ID: 876166
Sample Name: iata-25May2023.shtml
Cookbook: default.jbs
Time: 11:50:06
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

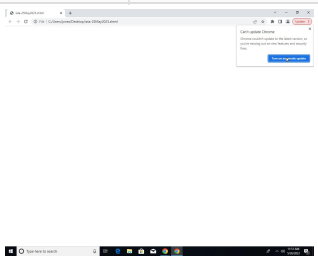
Windows Analysis Report

iata-25May2023.shtml

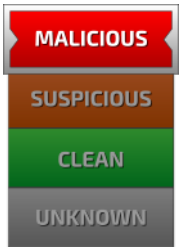
Overview

General Information

Sample Name:	iata-25May2023.shtml
Analysis ID:	876166
MD5:	38f37466740c0..
SHA1:	d9dc91b0df8a0..
SHA256:	48cd890109fa7..
Infos:	



Detection

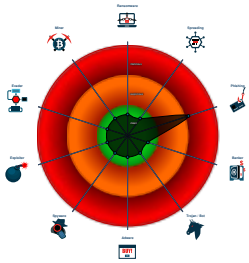


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Detected javascript redirector / loader
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5688 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\iata-25May2023.shtml MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5148 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1888 --field-trial-handle=1812,i,18360485486545431331,5420382872932820938,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

