ID: 800689
Cookbook: browseurl.jbs
Time: 18:11:59
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report http://suzy_lamplugh@email.dhqbmail.co.uk 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 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 7
General Information 8
Errors 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
Network Behavior 9
Network Port Distribution 9
TCP Packets 9
UDP Packets 11
DNS Queries 11
DNS Answers 11
HTTP Request Dependency Graph 12
Statistics 12
Behavior 12
System Behavior 12
Analysis Process: chrome.exePID: 5504, Parent PID: 3716 12
General 12
File Activities 13
Registry Activities 13
Analysis Process: chrome.exePID: 4720, Parent PID: 5504 13
General 13
File Activities 13
Analysis Process: chrome.exePID: 5268, Parent PID: 3716 13
General 13
Registry Activities 13
Disassembly 14

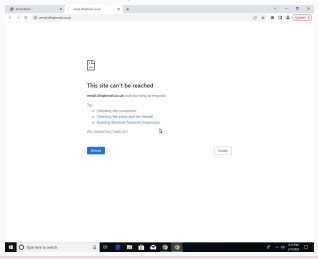
Windows Analysis Report

http://suzy_lamplugh@email.dhqbmail.co.uk

Overview

General Information

Sample URL:	http://suzy_lamplugh@email.dhqbmail.co.uk
Analysis ID:	800689
Infos:	



Errors

URL not reachable

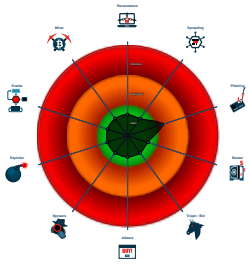
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5504 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4720 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=1948 --field-trial-handle=1776,i,12988346674410521245,11443754851562044237,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5268 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://suzy_lamplugh@email.dhqbmail.co.uk MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

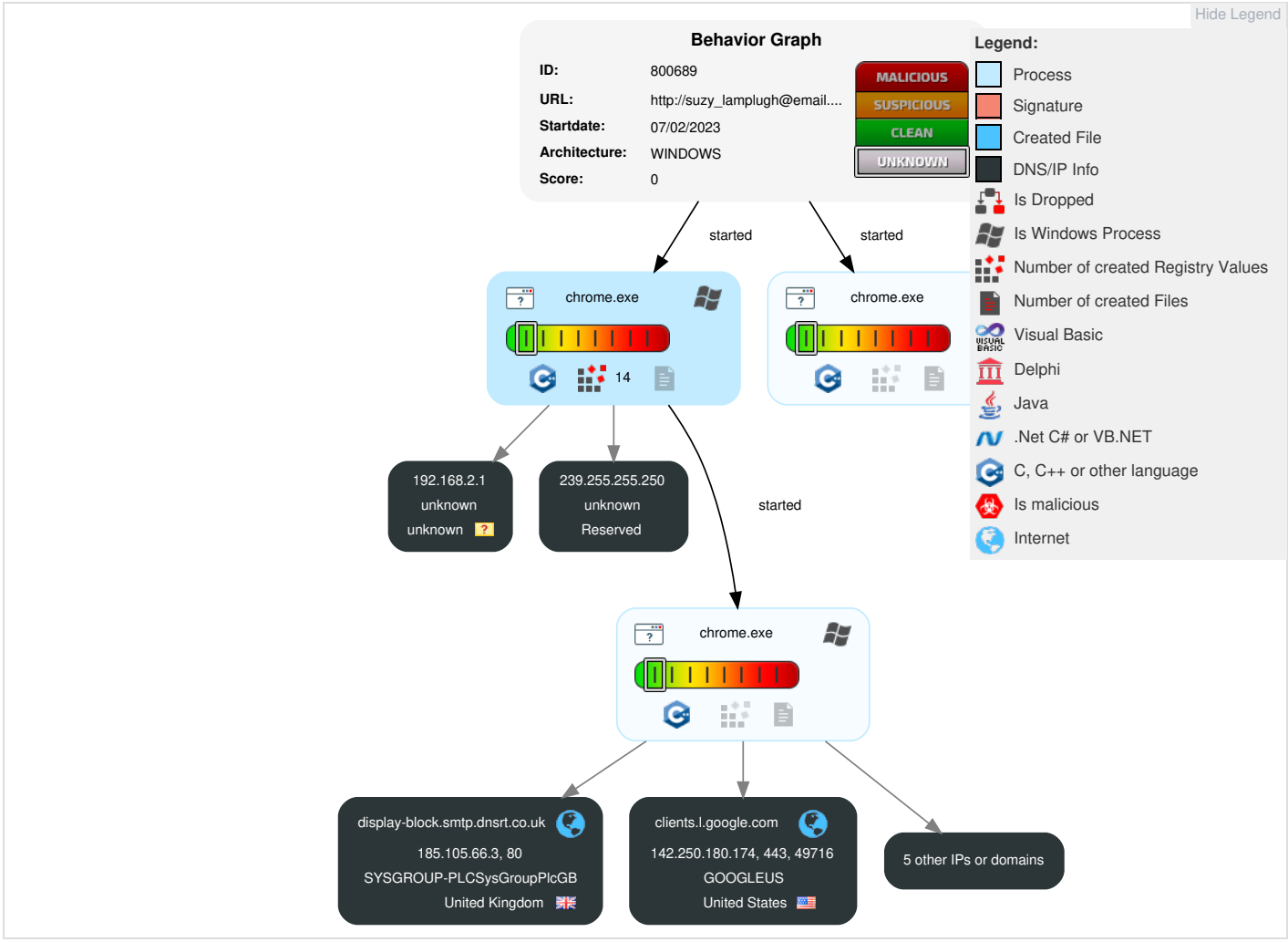
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	1 Process Injection	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	Rootkit	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

