ID: 756169
Cookbook: browseurl.jbs
Time: 19:01:18
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

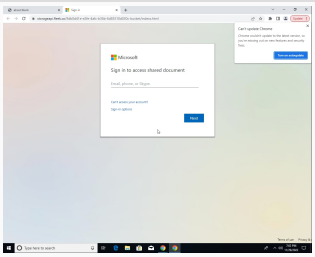
Windows Analysis Report

https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html

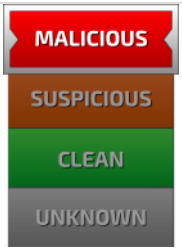
Overview

General Information

Sample URL:	http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html
Analysis ID:	756169
Infos:	



Detection



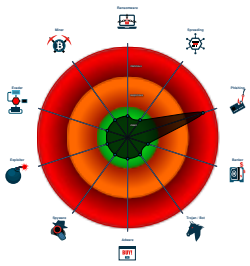
HTMLPhisher

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Multi AV Scanner detection for dom…
- Yara detected HtmlPhish10
- Multi AV Scanner detection for subm…
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6052 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4536 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=1796,i,15701762142637122687,14432371106928829043,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 1408 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
81822.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

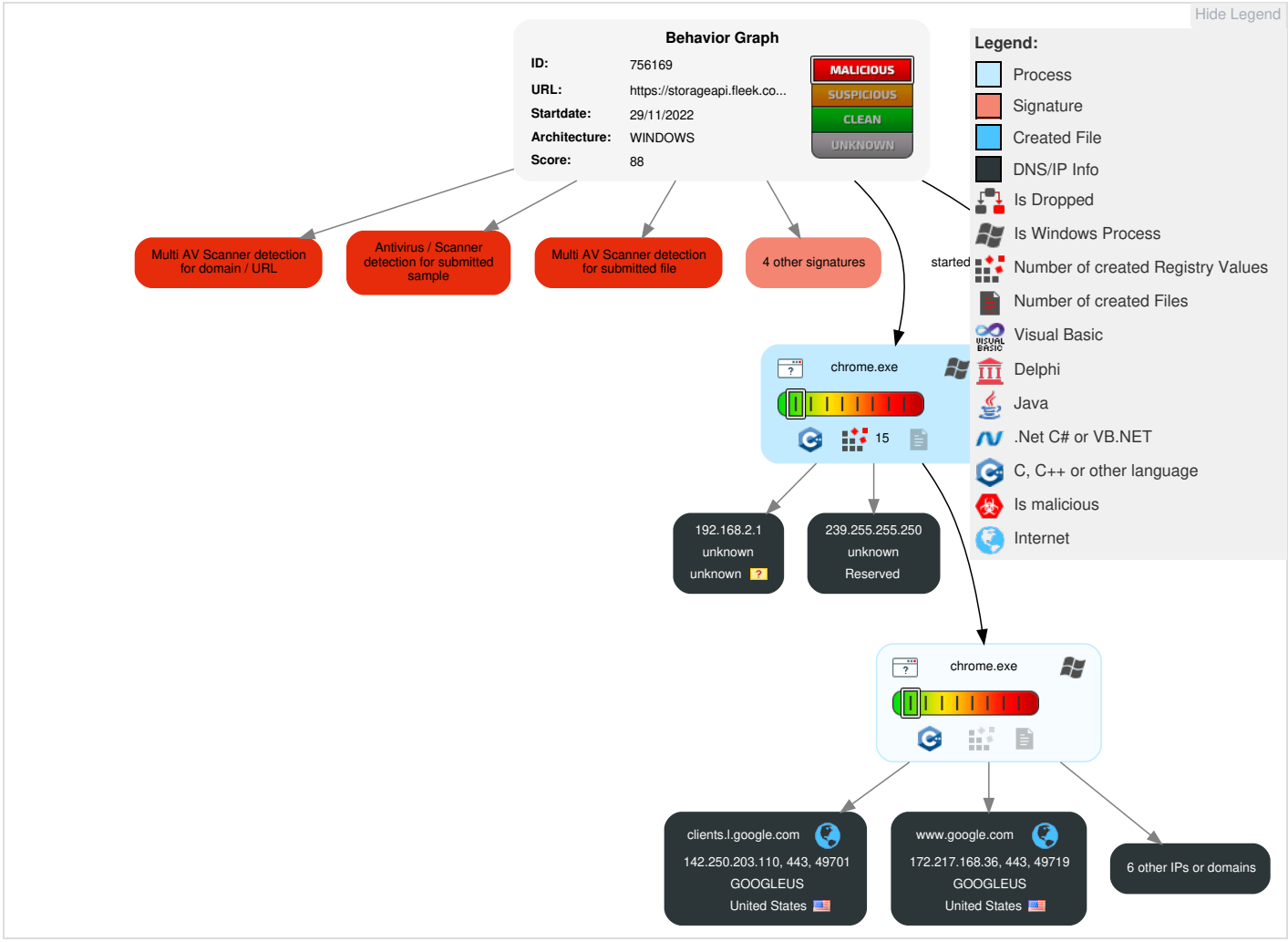
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