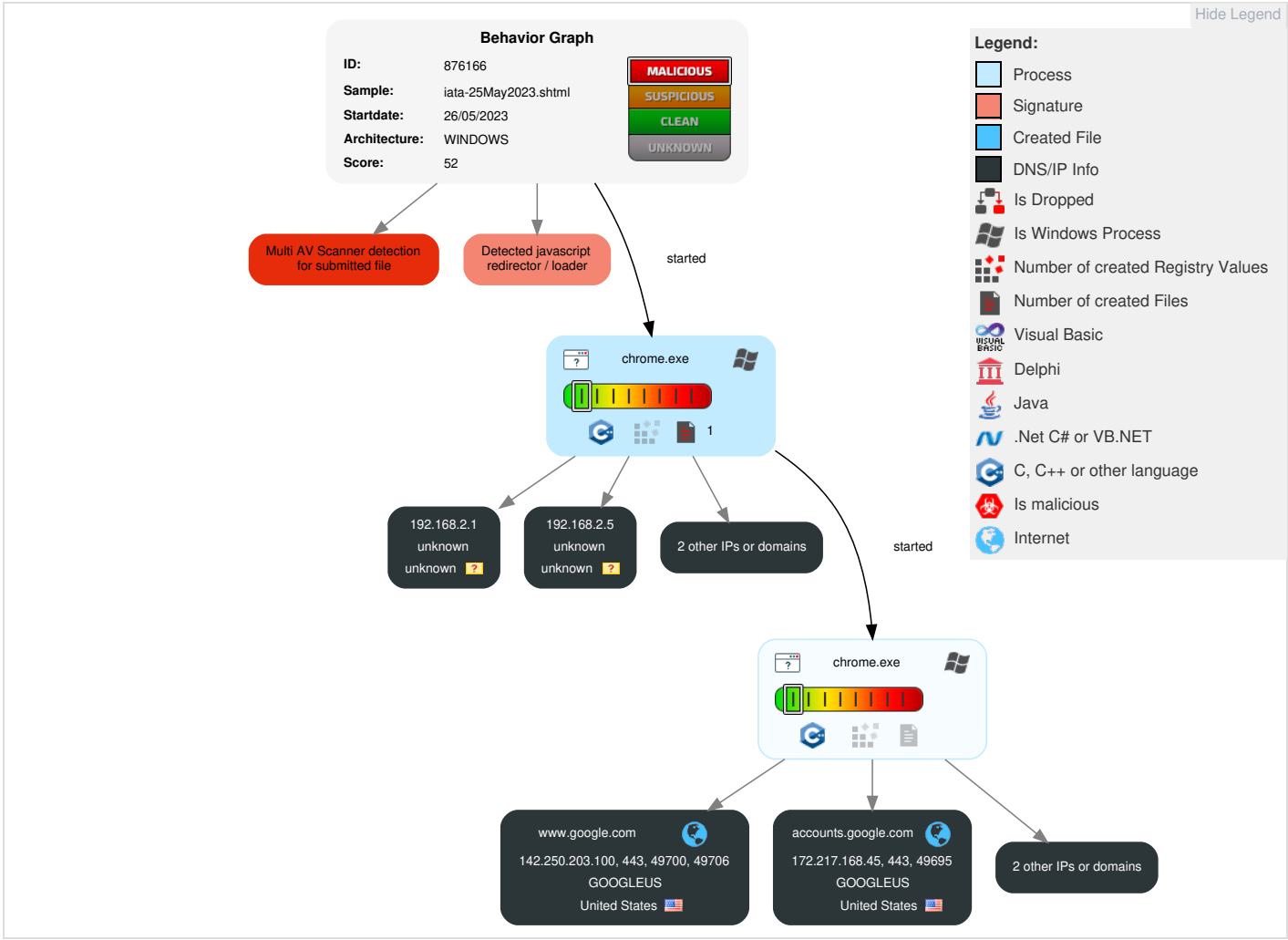
Phishing

Detected javascript redirector / loader

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	1 Extra Window Memory Injection	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)	1 Extra Window Memory Injection	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

