ID: 778233
Cookbook: browseurl.jbs
Time: 09:01:24
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report http://c499eaf6.edwardsinstallationsltd.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
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 12
HTTP Request Dependency Graph 12
Statistics 12
Behavior 12
System Behavior 13
Analysis Process: chrome.exePID: 5956, Parent PID: 4588 13
General 13
File Activities 13
Registry Activities 13
Analysis Process: chrome.exePID: 4984, Parent PID: 5956 13
General 13
File Activities 14
Analysis Process: chrome.exePID: 6160, Parent PID: 4588 14
General 14
Registry Activities 14
Disassembly 14

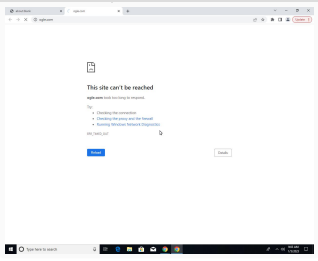
Windows Analysis Report

http://c499eaf6.edwardsinstallationsltd.co.uk/

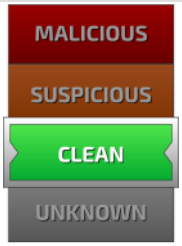
Overview

General Information

Sample URL:	http://c499eaf6.edwardsinstallationsltd.co.uk/
Analysis ID:	778233
Infos:	



Detection

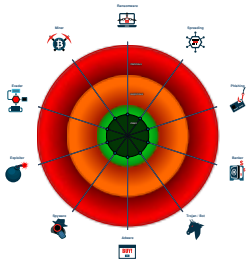


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5956 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4984 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=1932 --field-trial-handle=1748,i,12783018763609111580,4223455923677708739,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6160 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://c499eaf6.edwardsinstallationsltd.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

