ID: 764041
Cookbook: browseurl.jbs
Time: 10:56:20
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

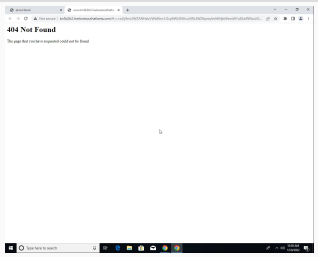
Windows Analysis Report

http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVW..

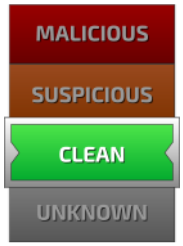
Overview

General Information

Sample URL:	www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHc...Nnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
Analysis ID:	764041
Infos:	



Detection

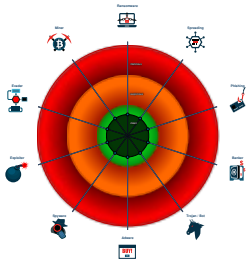


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5852 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2080 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=1956 --field-trial-handle=1568,i,14781660650222300864,2008606683164464388,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 676 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga 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

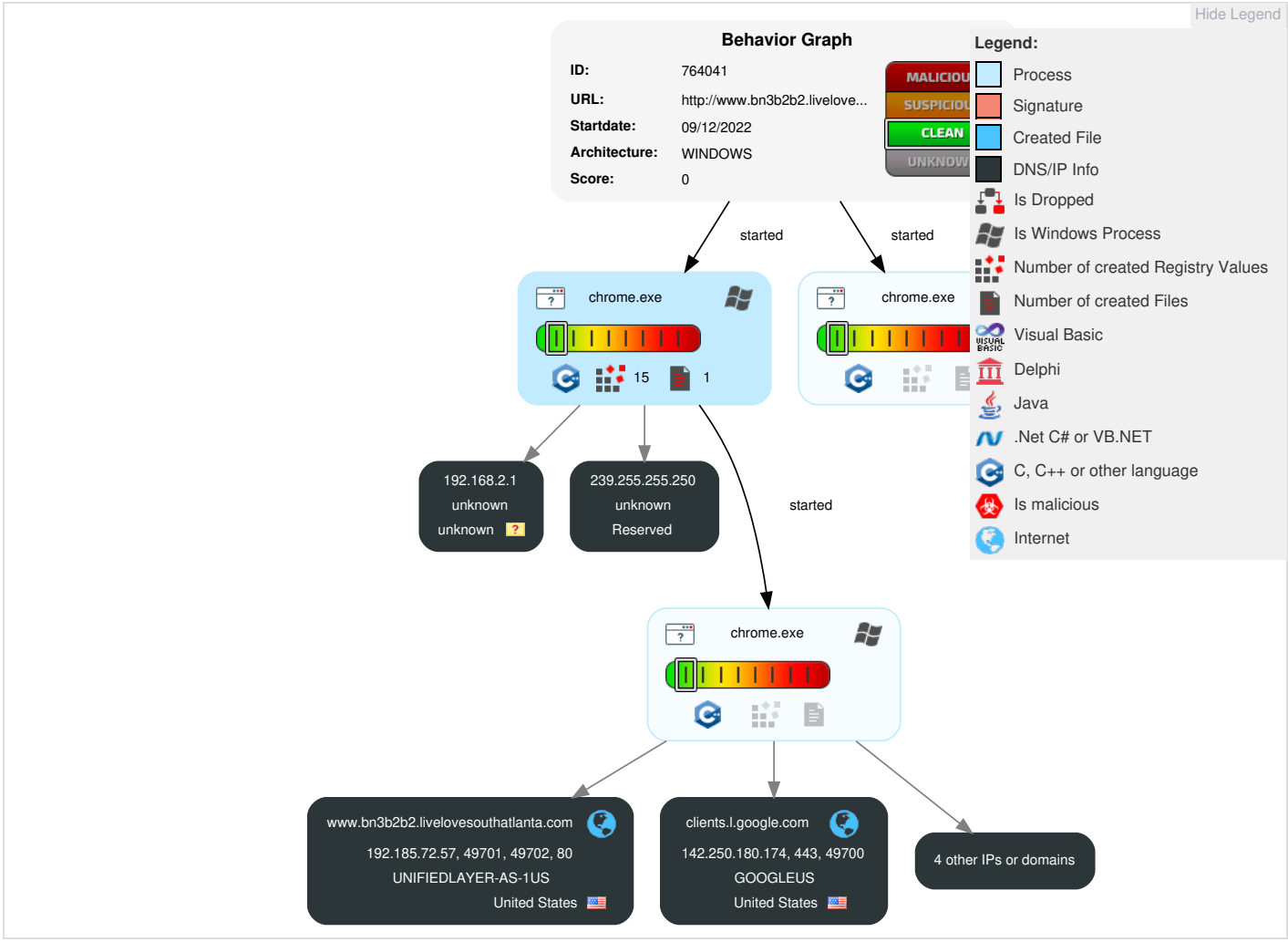
Joe Sandbox Signatures

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

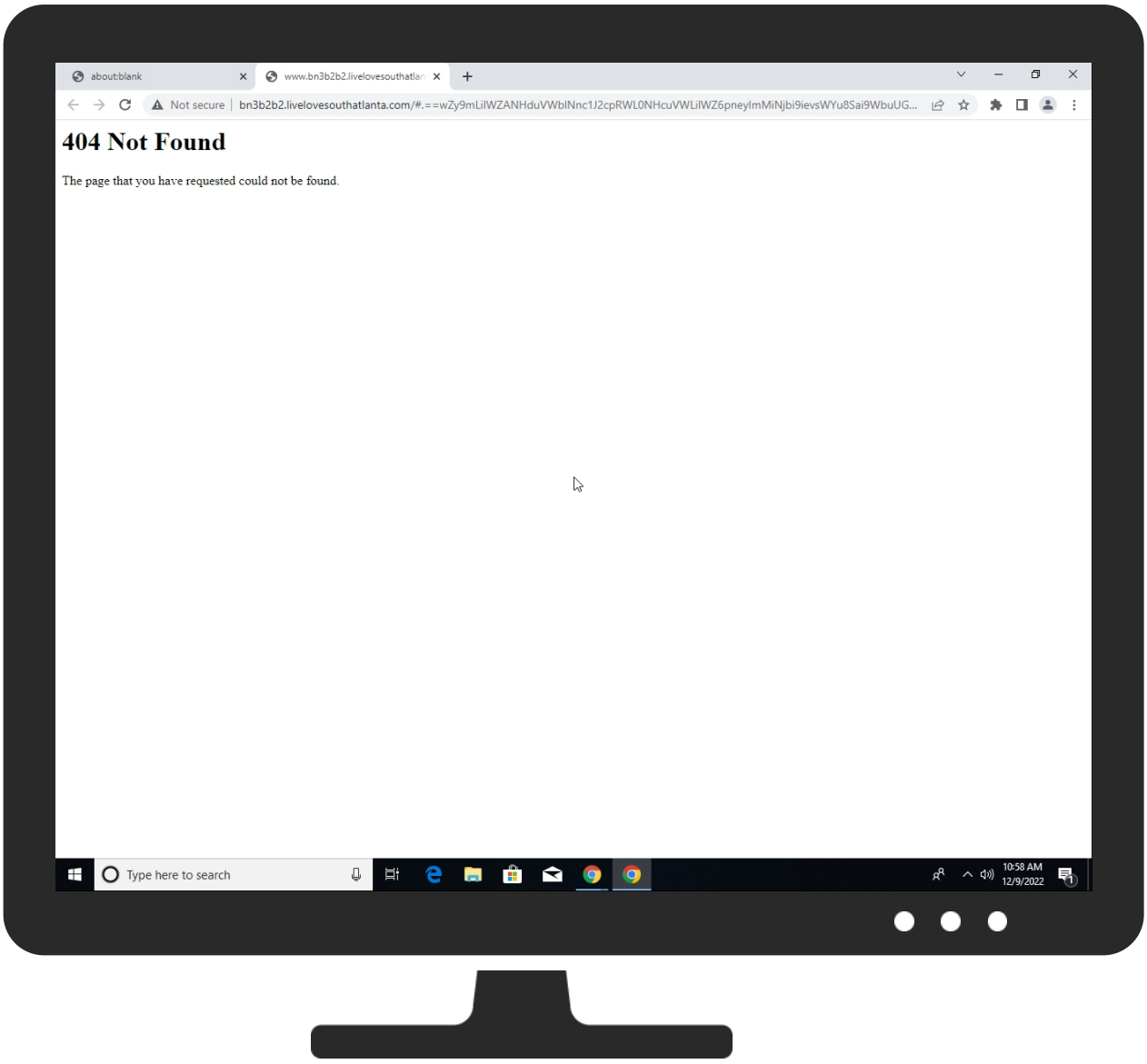
Behavior Graph



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://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLiIWZANHduVWblNnc1J2cpRWL0NHcuVWLiIWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	0%	Virustotal		Browse
