ID: 800713
Cookbook: browseurl.jbs
Time: 18:33:56
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

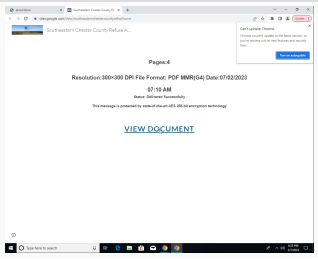
Windows Analysis Report

https://sites.google.com/view/southeasternchestercountyrefus/home

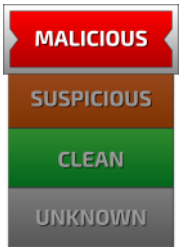
Overview

General Information

Sample URL:	http://https://sites.google.com/view/southeasternchestercountyrefus/home
Analysis ID:	800713
Infos:	



Detection

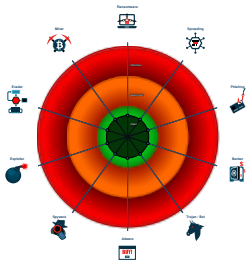


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4688 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1116 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=1576 --field-trial-handle=1844,i,10637429234006776294,9776587234221978637,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2432 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://sites.google.com/view/southeasternchestercountyrefus/home 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

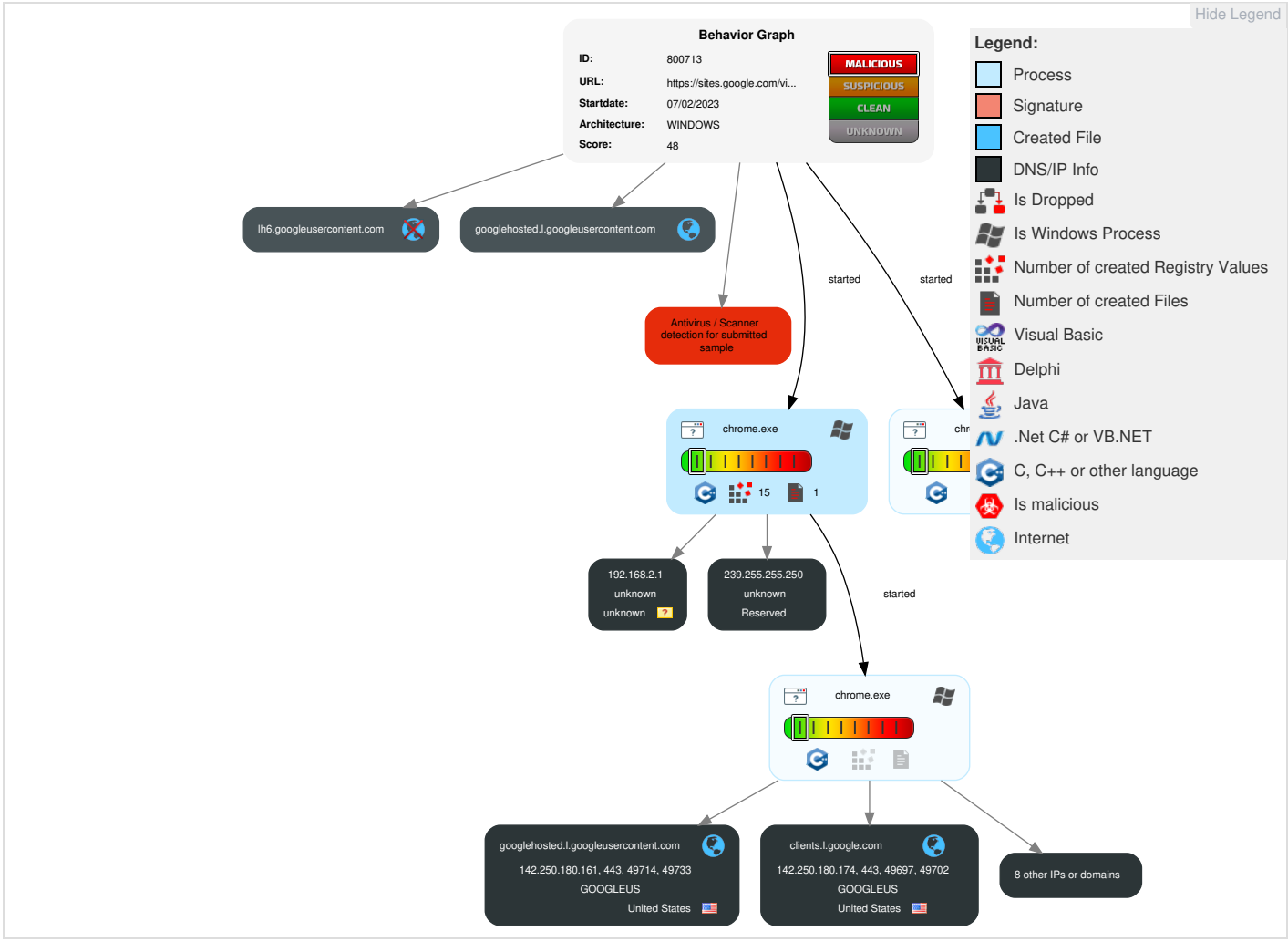
AV Detection

Antivirus / Scanner detection for submitted sample

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

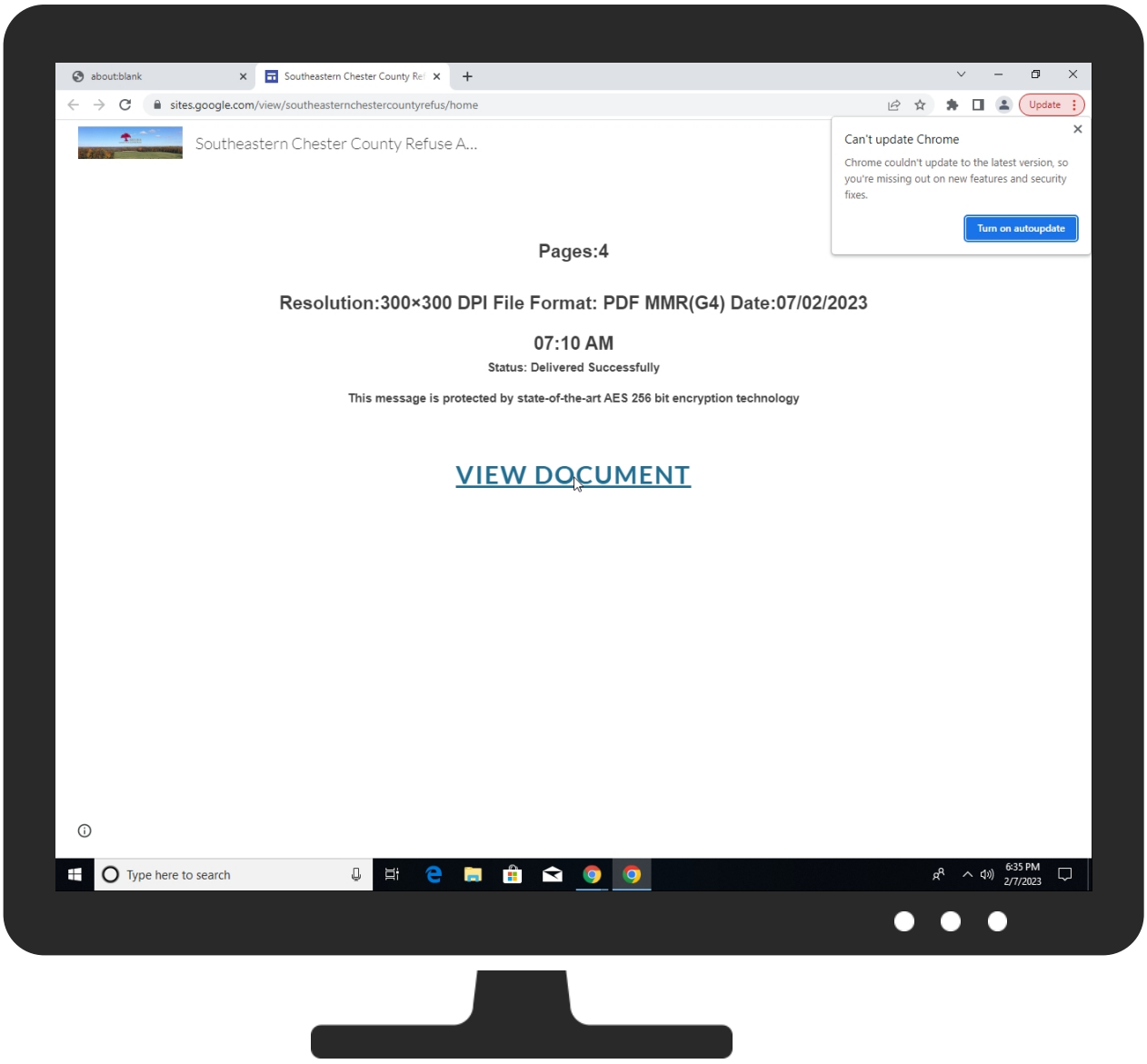