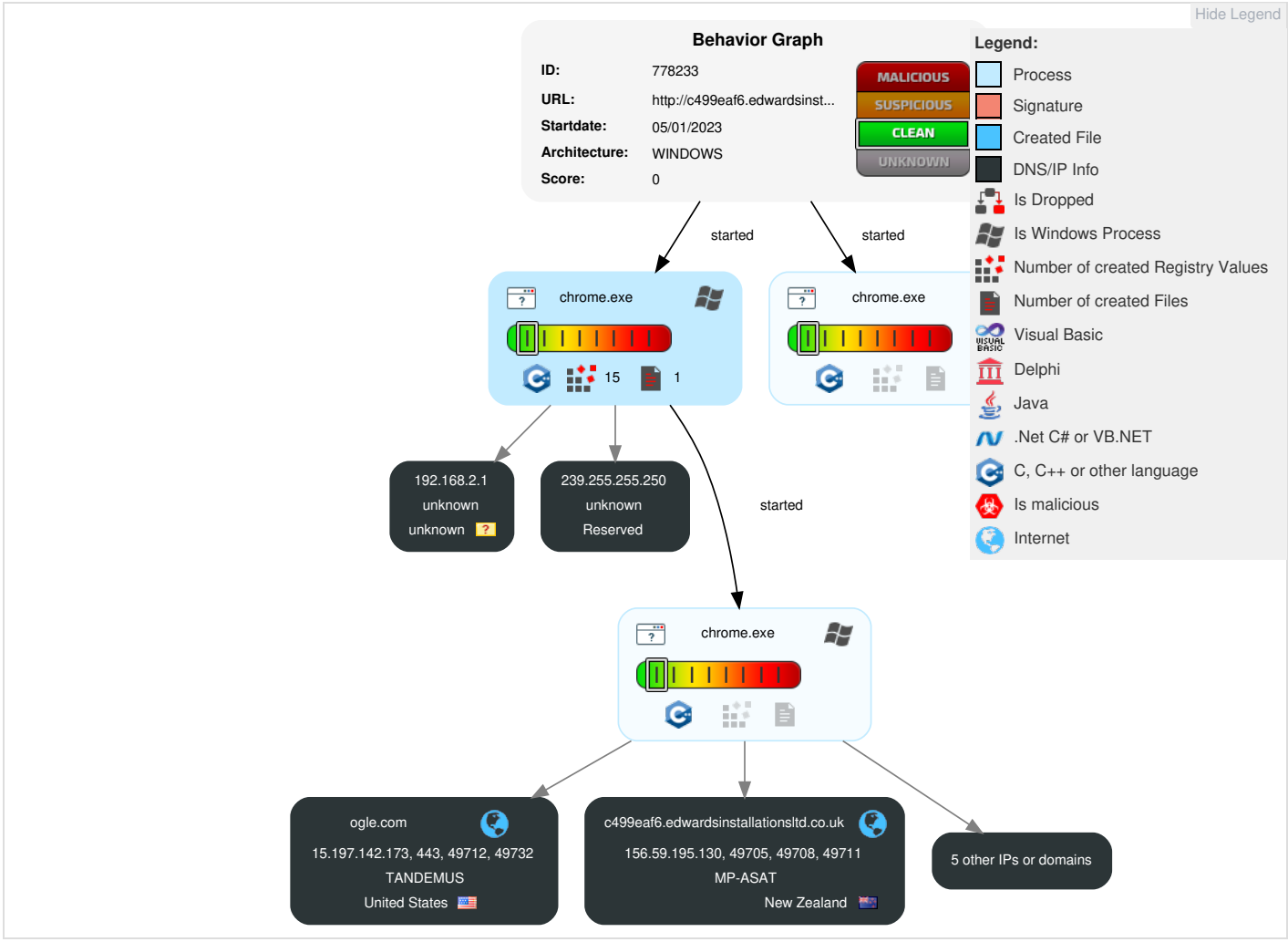
Joe Sandbox Signatures

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	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