http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLiIWZANHduVWblNnc1J2cpRWL0NHcuVWLiIWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.bn3b2b2.livelovesouthatlanta.com/favicon.ico	0%	Avira URL Cloud	safe	
http://www.bn3b2b2.livelovesouthatlanta.com/	0%	Virustotal		Browse
http://www.bn3b2b2.livelovesouthatlanta.com/	0%	Avira URL Cloud	safe	
http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	0%	Virustotal		Browse

Domains and IPs

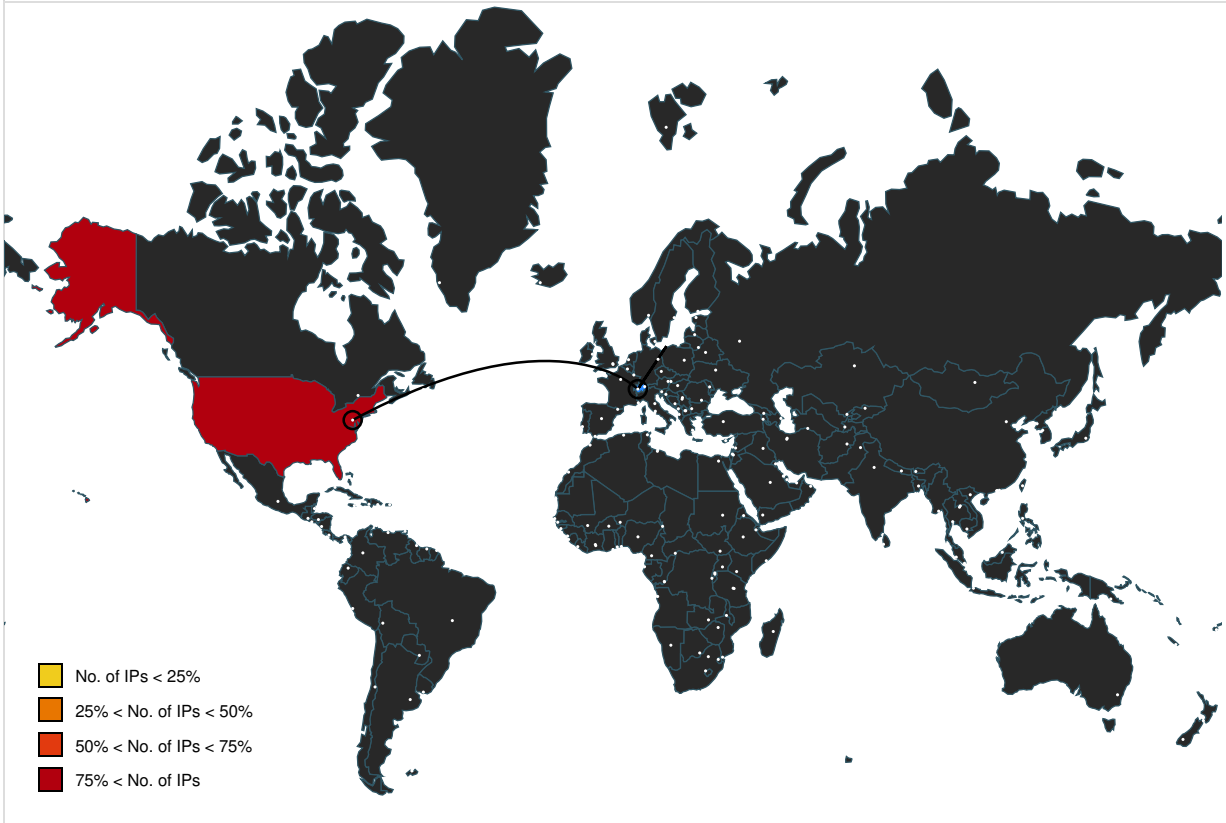
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bn3b2b2.livelovesouthatlanta.com	192.185.72.57	true	false		unknown
accounts.google.com	142.250.184.45	true	false		high
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