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

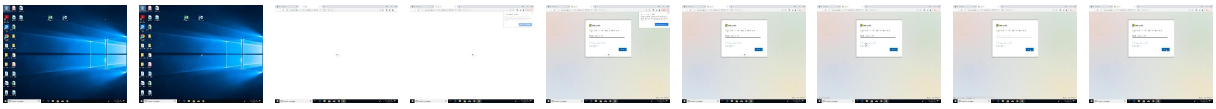
Behavior Graph

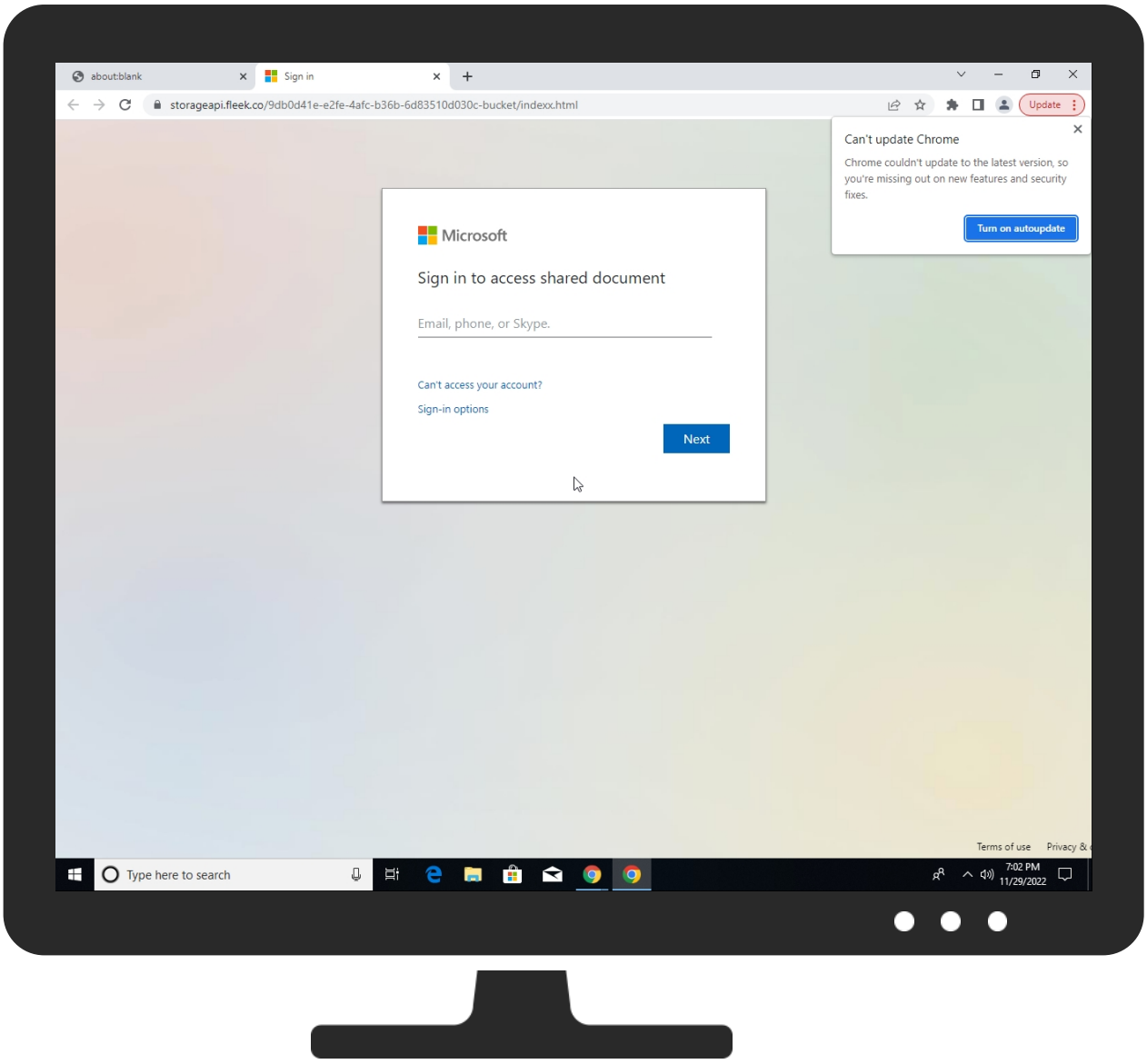


Screenshots

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://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	22%	Virustotal		Browse
http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	100%	Avira URL Cloud	phishing	
http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	22%	Virustotal		Browse

Domains and IPs

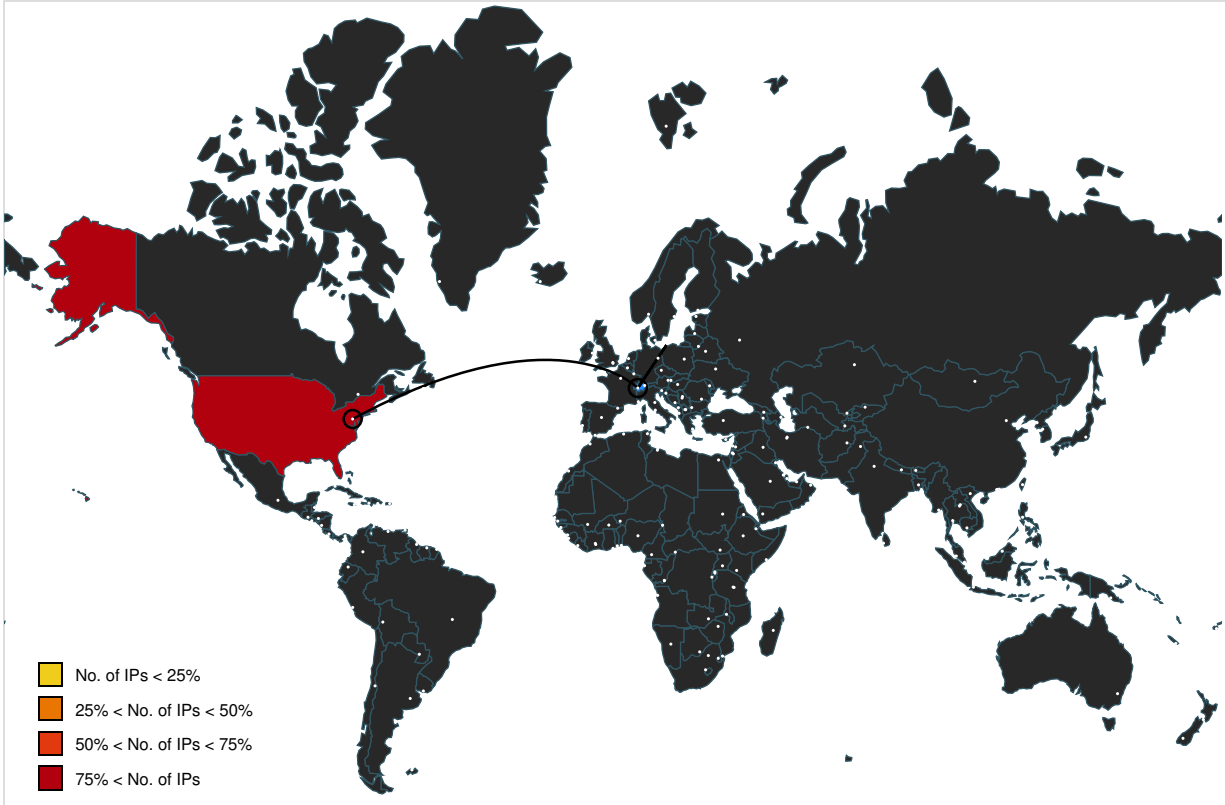
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
storageapi.fleek.co	104.18.6.145	true	false		unknown
www.google.com	172.217.168.36	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js	false		high
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://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	false		high
http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	true	• 22%, Virustotal, Browse	unknown
http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html	true	• 22%, Virustotal, Browse	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.bundle.min.js	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js	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
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.6.145	storageapi.fleek.co	United States		13335	CLOUDFLARENETUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756169
Start date and time:	2022-11-29 19:01:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html
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:	MAL
Classification:	mal88.phis.win@24/0@6/9
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): 172.217.168.67, 34.104.35.123, 142.250.203.106, 172.217.168.10, 172.217.168.42, 172.217.168.74, 216.58.215.234
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, ajax.googleapis.com, clientservices.googleapis.com, firebasestorage.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