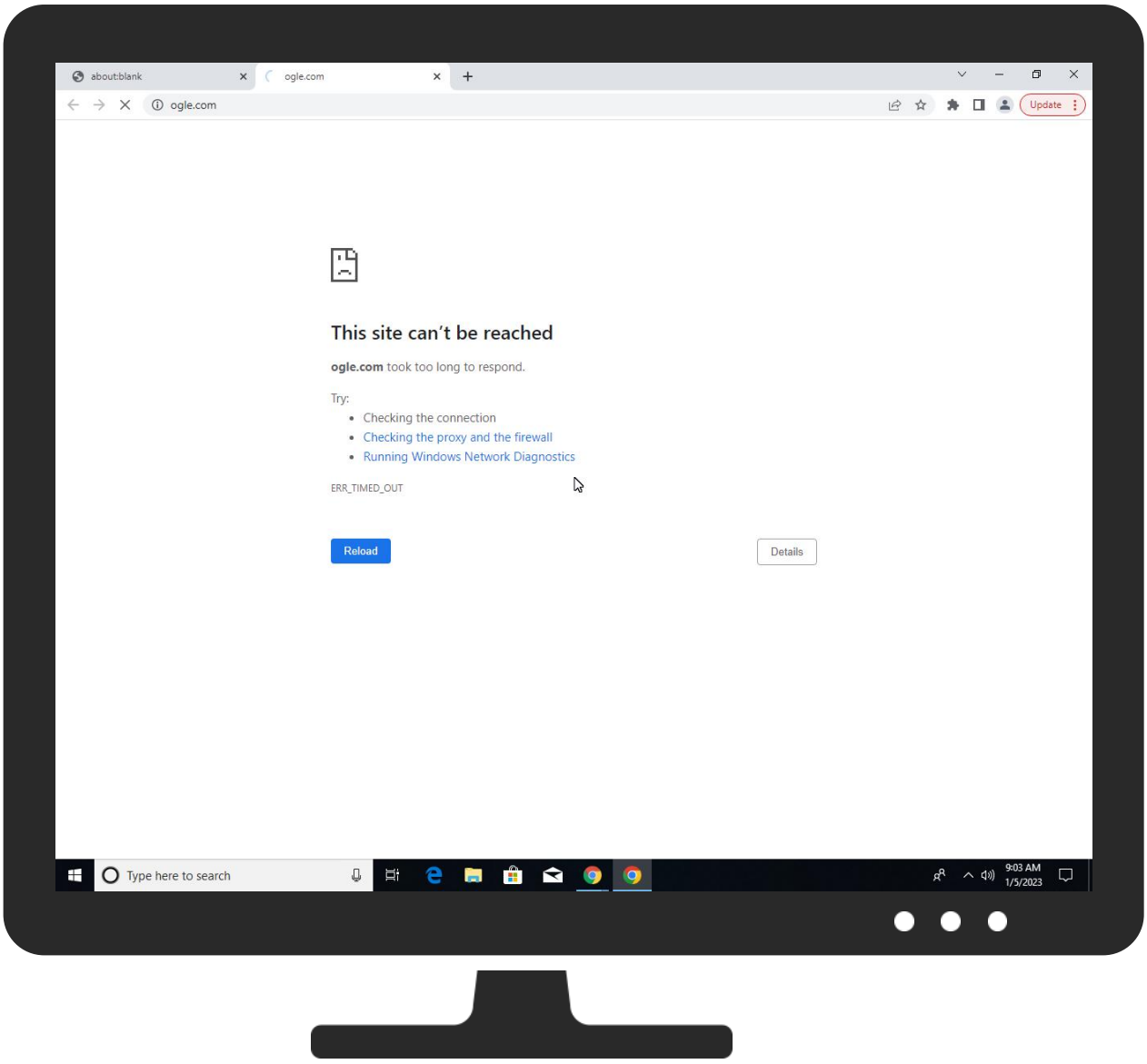
Behavior Graph



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
http://c499eaf6.edwardsinstallationsltd.co.uk/	0%	Virustotal		Browse
http://c499eaf6.edwardsinstallationsltd.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

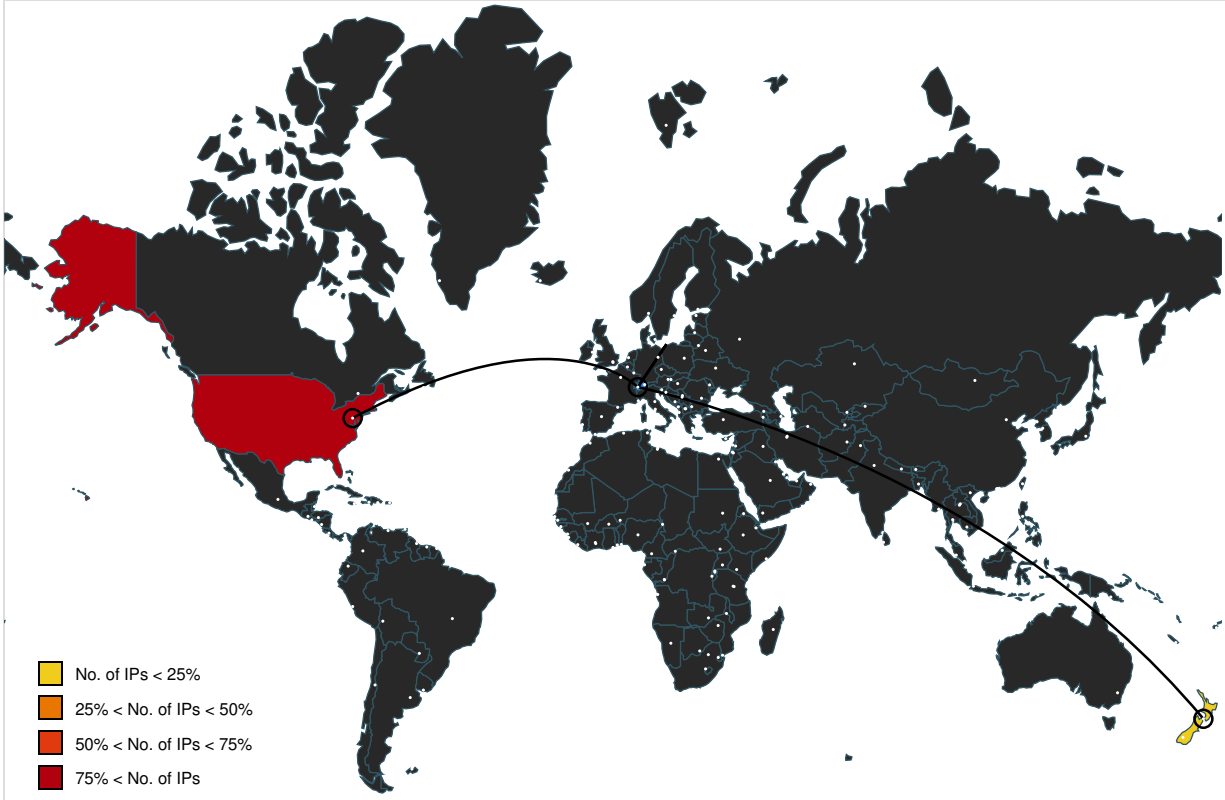
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ogle.com	15.197.142.173	true	false		unknown
accounts.google.com	142.251.209.13	true	false		high
c499eaf6.edwardsinstallationsltd.co.uk	156.59.195.130	true	false		unknown
www.google.com	142.250.184.36	true	false		high
clients.l.google.com	142.250.184.78	true	false		high
clients2.google.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
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://c499eaf6.edwardsinstallationsltd.co.uk/	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.78	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.36	www.google.com	United States		15169	GOOGLEUS	false
15.197.142.173	ogle.com	United States		7430	TANDEMUS	false
142.251.209.13	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
156.59.195.130	c499eaf6.edwardsinstallationsltd.co.uk	New Zealand		199083	MP-ASAT	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778233
Start date and time:	2023-01-05 09:01:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://c499eaf6.edwardsinstallationsltd.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:	5
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:	CLEAN
Classification:	clean0.win@29/0@7/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.35, 34.104.35.123, 142.250.184.99, 142.250.184.67
- Excluded domains from analysis (whitelisted): client.wns.windows.com, edgedl.me.gvt1.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.gstatic.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

