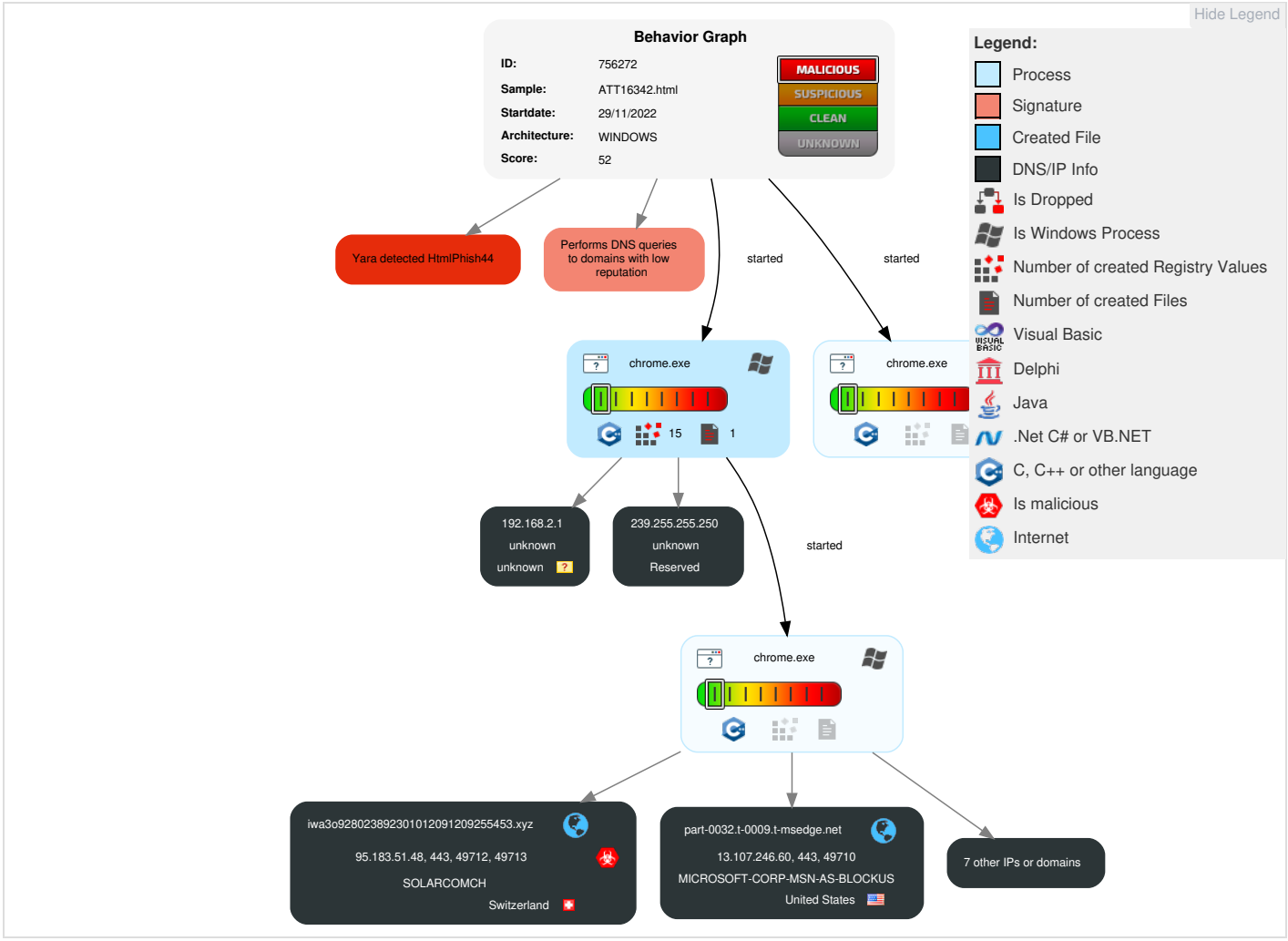


Performs DNS queries to domains with low reputation

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

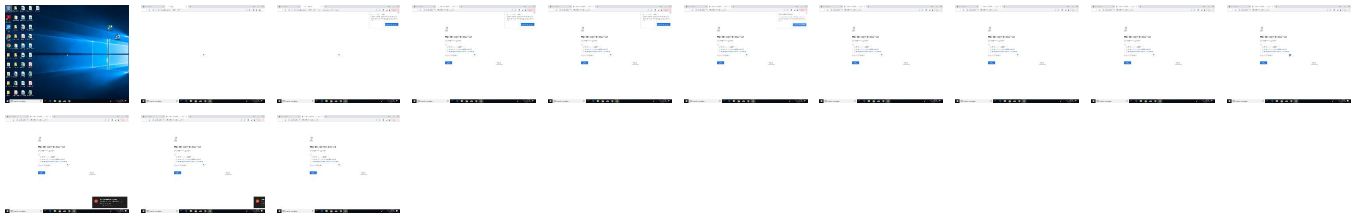
Behavior Graph

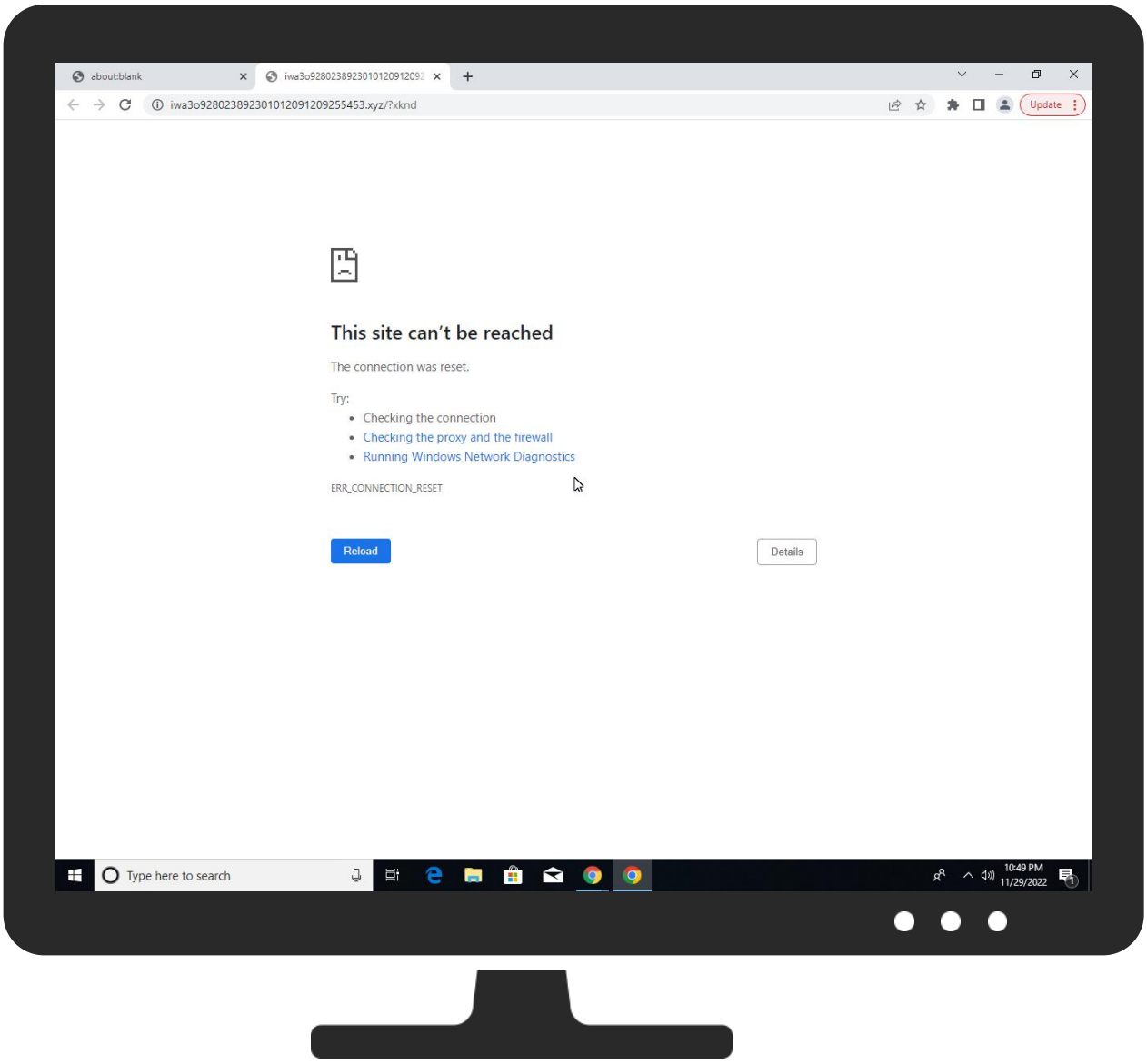


Screenshots

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
ATT16342.html	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
part-0032.t-0009.t-msedge.net	0%	Virustotal		Browse
interc0mpanyc0mmunications98749378430329083.azurefd.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://interc0mpanyc0mmunications98749378430329083.azurefd.net/toazure.js	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