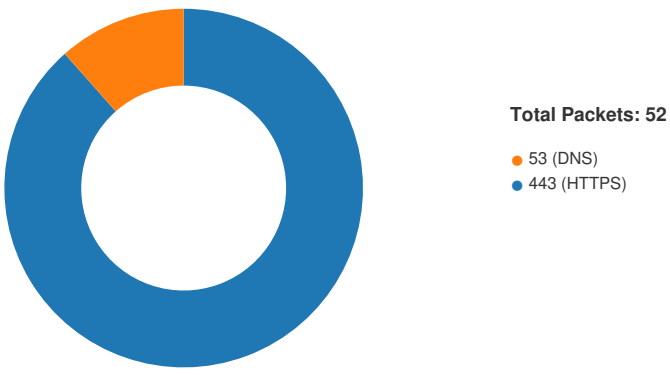
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:02:13.055984020 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.056051970 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:13.056153059 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.057007074 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.057068110 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:13.057486057 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.057537079 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.057624102 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.057898998 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:13.057986021 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:13.058100939 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:13.058134079 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.058151007 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.058423996 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:13.058443069 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:13.210355043 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:13.229434013 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:13.229537010 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.251533985 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.269536018 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:13.273617029 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.273654938 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.273929119 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:13.273963928 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:13.275038958 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.275084019 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:13.275188923 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.275288105 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.278841019 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:13.278857946 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:13.278948069 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:13.278997898 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:13.279031992 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:13.279231071 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:14.256866932 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:14.256958008 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:14.257230043 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:14.257395983 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:14.257468939 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.257479906 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:14.257503033 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:14.257777929 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.257927895 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:14.258018017 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.258254051 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:14.258291006 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.258356094 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:14.258357048 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.258397102 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.295433044 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.295677900 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:14.295722961 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.295754910 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.296655893 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:14.312655926 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.312781096 CET	49702	443	192.168.2.3	172.217.168.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:02:14.312824011 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.312971115 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.313086987 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:14.326235056 CET	49702	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:02:14.326297045 CET	443	49702	172.217.168.45	192.168.2.3
Nov 29, 2022 19:02:14.326786041 CET	49701	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:02:14.326827049 CET	443	49701	142.250.203.110	192.168.2.3
Nov 29, 2022 19:02:14.466936111 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:14.467220068 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.291342020 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291465044 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291549921 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291620016 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.291634083 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291663885 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291743994 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.291779041 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291838884 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.291841984 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291865110 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.291920900 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.292025089 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.292160034 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.292296886 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.292320967 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.292411089 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.292464972 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.292479992 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.293112040 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.293198109 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.293215036 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.293456078 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.293526888 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.339637041 CET	49700	443	192.168.2.3	104.18.6.145
Nov 29, 2022 19:02:15.339683056 CET	443	49700	104.18.6.145	192.168.2.3
Nov 29, 2022 19:02:15.380485058 CET	49711	443	192.168.2.3	104.18.10.207
Nov 29, 2022 19:02:15.380542040 CET	443	49711	104.18.10.207	192.168.2.3
Nov 29, 2022 19:02:15.380626917 CET	49711	443	192.168.2.3	104.18.10.207
Nov 29, 2022 19:02:15.380836964 CET	49712	443	192.168.2.3	104.18.10.207
Nov 29, 2022 19:02:15.380894899 CET	443	49712	104.18.10.207	192.168.2.3
Nov 29, 2022 19:02:15.380970001 CET	49712	443	192.168.2.3	104.18.10.207
Nov 29, 2022 19:02:15.381182909 CET	49713	443	192.168.2.3	104.18.10.207
Nov 29, 2022 19:02:15.381273031 CET	443	49713	104.18.10.207	192.168.2.3
Nov 29, 2022 19:02:15.381360054 CET	49713	443	192.168.2.3	104.18.10.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:02:12.946363926 CET	56924	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:02:12.946650982 CET	60625	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:02:12.965759039 CET	53	56924	8.8.8.8	192.168.2.3
Nov 29, 2022 19:02:12.971020937 CET	49302	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:02:12.973987103 CET	53	60625	8.8.8.8	192.168.2.3
Nov 29, 2022 19:02:12.994007111 CET	53	49302	8.8.8.8	192.168.2.3
Nov 29, 2022 19:02:15.356497049 CET	57134	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:02:15.356712103 CET	56042	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:02:15.379307032 CET	53	57134	8.8.8.8	192.168.2.3
Nov 29, 2022 19:02:15.380393982 CET	53	56042	8.8.8.8	192.168.2.3
Nov 29, 2022 19:02:16.164645910 CET	59636	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:02:16.182365894 CET	53	59636	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
Nov 29, 2022 19:02:12.946363926 CET	192.168.2.3	8.8.8.8	0x7d09	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:12.946650982 CET	192.168.2.3	8.8.8.8	0xc00a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:12.971020937 CET	192.168.2.3	8.8.8.8	0xe153	Standard query (0)	storageapi.fleek.co	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.356497049 CET	192.168.2.3	8.8.8.8	0xe6c5	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.356712103 CET	192.168.2.3	8.8.8.8	0xd42a	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:16.164645910 CET	192.168.2.3	8.8.8.8	0xfb2e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