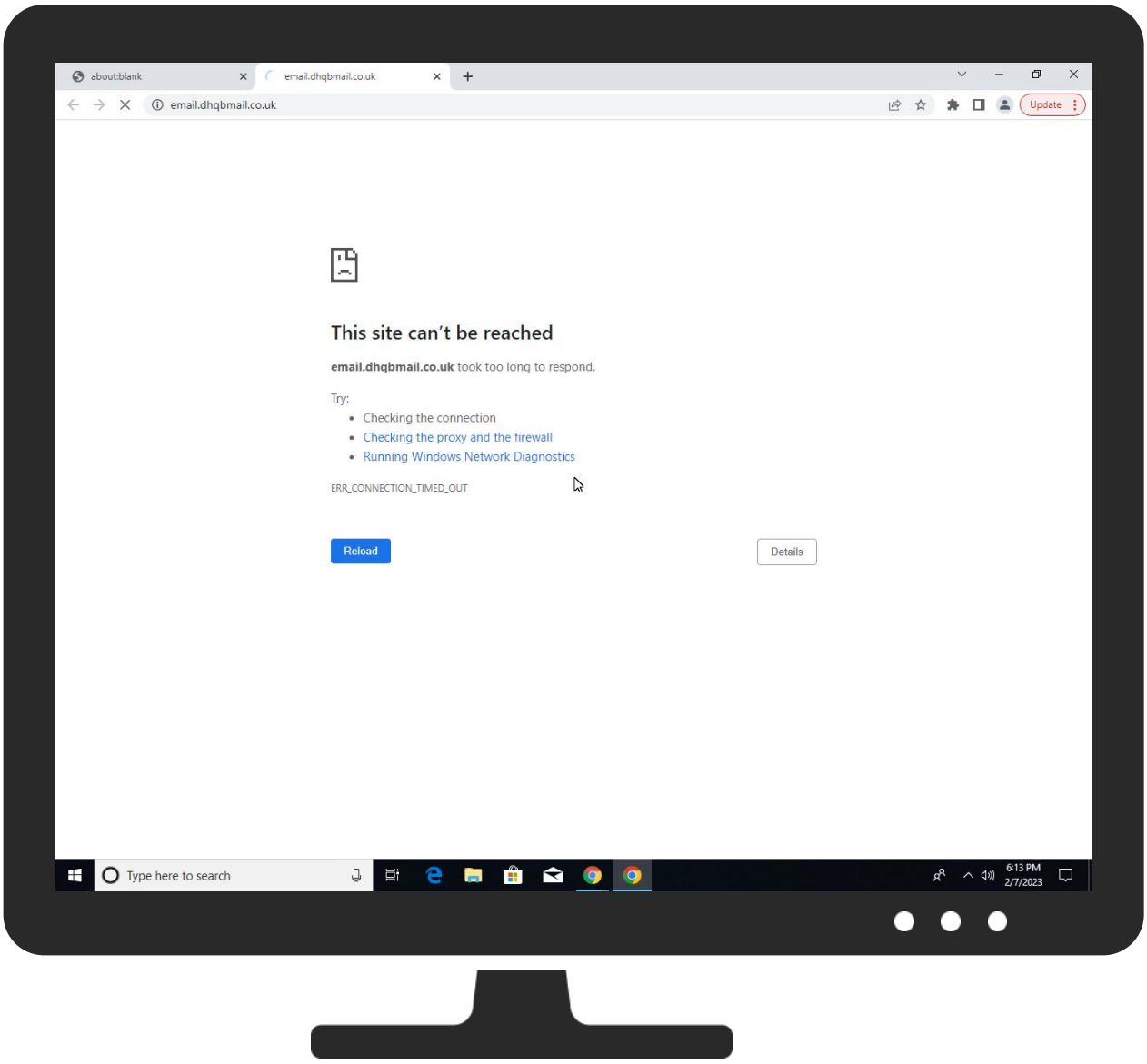
Behavior Graph



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
http://suzy_lamplugh@email.dhqbmail.co.uk	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

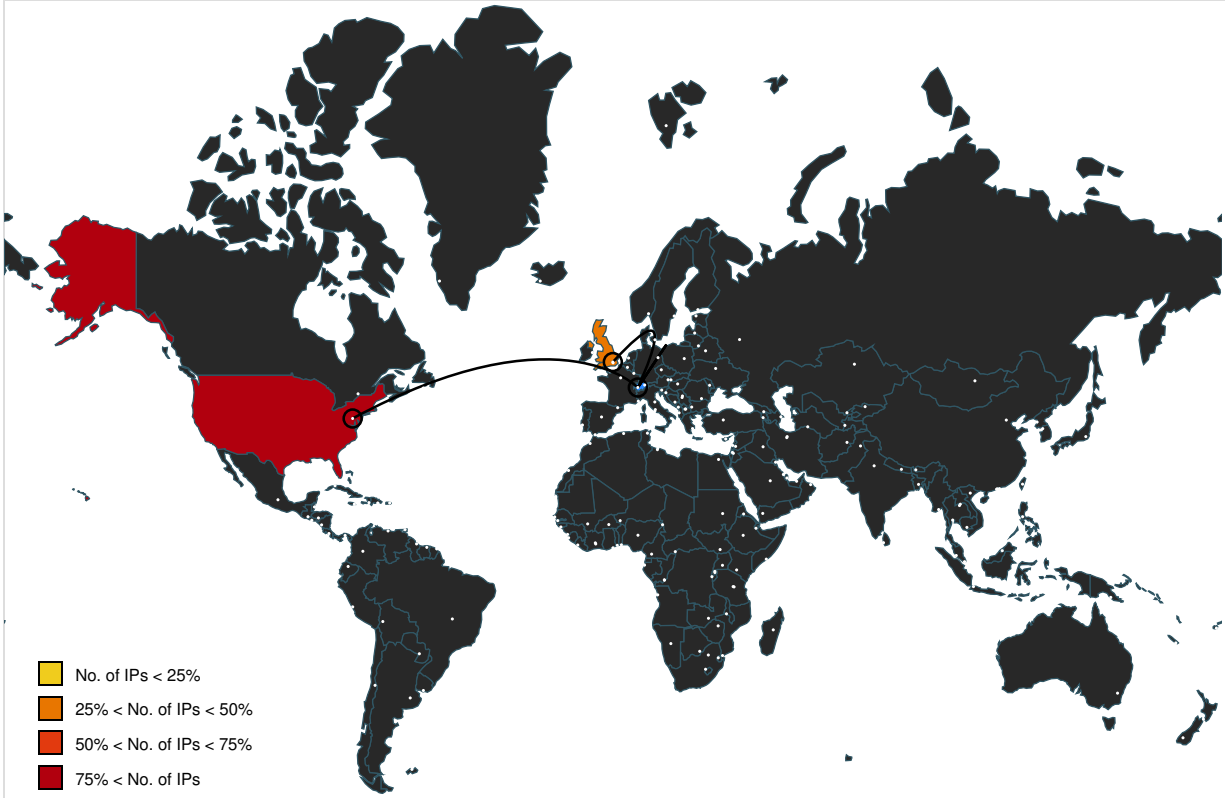
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
display-block.smtp.dnsrt.co.uk	185.105.66.3	true	false		unknown
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
clients2.google.com	unknown	unknown	false		high
email.dhqbmail.co.uk	unknown	unknown	false		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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.105.66.3	display-block.smtp.dnsrt.co.uk	United Kingdom		16376	SYSGROUP-PLCSysGroupPlcGB	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800689
Start date and time:	2023-02-07 18:11:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://suzy_lamplugh@email.dhqbmail.co.uk
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:	10
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:	UNKNOWN
Classification:	unknown0.win@26/0@5/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• **URL browsing timeout or error**