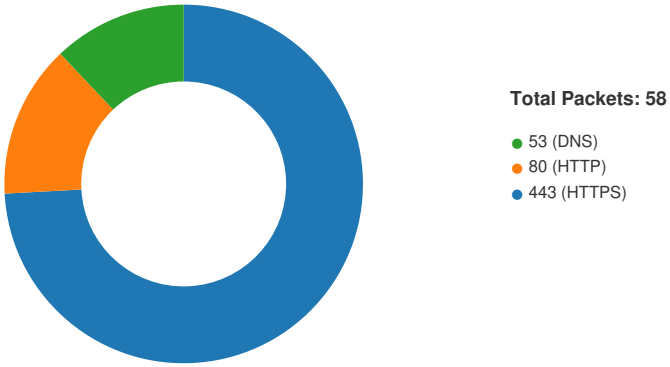
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:02:23.836384058 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.836473942 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.836699009 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.836867094 CET	49705	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:23.837862968 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:23.837888956 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:23.837953091 CET	49707	443	192.168.2.5	142.251.209.13

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:02:23.838314056 CET	49708	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:23.839148998 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:23.839169025 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:23.839224100 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:23.839603901 CET	49711	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:23.839888096 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.839931011 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.840367079 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:23.840382099 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:23.841425896 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:23.841439962 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:23.920623064 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.921334028 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.921377897 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.921843052 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.921962976 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.922777891 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:23.922868967 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:23.973788023 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:23.974622011 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.030558109 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.031131029 CET	80	49711	156.59.195.130	192.168.2.5
Jan 5, 2023 09:02:24.031280994 CET	49711	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:24.075100899 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.131783962 CET	80	49708	156.59.195.130	192.168.2.5
Jan 5, 2023 09:02:24.131992102 CET	49708	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:24.146416903 CET	80	49705	156.59.195.130	192.168.2.5
Jan 5, 2023 09:02:24.146508932 CET	49705	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:24.177342892 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.177386045 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.179884911 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.179943085 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.179997921 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.272586107 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.368721008 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.368782043 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.371659040 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.371731997 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.371761084 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.433572054 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.519285917 CET	49711	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:24.760751009 CET	80	49711	156.59.195.130	192.168.2.5
Jan 5, 2023 09:02:24.882585049 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.882612944 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.882848978 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.882877111 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.882891893 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.882971048 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.883105993 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.883117914 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.883368015 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:24.883414984 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.883480072 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:24.883490086 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.883569956 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.926923990 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.926990032 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:24.927031040 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.927139997 CET	443	49704	142.250.184.78	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:02:24.927187920 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:24.939505100 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.939541101 CET	443	49710	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.945216894 CET	49704	443	192.168.2.5	142.250.184.78
Jan 5, 2023 09:02:24.945254087 CET	443	49704	142.250.184.78	192.168.2.5
Jan 5, 2023 09:02:24.952675104 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.952714920 CET	80	49711	156.59.195.130	192.168.2.5
Jan 5, 2023 09:02:24.952745914 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.952765942 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.952869892 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:24.952914000 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.961368084 CET	49707	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:24.961395025 CET	443	49707	142.251.209.13	192.168.2.5
Jan 5, 2023 09:02:25.072576046 CET	49711	80	192.168.2.5	156.59.195.130
Jan 5, 2023 09:02:25.079389095 CET	49712	443	192.168.2.5	15.197.142.173
Jan 5, 2023 09:02:25.079435110 CET	443	49712	15.197.142.173	192.168.2.5
Jan 5, 2023 09:02:25.079545021 CET	49712	443	192.168.2.5	15.197.142.173
Jan 5, 2023 09:02:25.079845905 CET	49712	443	192.168.2.5	15.197.142.173
Jan 5, 2023 09:02:25.079858065 CET	443	49712	15.197.142.173	192.168.2.5
Jan 5, 2023 09:02:25.131617069 CET	49710	443	192.168.2.5	142.251.209.13
Jan 5, 2023 09:02:25.756771088 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.756855965 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.756973982 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.757189035 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.757220030 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.825167894 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.838792086 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.838865995 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.840248108 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.840385914 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.842569113 CET	49714	443	192.168.2.5	142.250.184.36
Jan 5, 2023 09:02:25.842587948 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.842732906 CET	443	49714	142.250.184.36	192.168.2.5
Jan 5, 2023 09:02:25.972664118 CET	49714	443	192.168.2.5	142.250.184.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:02:23.630899906 CET	49724	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:02:23.659053087 CET	53	49724	8.8.8.8	192.168.2.5
Jan 5, 2023 09:02:23.688591003 CET	61452	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:02:23.694727898 CET	51484	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:02:23.720295906 CET	53	51484	8.8.8.8	192.168.2.5
Jan 5, 2023 09:02:23.723825932 CET	53	61452	8.8.8.8	192.168.2.5
Jan 5, 2023 09:02:25.046854019 CET	56751	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:02:25.068192959 CET	53	56751	8.8.8.8	192.168.2.5
Jan 5, 2023 09:02:25.736881971 CET	60975	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:02:25.754796982 CET	53	60975	8.8.8.8	192.168.2.5
Jan 5, 2023 09:03:25.843914986 CET	57482	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:03:25.861615896 CET	53	57482	8.8.8.8	192.168.2.5
Jan 5, 2023 09:03:31.692584991 CET	60294	53	192.168.2.5	8.8.8.8
Jan 5, 2023 09:03:31.710455894 CET	53	60294	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
Jan 5, 2023 09:02:23.630899906 CET	192.168.2.5	8.8.8.8	0x2b4f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:02:23.688591003 CET	192.168.2.5	8.8.8.8	0xd82c	Standard query (0)	c499eaf6.edwardsinstallationsltd.co.uk	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:23.694727898 CET	192.168.2.5	8.8.8.8	0xb65b	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:25.046854019 CET	192.168.2.5	8.8.8.8	0xf0a4	Standard query (0)	ogle.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:25.736881971 CET	192.168.2.5	8.8.8.8	0x9da8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:25.843914986 CET	192.168.2.5	8.8.8.8	0x6401	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:31.692584991 CET	192.168.2.5	8.8.8.8	0x5ced	Standard query (0)	ogle.com	A (IP address)	IN (0x0001)	false