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://www.bn3b2b2.livelovesouthatlanta.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://www.bn3b2b2.livelovesouthatlanta.com/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	false	• 0%, Virustotal, Browse	unknown
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
142.250.184.45	accounts.google.com	United States		15169	GOOGLEUS	false
192.185.72.57	www.bn3b2b2.livelovesouthatlanta.com	United States		46606	UNIFIEDLAYER-AS-1US	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:	764041
Start date and time:	2022-12-09 10:56:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
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:	12
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@25/0@5/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.131
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, update.googleapis.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

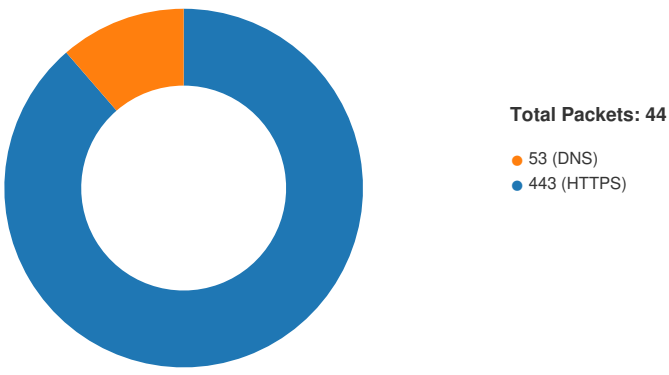
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:20.724873066 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.724934101 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.725014925 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.726068974 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.726111889 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.726172924 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.728313923 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.728343010 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.728728056 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.728750944 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.730803013 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:20.730840921 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.730901957 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:20.731277943 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:20.731292963 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.835386992 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.864635944 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.864667892 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.867883921 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.867994070 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.918857098 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.932934999 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.960460901 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:20.960499048 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.960747004 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.960781097 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.961427927 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.961510897 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:20.962198019 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:20.962276936 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:20.962980032 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:20.963032961 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.636409044 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:22.637362957 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.637438059 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.637751102 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.637768984 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.638407946 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.638686895 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.638722897 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.638853073 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.638897896 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.639143944 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.639234066 CET	443	49698	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.640693903 CET	49702	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:22.640885115 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.640924931 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.683183908 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.683331966 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.683383942 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.683446884 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.683516979 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.702456951 CET	49700	443	192.168.2.3	142.250.180.174
Dec 9, 2022 10:57:22.702514887 CET	443	49700	142.250.180.174	192.168.2.3
Dec 9, 2022 10:57:22.725333929 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.725374937 CET	443	49698	142.250.184.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:22.746534109 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.746670008 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.746696949 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.746809006 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.746889114 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.755578041 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:22.755878925 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:22.759623051 CET	80	49702	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:22.759800911 CET	49702	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:22.788525105 CET	49697	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.788569927 CET	443	49697	142.250.184.45	192.168.2.3
Dec 9, 2022 10:57:22.789776087 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:22.825318098 CET	49698	443	192.168.2.3	142.250.184.45
Dec 9, 2022 10:57:22.908603907 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:22.998321056 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:23.125403881 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:23.173238993 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.173305035 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.173408985 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.173826933 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.173846960 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.178301096 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:23.251678944 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.252096891 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.252139091 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.253683090 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.253808975 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.260540962 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.260575056 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.260813951 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.296937943 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:23.313225031 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:23.333353996 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.333395958 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:23.537157059 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:23.537168026 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:28.316688061 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:28.316771984 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:29.651099920 CET	49701	80	192.168.2.3	192.185.72.57
Dec 9, 2022 10:57:29.770451069 CET	80	49701	192.185.72.57	192.168.2.3
Dec 9, 2022 10:57:33.227669954 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:33.227756023 CET	443	49705	142.250.184.100	192.168.2.3
Dec 9, 2022 10:57:33.227863073 CET	49705	443	192.168.2.3	142.250.184.100
Dec 9, 2022 10:57:36.984302998 CET	49705	443	192.168.2.3	142.250.184.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:19.726564884 CET	62704	53	192.168.2.3	8.8.8.8
Dec 9, 2022 10:57:19.744106054 CET	53	62704	8.8.8.8	192.168.2.3
Dec 9, 2022 10:57:20.031619072 CET	57840	53	192.168.2.3	8.8.8.8
Dec 9, 2022 10:57:20.057452917 CET	53	57840	8.8.8.8	192.168.2.3
Dec 9, 2022 10:57:22.112679958 CET	52387	53	192.168.2.3	8.8.8.8
Dec 9, 2022 10:57:22.237191916 CET	53	52387	8.8.8.8	192.168.2.3
Dec 9, 2022 10:57:23.136977911 CET	53975	53	192.168.2.3	8.8.8.8
Dec 9, 2022 10:57:23.154027939 CET	53	53975	8.8.8.8	192.168.2.3
Dec 9, 2022 10:58:23.204354048 CET	58691	53	192.168.2.3	8.8.8.8
Dec 9, 2022 10:58:23.222253084 CET	53	58691	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
Dec 9, 2022 10:57:19.726564884 CET	192.168.2.3	8.8.8.8	0x1e04	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:20.031619072 CET	192.168.2.3	8.8.8.8	0xc336	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:22.112679958 CET	192.168.2.3	8.8.8.8	0x266d	Standard query (0)	www.bn3b2b2.livelovesouthatlanta.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:23.136977911 CET	192.168.2.3	8.8.8.8	0x9b61	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:58:23.204354048 CET	192.168.2.3	8.8.8.8	0xdc03	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