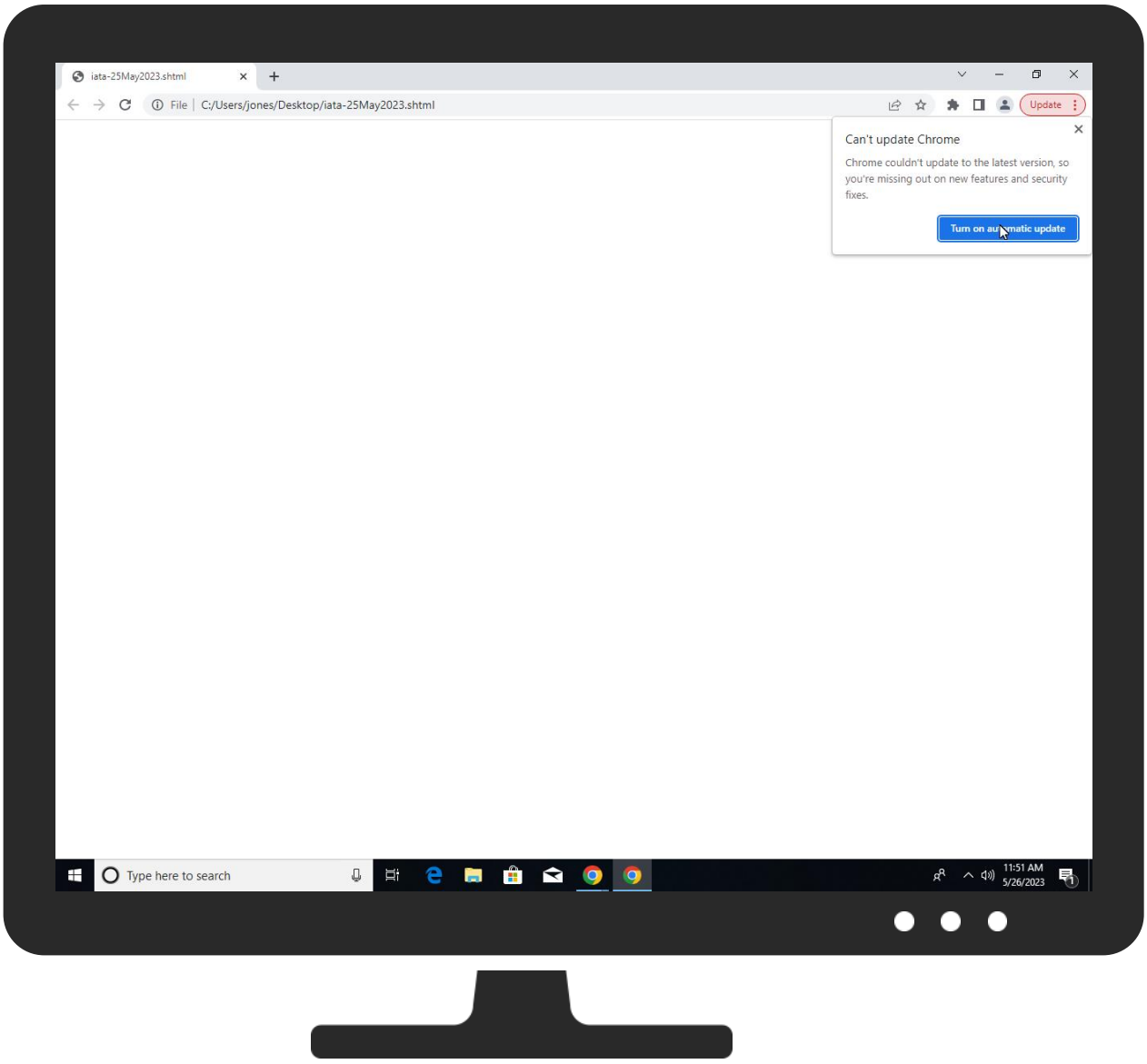
Behavior Graph



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
iata-25May2023.shtml	14%	ReversingLabs	Document-HTML.Phishing.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2023

Domains and IPs

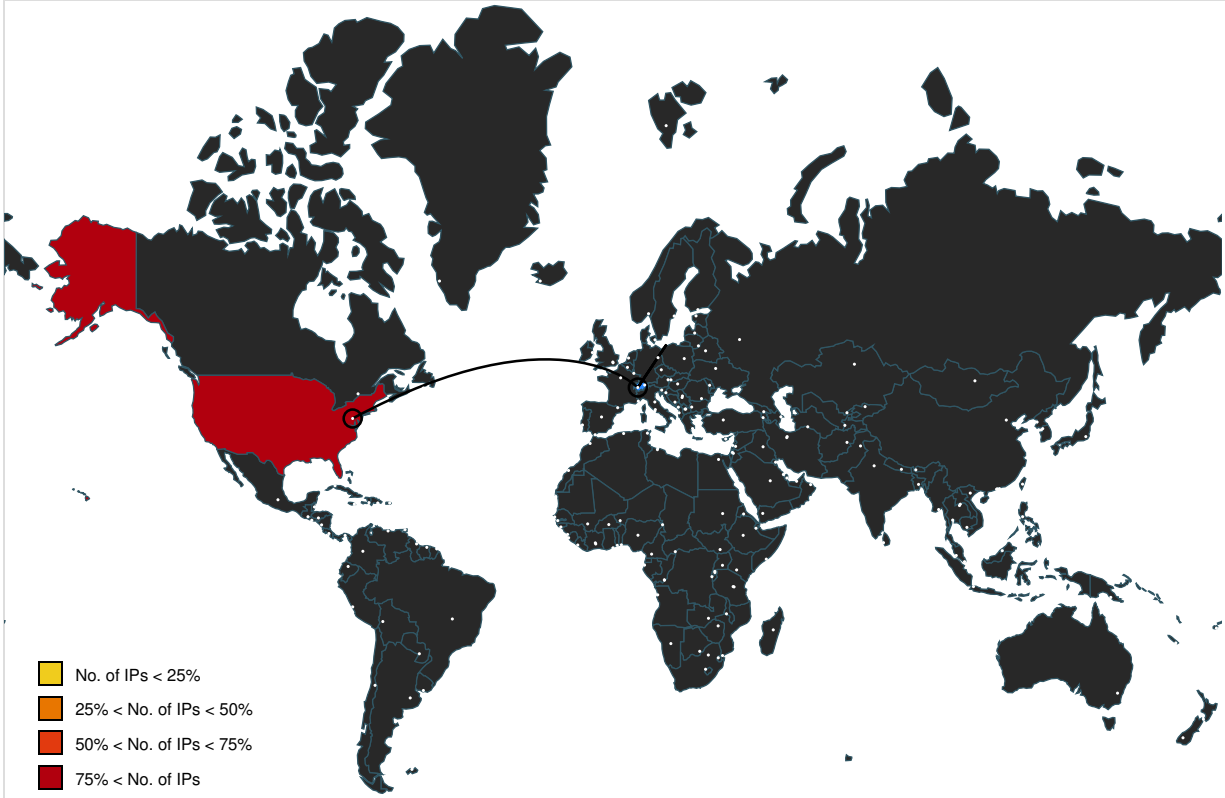
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/iata-25May2023.shtml	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-GB&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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.6
192.168.2.5