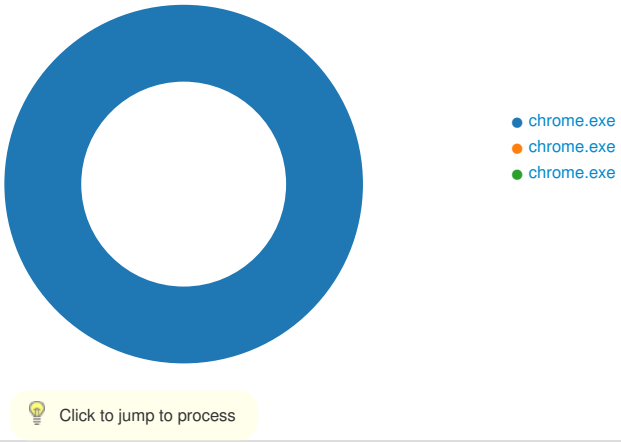
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 19:02:12.965759039 CET	8.8.8.8	192.168.2.3	0x7d09	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:12.973987103 CET	8.8.8.8	192.168.2.3	0xc00a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:02:12.973987103 CET	8.8.8.8	192.168.2.3	0xc00a	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:12.994007111 CET	8.8.8.8	192.168.2.3	0xe153	No error (0)	storageapi.fleek.co		104.18.6.145	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:12.994007111 CET	8.8.8.8	192.168.2.3	0xe153	No error (0)	storageapi.fleek.co		104.18.7.145	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.379307032 CET	8.8.8.8	192.168.2.3	0xe6c5	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.379307032 CET	8.8.8.8	192.168.2.3	0xe6c5	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.380393982 CET	8.8.8.8	192.168.2.3	0xd42a	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:15.380393982 CET	8.8.8.8	192.168.2.3	0xd42a	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:02:16.182365894 CET	8.8.8.8	192.168.2.3	0xfb2e	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- storageapi.fleek.co
- accounts.google.com
- clients2.google.com
- https:
  - stackpath.bootstrapcdn.com
  - cdnjs.cloudflare.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6052**, Parent PID: **3424**

General

Target ID:	0
Start time:	19:02:09
Start date:	29/11/2022
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	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: **4536**, Parent PID: **6052**

General

Target ID:	1
Start time:	19:02:10
Start date:	29/11/2022

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=1932 --field-trial-handle=1796,i,15701762142637122687,14432371106928829043,131072 --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: **1408**, Parent PID: **3424**

General

Target ID:	2
Start time:	19:02:11
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://storageapi.fleek.co/9db0d41e-e2fe-4afc-b36b-6d83510d030c-bucket/indexx.html
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