Errors

- URL not reachable

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 173.222.108.226, 173.222.108.147, 20.90.156.32
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wns.notify.trafficmanager.net, fs.microsoft.com, edgedl.me.gvt1.com, clientservices.googleapis.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.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

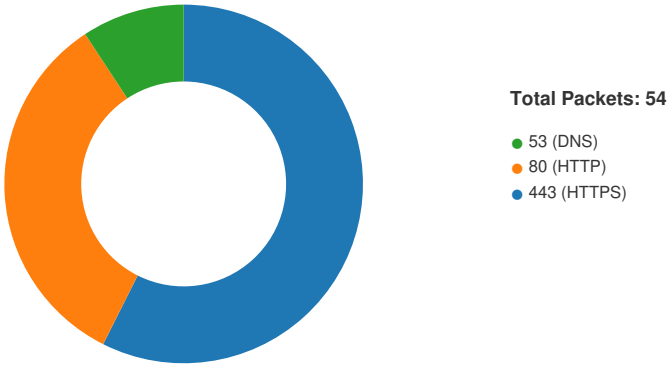
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:13:08.977057934 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:08.977112055 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:08.977189064 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:08.977653980 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:08.977675915 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:08.991761923 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:08.991813898 CET	443	49717	216.58.209.45	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:13:08.991892099 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:08.992202997 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:08.992223024 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:08.994379044 CET	49718	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:08.994667053 CET	49719	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:09.021274090 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.021325111 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.021403074 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.021858931 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.021876097 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.067209005 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.067732096 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.067771912 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.069708109 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.069825888 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.083945990 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.091051102 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.103393078 CET	49721	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:09.103852987 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.103885889 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.104120016 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.104152918 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.105175972 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.105264902 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.106584072 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.106652975 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.108134031 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.108233929 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.372176886 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.372239113 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.372409105 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.372714043 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.372754097 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.373064041 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.373100996 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.373191118 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.378617048 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.378680944 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.378803015 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.378812075 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.378967047 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.421870947 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.422056913 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.422074080 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.422128916 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.424755096 CET	49716	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:13:09.424787045 CET	443	49716	142.250.180.174	192.168.2.6
Feb 7, 2023 18:13:09.439872026 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.439980030 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.440031052 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.440068960 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.440126896 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.442322016 CET	49717	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:13:09.442367077 CET	443	49717	216.58.209.45	192.168.2.6
Feb 7, 2023 18:13:09.457576036 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:09.457597017 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:09.557614088 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:12.057815075 CET	49719	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:12.087819099 CET	49718	80	192.168.2.6	185.105.66.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:13:12.157824039 CET	49721	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:18.058303118 CET	49719	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:18.088257074 CET	49718	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:18.158711910 CET	49721	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:19.067739964 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:19.067867994 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:19.067989111 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:20.547534943 CET	49720	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:13:20.547583103 CET	443	49720	142.250.184.100	192.168.2.6
Feb 7, 2023 18:13:31.136977911 CET	49735	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:31.137228012 CET	49736	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:31.393841982 CET	49737	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:34.159620047 CET	49736	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:34.190045118 CET	49735	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:34.489706039 CET	49737	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:40.160026073 CET	49736	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:40.193042040 CET	49735	80	192.168.2.6	185.105.66.3
Feb 7, 2023 18:13:40.490796089 CET	49737	80	192.168.2.6	185.105.66.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:13:08.940345049 CET	62910	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:13:08.942428112 CET	63229	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:13:08.945241928 CET	62538	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:13:08.946662903 CET	54903	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:13:08.969158888 CET	53	62910	8.8.8.8	192.168.2.6
Feb 7, 2023 18:13:08.974514008 CET	53	54903	8.8.8.8	192.168.2.6
Feb 7, 2023 18:13:08.981478930 CET	53	63229	8.8.8.8	192.168.2.6
Feb 7, 2023 18:13:08.983982086 CET	53	62538	8.8.8.8	192.168.2.6
Feb 7, 2023 18:13:08.990489006 CET	51530	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:13:09.019473076 CET	53	51530	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:13:08.940345049 CET	192.168.2.6	8.8.8.8	0x648b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.942428112 CET	192.168.2.6	8.8.8.8	0x7199	Standard query (0)	email.dhqbmail.co.uk	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.945241928 CET	192.168.2.6	8.8.8.8	0x2298	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.946662903 CET	192.168.2.6	8.8.8.8	0xdf55	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.990489006 CET	192.168.2.6	8.8.8.8	0x3352	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
Feb 7, 2023 18:13:08.969158888 CET	8.8.8.8	192.168.2.6	0x648b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:13:08.969158888 CET	8.8.8.8	192.168.2.6	0x648b	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.974514008 CET	8.8.8.8	192.168.2.6	0xdf55	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.981478930 CET	8.8.8.8	192.168.2.6	0x7199	No error (0)	email.dhqbmail.co.uk	display-block.smtp.dnsrt.co.uk		CNAME (Canonical name)	IN (0x0001)	false