DNS Answers

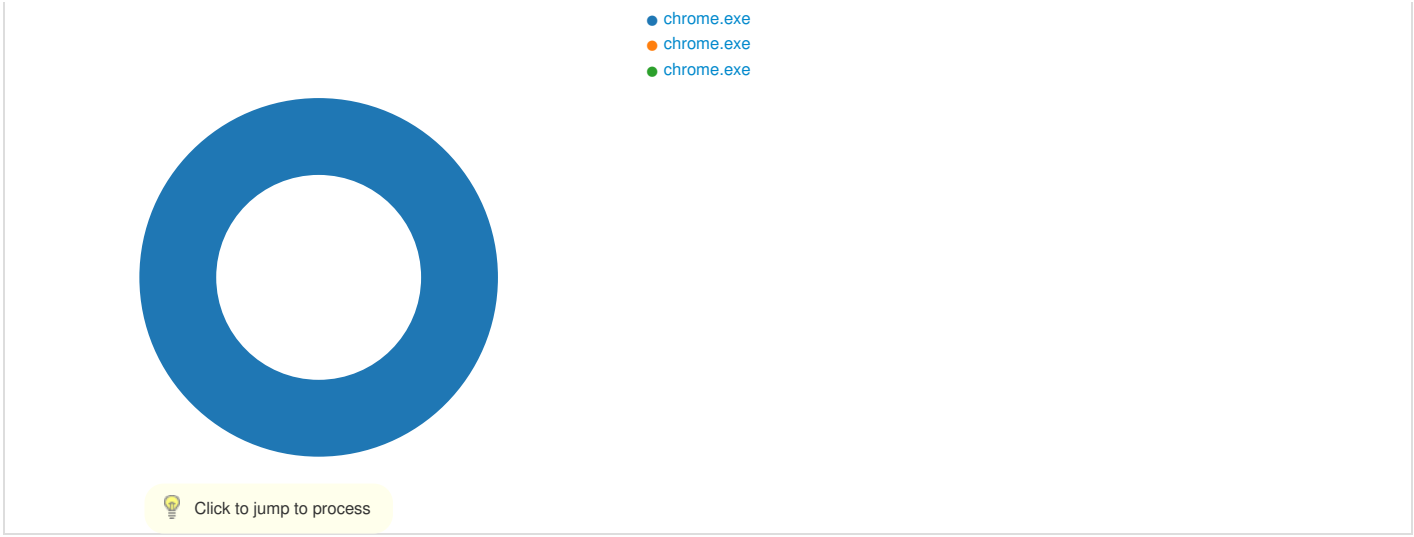
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:02:23.659053087 CET	8.8.8.8	192.168.2.5	0x2b4f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:02:23.659053087 CET	8.8.8.8	192.168.2.5	0x2b4f	No error (0)	clients.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:23.720295906 CET	8.8.8.8	192.168.2.5	0xb65b	No error (0)	accounts.google.com		142.251.209.13	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:23.723825932 CET	8.8.8.8	192.168.2.5	0xd82c	No error (0)	c499eaf6.edwardsinstallationsltd.co.uk		156.59.195.130	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:25.068192959 CET	8.8.8.8	192.168.2.5	0xf0a4	No error (0)	ogle.com		15.197.142.173	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:25.068192959 CET	8.8.8.8	192.168.2.5	0xf0a4	No error (0)	ogle.com		3.33.152.147	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:02:25.754796982 CET	8.8.8.8	192.168.2.5	0x9da8	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:25.861615896 CET	8.8.8.8	192.168.2.5	0x6401	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:31.710455894 CET	8.8.8.8	192.168.2.5	0x5ced	No error (0)	ogle.com		15.197.142.173	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:31.710455894 CET	8.8.8.8	192.168.2.5	0x5ced	No error (0)	ogle.com		3.33.152.147	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- c499eaf6.edwardsinstallationsltd.co.uk

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5956, Parent PID: 4588

General

Target ID:	0
Start time:	09:02:18
Start date:	05/01/2023
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:	low

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: 4984, Parent PID: 5956

General

Target ID:	1
Start time:	09:02:20
Start date:	05/01/2023
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=1932 --field-trial-handle=1748,i,12783018763609111580,4223455923677708739,131072 --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:	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

Analysis Process: chrome.exe PID: **6160**, Parent PID: **4588**

General

Target ID:	2
Start time:	09:02:21
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://c499eaf6.edwardsinstallationsltd.co.uk/
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:	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