Behavior Graph



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://https://sites.google.com/view/southeasternchestercountyrefus/home	0%	Avira URL Cloud	safe	
http://https://sites.google.com/view/southeasternchestercountyrefus/home	1%	Virustotal		Browse
http://https://sites.google.com/view/southeasternchestercountyrefus/home	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

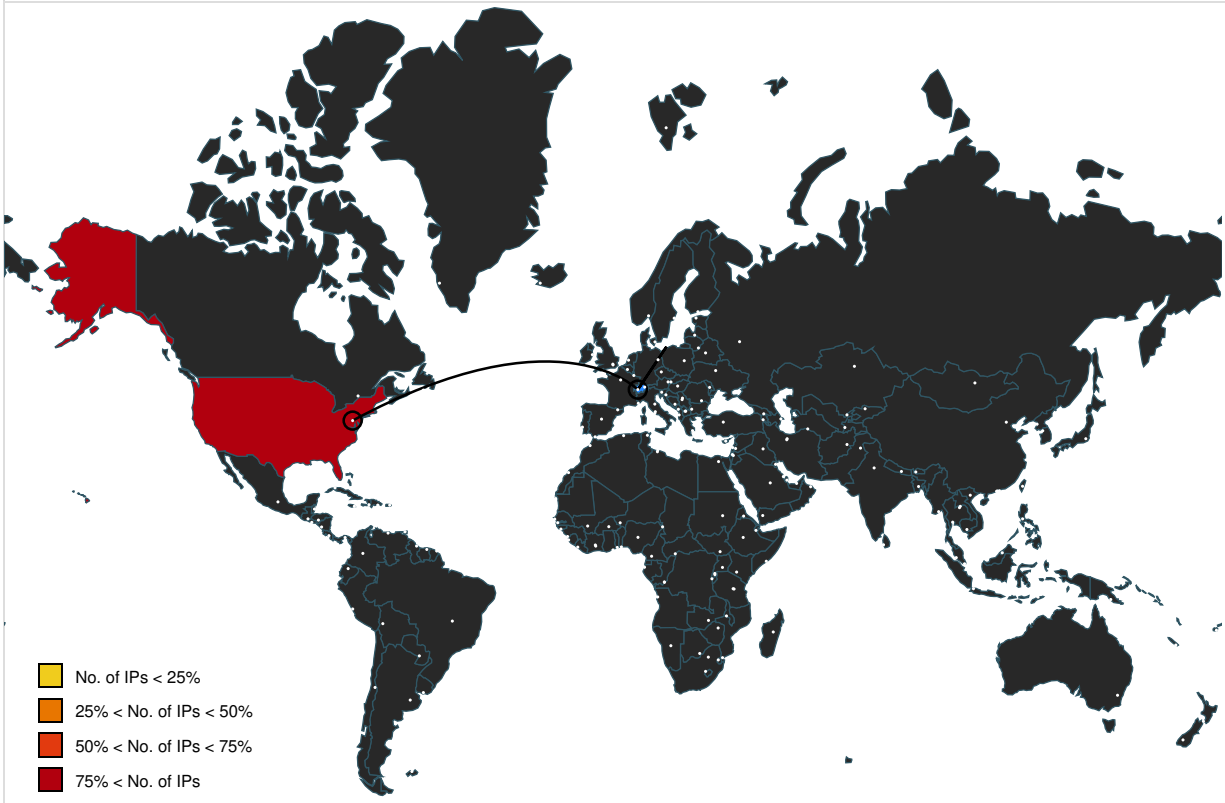
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
plus.l.google.com	142.250.184.110	true	false		high
sites.google.com	142.250.184.78	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.161	true	false		high
clients2.google.com	unknown	unknown	false		high
lh6.googleusercontent.com	unknown	unknown	false		high
apis.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://lh6.googleusercontent.com/xBeHiJ-CSXhPY2tjWkIedmRNH737CR6-tuCPOrWoomysQnz4KXL_8S5U8c4UZkQ7Vxd5KbWTXG3S06MPGp2-PFw=w16383	false		high
http://https://sites.google.com/_/view/logImpressions?authuser=0	false		high
http://https://sites.google.com/view/southeasternchestercountyrefus/home	false		high
http://https://sites.google.com/view/southeasternchestercountyrefus/home	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.lb.en.AMZ27oQJoUI.O/m=client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo9dsXwz2g0gTMdQFEKa7ZoVvtQf4g/cb=gapi.loaded_0?le=scs	false		high
http://https://apis.google.com/js/client.js?onload=gapiLoaded	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
142.250.184.78	sites.google.com	United States		15169	GOOGLEUS	false
142.250.184.110	plus.l.google.com	United States		15169	GOOGLEUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.180.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	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:	800713
Start date and time:	2023-02-07 18:33:56 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sites.google.com/view/southeasternchestercountyrefus/home
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:	14
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:	mal48.win@25/0@8/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://bafybeidr4sutsrgsviivzdf6ljqgkxjbrrnfl46ee3qxvuzwb2ch4ukdmi.ipfs.dweb.link/microsoftonline%20%281%29%20%281%29.html