Copyright Joe Security LLC 2023

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876166
Start date and time:	2023-05-26 11:50:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.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:	2
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:	iata-25May2023.shtml
Detection:	MAL
Classification:	mal52.phis.winSHTML@24/0@6/7
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: .shtml

Warnings

- Excluded IPs from analysis (whitelisted): 172.217.168.3, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information

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 CRLF line terminators
Entropy (8bit):	4.492634755198107
TrID:	
File name:	iata-25May2023.shtml
File size:	3081826
MD5:	38f37466740c0aa09b17fd1f9c260a30
SHA1:	d9dc91b0df8a03a5d14ee5de5c6d4385ad9a32cf
SHA256:	48cd890109fa77fac8ee43807cd4a5e65fec600b9b7a7ea68be528ac81c4eb6a
SHA512:	7f3b7e69e428ecddc1f23bcf9bf18a9be95553cb1961954f160a33670a513dd1712141f28b221161e6d7ddad0919d8ef9a66927685496ceba4326b57f1fce701
SSDEEP:	24576:Z6Mzvx9mp6DA1Q3Re6h9D1RHaQhJ7E5dLqOAMsWdllsV56oqZdd5bbFnkza:1fFAO5pGYW7hqe
TLSH:	F5E5659C5A019AC44F01CC71B9021C09F28B7DCAAFAB0BA5DD659360B7FF671BE1D4A1
File Content Preview:	<!Doctype html><marquee onstart='var fzknjalsdk = `%3..C%..21..DO..CT..YP..E%..20..ht..ml..%3..E%..0A..%3..Ch..ea..d%..3E..%0..A%..3C..ti..tl..e%..3E..%3..C/..ti..tl..e%..3E..%0..A%..3C..sc..ri..pt..%2..0s..rc..%3..D%..22..%2..2%..3E..%3..C/..sc..ri..pt..

File Icon

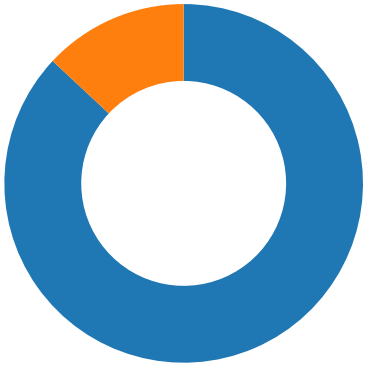
Icon Hash:	0f3149cc4c490307

Network Behavior

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:51:12.374830961 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.374862909 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.374924898 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.375211000 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.375274897 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.375348091 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.375921011 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.375931978 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.376101971 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.376137972 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.516033888 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.516360044 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.516415119 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.516670942 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.516848087 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.516932011 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.518029928 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.518117905 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.518235922 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.518265963 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.520411015 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.520514965 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.766942978 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.767162085 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.767194986 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.767426968 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.767661095 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.767785072 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.767805099 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.767903090 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.801027060 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.801146030 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.801187038 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.801290035 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.801359892 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.804172039 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:51:12.804205894 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:51:12.808182955 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.808207035 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.847625971 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.847805977 CEST	49695	443	192.168.2.4	172.217.168.45