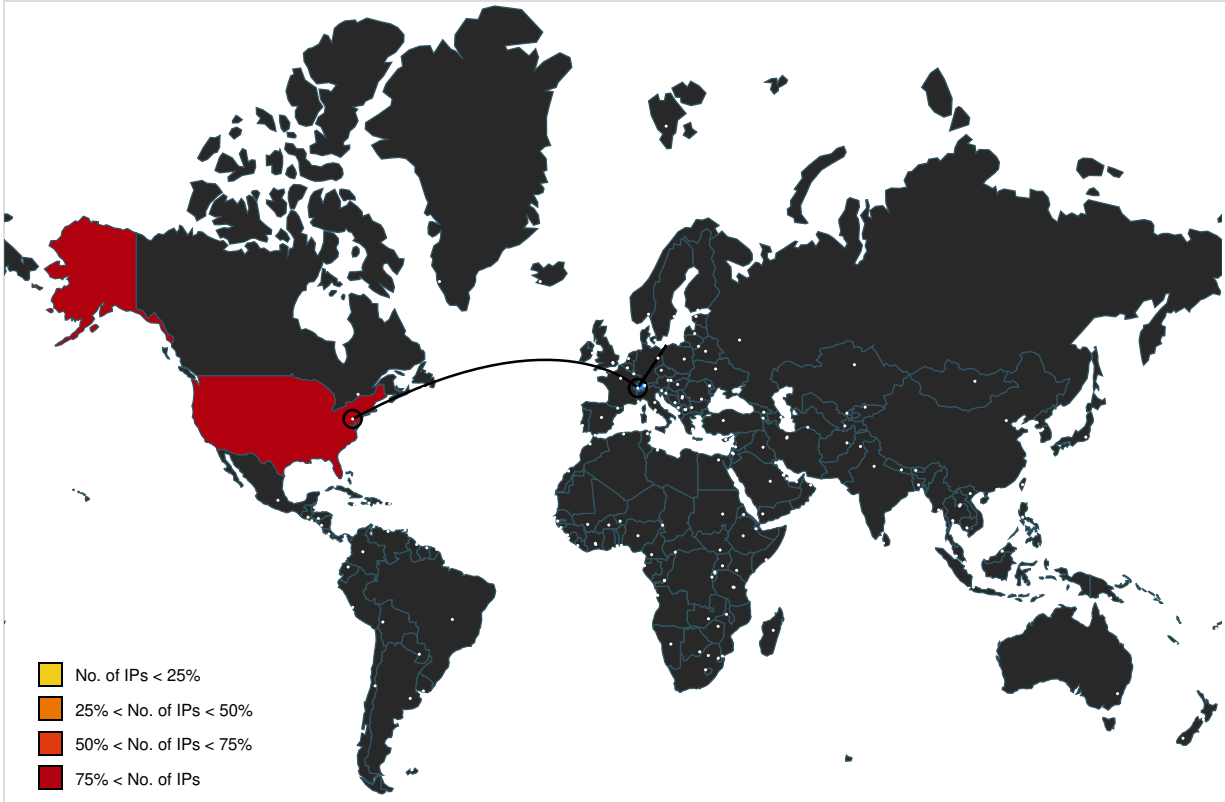
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
part-0032.t-0009.t-msedge.net	13.107.246.60	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
iwa3o928023892301012091209255453.xyz	95.183.51.48	true	true		unknown
clients2.google.com	unknown	unknown	false		high
interc0mpanyc0mmunications9874937843032908 3.azurefd.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

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
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://interc0mpanyc0mmunications98749378430329083.azurefd.net/toazure.js	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.183.51.48	iwa3o928023892301012091209255453.xyz	Switzerland		197988	SOLARCOMCH	true
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.246.60	part-0032.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756272
Start date and time:	2022-11-29 22:46:57 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATT16342.html
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:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.troj.winHTML@37/0@9/8
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: .html

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123
- Excluded domains from analysis (whitelisted): client.wns.windows.com, edgedl.me.gvt1.com, star-azurefd-prod.trafficmanager.net, update.googleapis.com, clientservices.googleapis.com
- 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