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.163, 142.250.180.138, 142.250.184.67, 142.250.184.74, 142.250.184.106, 142.250.180.170, 142.251.209.10, 142.251.209.42
- Excluded domains from analysis (whitelisted): www.bing.com, fonts.googleapis.com, ssl.gstatic.com, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, fonts.gstatic.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

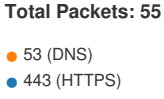
No created / dropped files found

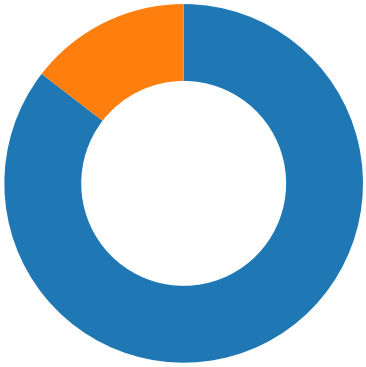
Static File Info

No static file info

Network Behavior

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:58.474042892 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.474109888 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.474217892 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.475406885 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.475429058 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.475498915 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.476669073 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.476720095 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.476808071 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.477111101 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.477145910 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.477221012 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.478216887 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.478257895 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.479079962 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.479105949 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.479882956 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.479902983 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.480287075 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.480314016 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.557678938 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.580547094 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.621932983 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.647264957 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.648318052 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.648344994 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.648531914 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.648569107 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.649200916 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.649221897 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.649297953 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.650199890 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.650202036 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.650244951 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.650291920 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.650295019 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.658399105 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.658443928 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.658588886 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.658637047 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.659082890 CET	443	49702	142.250.180.174	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:58.659182072 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.659903049 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:58.660026073 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:58.662796021 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:58.662930012 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:58.761827946 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.785820007 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.785897970 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.786006927 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.786053896 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.786072969 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.786338091 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.786731958 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.786768913 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.786993027 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.787019968 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.787193060 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.787216902 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.787259102 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.787436962 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.787451029 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.787468910 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.829991102 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.830110073 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.830140114 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.830288887 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.830379963 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.832557917 CET	49697	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.832595110 CET	443	49697	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.855396032 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.855545998 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.855576992 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.855742931 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.855837107 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.861915112 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.861941099 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:34:59.867892981 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.867925882 CET	443	49702	142.250.180.174	192.168.2.3