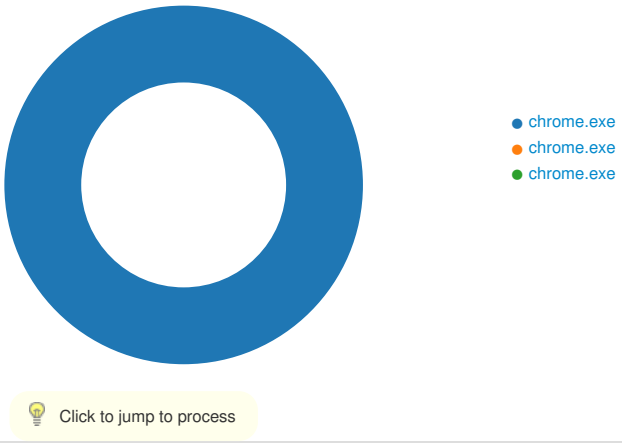
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:13:08.981478930 CET	8.8.8.8	192.168.2.6	0x7199	No error (0)	display-block.smtp.dnsrt.co.uk		185.105.66.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:08.983982086 CET	8.8.8.8	192.168.2.6	0x2298	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:13:09.019473076 CET	8.8.8.8	192.168.2.6	0x3352	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5504**, Parent PID: **3716**

General

Target ID:	0
Start time:	18:13:02
Start date:	07/02/2023
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:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

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

Registry Activities

Analysis Process: chrome.exe PID: **4720**, Parent PID: **5504**

General

Target ID:	1
Start time:	18:13:04
Start date:	07/02/2023
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=1948 --field-trial-handle=1776,i,12988346674410521245,11443754851562044237,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: **5268**, Parent PID: **3716**

General

Target ID:	2
Start time:	18:13:04
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://suzy_lamplugh@email.dhqbmail.co.uk
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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