No created / dropped files found

Static File Info

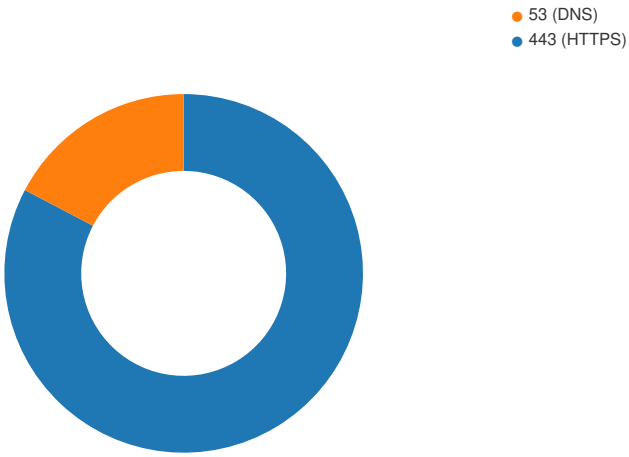
General

File type:	HTML document, ASCII text, with very long lines (65536), with no line terminators
Entropy (8bit):	4.7569573040035245
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	ATT16342.html
File size:	68819
MD5:	9b3a5b0636ee04ffd5560c7bbeacc1e2
SHA1:	2aa758ad0ea7a17fee0af1c0df392bc9b2984db4
SHA256:	bc67d13fb61a853de8c5db8e552689f1a80d7d2c7ea08eb27a4c12821bc0e24a
SHA512:	bd581ed24057762d12df1c4383bb7817993081a9191c531264054e3d43b807b4451c5bfa2d8408d49425042be6d3bbe240a2dafc8ac2352ad58c65519ac79a8d
SSDEEP:	1536:VXrnTxubAWIE3Uq70l/wnZQbic7fZJzqfIla9mtOxZ/rvKcSrW7EwWHbhN6pTWhI:VXZgAWI2Uq70l/wnZQbVJ2fIla9VG7hg
TLSH:	EA63DDC477C1F843128F4B73BB1BA6E9E53A5CE57088588BF104B898F4AC516FAA4D74
File Content Preview:	<script language=javascript>function _0x16c7e4(_0x2b4b5e,_0x4e7723,_0x53d233,_0x246bd0,_0xadf88f){return _0x2ff3(_0x53d233-0x318,_0x246bd0);}(function(_0x12a766,_0xb505e3){function _0x268ac2(_0x2d20db,_0x5dba14,_0x3f6ad8,_0x57871e,_0x4c4452){return _0x2ff

Network Behavior

Network Port Distribution

Total Packets: 52



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:47:50.746682882 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:50.746761084 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.746849060 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:50.747201920 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:50.747272015 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.749064922 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:50.749124050 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:50.749252081 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:50.749537945 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:50.749572039 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:50.815110922 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:50.815628052 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:50.815706968 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:50.817683935 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:50.817804098 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:50.818947077 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.821146011 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:50.821227074 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.821887016 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.821990013 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:50.822770119 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:50.822868109 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.023894072 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.023979902 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.024235010 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.024259090 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.024791002 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:52.024830103 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.024904013 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.025032997 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.025176048 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:52.025191069 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.061817884 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.061985016 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.062020063 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.062159061 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.062304974 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.099787951 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.099930048 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:52.099956989 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.100326061 CET	443	49709	172.217.168.45	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:47:52.100404978 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:52.103990078 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 22:47:52.104015112 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 22:47:52.105914116 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 22:47:52.105937958 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 22:47:52.863598108 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:52.863655090 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:52.863734007 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:52.864132881 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:52.864149094 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:52.976686001 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:52.977284908 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:52.977319956 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:52.978668928 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:52.978756905 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.044989109 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.045036077 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.045427084 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.047446012 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.047472000 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162476063 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162575960 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162602901 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162642002 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162653923 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162663937 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162698984 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162714005 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162722111 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162738085 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162775040 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162775040 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162797928 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162828922 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162911892 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162930965 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162962914 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.162971020 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.162982941 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.163013935 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188240051 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188366890 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188379049 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188404083 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188424110 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188431025 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188483953 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188492060 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188498974 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188530922 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188586950 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188652992 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188653946 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188668966 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188695908 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188718081 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188776970 CET	49710	443	192.168.2.5	13.107.246.60
Nov 29, 2022 22:47:53.188782930 CET	443	49710	13.107.246.60	192.168.2.5
Nov 29, 2022 22:47:53.188993931 CET	443	49710	13.107.246.60	192.168.2.5