Feb 7, 2023 18:34:59.961931944 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.967911959 CET	49702	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:34:59.986751080 CET	49701	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:34:59.986798048 CET	443	49701	216.58.209.45	192.168.2.3
Feb 7, 2023 18:35:00.396269083 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.396361113 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.396972895 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.429040909 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.429100037 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.496269941 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.498800039 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.498850107 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.499684095 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.500598907 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.501034975 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.502197981 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.503266096 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.503266096 CET	49703	443	192.168.2.3	142.250.184.78
Feb 7, 2023 18:35:00.503281116 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.503299952 CET	443	49703	142.250.184.78	192.168.2.3
Feb 7, 2023 18:35:00.503451109 CET	443	49703	142.250.184.78	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:58.091293097 CET	49977	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:34:58.094388008 CET	57840	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:34:58.119580030 CET	53	49977	8.8.8.8	192.168.2.3
Feb 7, 2023 18:34:58.123442888 CET	53	57840	8.8.8.8	192.168.2.3
Feb 7, 2023 18:34:59.797871113 CET	57990	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:34:59.826196909 CET	53	57990	8.8.8.8	192.168.2.3
Feb 7, 2023 18:35:00.854302883 CET	51139	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:35:00.880187035 CET	53	51139	8.8.8.8	192.168.2.3
Feb 7, 2023 18:35:01.269999981 CET	60582	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:35:01.275713921 CET	57134	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:35:01.287965059 CET	53	60582	8.8.8.8	192.168.2.3
Feb 7, 2023 18:35:01.316416979 CET	53	57134	8.8.8.8	192.168.2.3
Feb 7, 2023 18:35:04.348099947 CET	57704	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:35:04.368143082 CET	53	57704	8.8.8.8	192.168.2.3
Feb 7, 2023 18:36:01.427582979 CET	65017	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:36:01.454190969 CET	53	65017	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:34:58.091293097 CET	192.168.2.3	8.8.8.8	0x6802	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:58.094388008 CET	192.168.2.3	8.8.8.8	0x159c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:59.797871113 CET	192.168.2.3	8.8.8.8	0x535a	Standard query (0)	sites.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:00.854302883 CET	192.168.2.3	8.8.8.8	0x1f01	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:01.269999981 CET	192.168.2.3	8.8.8.8	0xfd15	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:01.275713921 CET	192.168.2.3	8.8.8.8	0xef35	Standard query (0)	lh6.googleusercontent.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:04.348099947 CET	192.168.2.3	8.8.8.8	0x48bd	Standard query (0)	lh6.googleusercontent.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:36:01.427582979 CET	192.168.2.3	8.8.8.8	0x1ce2	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 18:34:58.119580030 CET	8.8.8.8	192.168.2.3	0x6802	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:58.123442888 CET	8.8.8.8	192.168.2.3	0x159c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:58.123442888 CET	8.8.8.8	192.168.2.3	0x159c	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:59.826196909 CET	8.8.8.8	192.168.2.3	0x535a	No error (0)	sites.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:00.880187035 CET	8.8.8.8	192.168.2.3	0x1f01	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:35:00.880187035 CET	8.8.8.8	192.168.2.3	0x1f01	No error (0)	plus.l.google.com		142.250.184.110	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:01.287965059 CET	8.8.8.8	192.168.2.3	0xfd15	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:01.316416979 CET	8.8.8.8	192.168.2.3	0xef35	No error (0)	lh6.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false

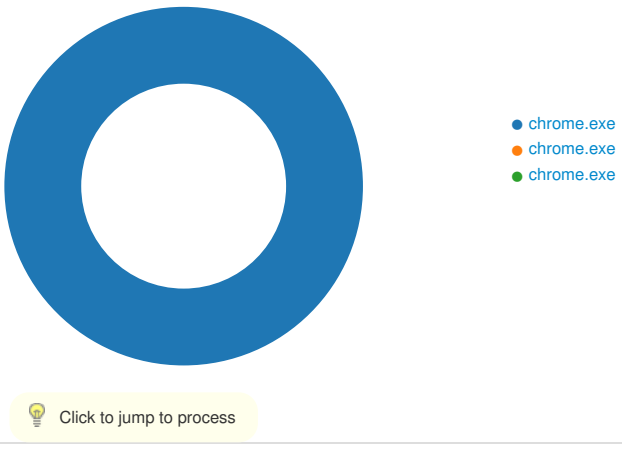
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:35:01.316416979 CET	8.8.8.8	192.168.2.3	0xef35	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.161	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:04.368143082 CET	8.8.8.8	192.168.2.3	0x48bd	No error (0)	lh6.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:35:04.368143082 CET	8.8.8.8	192.168.2.3	0x48bd	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.161	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:36:01.454190969 CET	8.8.8.8	192.168.2.3	0x1ce2	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
- sites.google.com
- https:
  - apis.google.com
  - lh6.googleusercontent.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4688**, Parent PID: **1948**

General

Target ID:	0
Start time:	18:34:54
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:	0x7ff614650000
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: **1116**, Parent PID: **4688**

General

Target ID:	1
Start time:	18:34:55
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=1576 --field-trial-handle=1844,i,10637429234006776294,9776587234221978637,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **2432**, Parent PID: **1948**

General

Target ID:	2
Start time:	18:34:57
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" "https://sites.google.com/view/southeasternchestercountyrefus/home
Imagebase:	0x7ff614650000
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