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:51:12.847826958 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.847934961 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:12.848015070 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.860277891 CEST	49695	443	192.168.2.4	172.217.168.45
May 26, 2023 11:51:12.860325098 CEST	443	49695	172.217.168.45	192.168.2.4
May 26, 2023 11:51:16.093437910 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.093512058 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.093750954 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.094300032 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.094336033 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.154120922 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.154529095 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.154561043 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.156131029 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.156223059 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.159624100 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.159774065 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.199790955 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:16.199856997 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:16.246659994 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:26.209671974 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:26.209805965 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:51:26.209920883 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:26.985879898 CEST	49700	443	192.168.2.4	142.250.203.100
May 26, 2023 11:51:26.985919952 CEST	443	49700	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.153338909 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:16.153429985 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.153543949 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:16.154000044 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:16.154035091 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.203176975 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.203567982 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:16.203605890 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.204420090 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.204991102 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:16.205843925 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:16.248635054 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:26.191317081 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:26.191519022 CEST	443	49706	142.250.203.100	192.168.2.4
May 26, 2023 11:52:26.191634893 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:26.657365084 CEST	49706	443	192.168.2.4	142.250.203.100
May 26, 2023 11:52:26.657411098 CEST	443	49706	142.250.203.100	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:51:12.333345890 CEST	58565	53	192.168.2.4	8.8.8.8
May 26, 2023 11:51:12.334191084 CEST	52239	53	192.168.2.4	8.8.8.8
May 26, 2023 11:51:12.353100061 CEST	53	58565	8.8.8.8	192.168.2.4
May 26, 2023 11:51:12.353858948 CEST	53	52239	8.8.8.8	192.168.2.4
May 26, 2023 11:51:16.047595024 CEST	59444	53	192.168.2.4	8.8.8.8
May 26, 2023 11:51:16.067703009 CEST	53	59444	8.8.8.8	192.168.2.4
May 26, 2023 11:51:16.073899031 CEST	55570	53	192.168.2.4	8.8.8.8
May 26, 2023 11:51:16.088655949 CEST	53	55570	8.8.8.8	192.168.2.4
May 26, 2023 11:52:16.111325026 CEST	63229	53	192.168.2.4	8.8.8.8
May 26, 2023 11:52:16.134435892 CEST	53	63229	8.8.8.8	192.168.2.4
May 26, 2023 11:52:16.137195110 CEST	58576	53	192.168.2.4	8.8.8.8
May 26, 2023 11:52:16.151894093 CEST	53	58576	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2023

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 11:51:12.333345890 CEST	192.168.2.4	8.8.8.8	0xa740	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:12.334191084 CEST	192.168.2.4	8.8.8.8	0x6830	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:16.047595024 CEST	192.168.2.4	8.8.8.8	0xef8b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:16.073899031 CEST	192.168.2.4	8.8.8.8	0xda00	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:16.111325026 CEST	192.168.2.4	8.8.8.8	0xd3af	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:16.137195110 CEST	192.168.2.4	8.8.8.8	0x8593	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

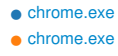
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 11:51:12.353100061 CEST	8.8.8.8	192.168.2.4	0xa740	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:51:12.353100061 CEST	8.8.8.8	192.168.2.4	0xa740	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:12.353858948 CEST	8.8.8.8	192.168.2.4	0x6830	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:16.067703009 CEST	8.8.8.8	192.168.2.4	0xef8b	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:51:16.088655949 CEST	8.8.8.8	192.168.2.4	0xda00	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:16.134435892 CEST	8.8.8.8	192.168.2.4	0xd3af	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:16.151894093 CEST	8.8.8.8	192.168.2.4	0x8593	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **5688**, Parent PID: **3528**

General

Target ID:	0
Start time:	11:51:09
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\iata-25May2023.shtml
Imagebase:	0x7ff683680000
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

Analysis Process: chrome.exe PID: **5148**, Parent PID: **5688**

General

Target ID:	1
Start time:	11:51:10
Start date:	26/05/2023
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1888 --field-trial-handle=1812,i,18360485486545431331,5420382872932820938,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
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

Disassembly

No disassembly

Copyright Joe Security LLC 2023