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:47:50.621371031 CET	65323	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:47:50.622133970 CET	51484	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:47:50.647510052 CET	53	65323	8.8.8.8	192.168.2.5
Nov 29, 2022 22:47:50.647546053 CET	53	51484	8.8.8.8	192.168.2.5
Nov 29, 2022 22:47:52.832496881 CET	56751	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:47:53.435863018 CET	59220	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:47:53.455653906 CET	53	59220	8.8.8.8	192.168.2.5
Nov 29, 2022 22:47:54.188219070 CET	56682	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:47:54.206001997 CET	53	56682	8.8.8.8	192.168.2.5
Nov 29, 2022 22:48:54.273896933 CET	58623	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:48:54.293354034 CET	53	58623	8.8.8.8	192.168.2.5
Nov 29, 2022 22:49:34.393140078 CET	52892	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:49:34.413666964 CET	53	52892	8.8.8.8	192.168.2.5
Nov 29, 2022 22:49:54.335998058 CET	55726	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:49:54.353460073 CET	53	55726	8.8.8.8	192.168.2.5
Nov 29, 2022 22:50:54.406117916 CET	49261	53	192.168.2.5	8.8.8.8
Nov 29, 2022 22:50:54.425745010 CET	53	49261	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
Nov 29, 2022 22:47:50.621371031 CET	192.168.2.5	8.8.8.8	0xaeec	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:50.622133970 CET	192.168.2.5	8.8.8.8	0x64dd	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:52.832496881 CET	192.168.2.5	8.8.8.8	0xe9ef	Standard query (0)	interc0mpanyc0mmunications98749378430329083.azurefd.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:53.435863018 CET	192.168.2.5	8.8.8.8	0x41cd	Standard query (0)	iwa3o928023892301012091209255453.xyz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:54.188219070 CET	192.168.2.5	8.8.8.8	0x235b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:54.273896933 CET	192.168.2.5	8.8.8.8	0xb56e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:49:34.393140078 CET	192.168.2.5	8.8.8.8	0x278a	Standard query (0)	iwa3o928023892301012091209255453.xyz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:49:54.335998058 CET	192.168.2.5	8.8.8.8	0xdda9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:50:54.406117916 CET	192.168.2.5	8.8.8.8	0x40b6	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
Nov 29, 2022 22:47:50.647510052 CET	8.8.8.8	192.168.2.5	0xaeec	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:50.647546053 CET	8.8.8.8	192.168.2.5	0x64dd	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:47:50.647546053 CET	8.8.8.8	192.168.2.5	0x64dd	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:52.855330944 CET	8.8.8.8	192.168.2.5	0xe9ef	No error (0)	interc0mpanyc0mmunications98749378430329083.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false

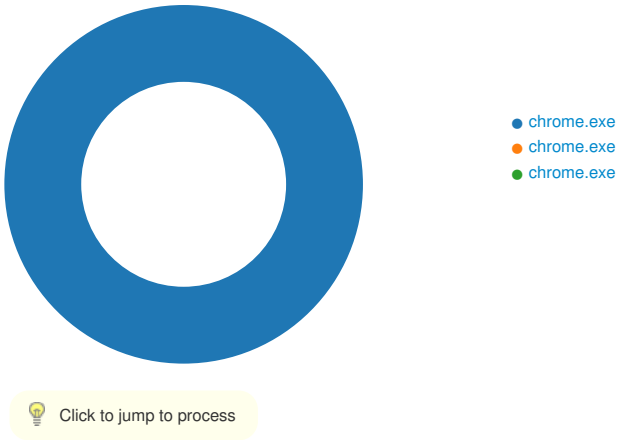
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 22:47:52.855330944 CET	8.8.8.8	192.168.2.5	0xe9ef	No error (0)	dual.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:47:52.855330944 CET	8.8.8.8	192.168.2.5	0xe9ef	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:52.855330944 CET	8.8.8.8	192.168.2.5	0xe9ef	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:53.455653906 CET	8.8.8.8	192.168.2.5	0x41cd	No error (0)	iwa3o92802389230101209125545 3.xyz		95.183.51.48	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:47:54.206001997 CET	8.8.8.8	192.168.2.5	0x235b	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:54.293354034 CET	8.8.8.8	192.168.2.5	0xb56e	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:49:34.413666964 CET	8.8.8.8	192.168.2.5	0x278a	No error (0)	iwa3o92802389230101209125545 3.xyz		95.183.51.48	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:49:54.353460073 CET	8.8.8.8	192.168.2.5	0xdda9	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:50:54.425745010 CET	8.8.8.8	192.168.2.5	0x40b6	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- interc0mpanyc0mmunications98749378430329083.azurefd.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2884**, Parent PID: **2204**

General

Target ID:	2
Start time:	22:47:47
Start date:	29/11/2022
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: **4844**, Parent PID: **2884**

General

Target ID:	3
Start time:	22:47:48
Start date:	29/11/2022
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=1768 --field-trial-handle=1776,i,2414851685685751221,11507612187326661899,131072 --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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6356**, Parent PID: **2204**

General	
Target ID:	4
Start time:	22:47:49
Start date:	29/11/2022
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\ATT16342.html
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