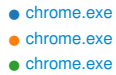
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:57:19.744106054 CET	8.8.8.8	192.168.2.3	0x1e04	No error (0)	accounts.google.com		142.250.184.45	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:20.057452917 CET	8.8.8.8	192.168.2.3	0xc336	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:57:20.057452917 CET	8.8.8.8	192.168.2.3	0xc336	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:22.237191916 CET	8.8.8.8	192.168.2.3	0x266d	No error (0)	www.bn3b2b2.livelovesouthatlanta.com		192.185.72.57	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:23.154027939 CET	8.8.8.8	192.168.2.3	0x9b61	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:58:23.222253084 CET	8.8.8.8	192.168.2.3	0xdc03	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

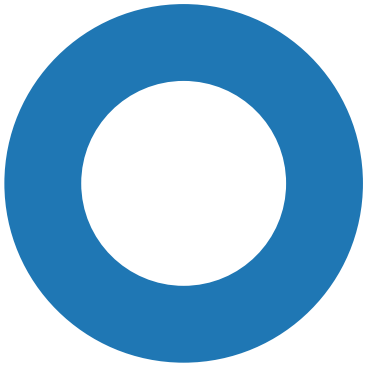
HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- www.bn3b2b2.livelovesouthatlanta.com

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5852, Parent PID: 2620

General

Target ID:	0
Start time:	10:58:07
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	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: 2080, Parent PID: 5852

General

Target ID:	1
Start time:	10:58:08
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1568,i,14781660650222300864,2008606683164464388,131072 --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: **676**, Parent PID: **2620**

General

Target ID:	2
Start time:	10:58:09
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.bn3b2b2.livelovesouthatlanta.com/#.==wZy9mLilWZANHduVWblNnc1J2cpRWL0NHcuVWLilWZ6pneyImMiNjbi9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
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