ID: 1296925
Cookbook: browseurl.jbs
Time: 19:54:42
Date: 24/08/2023
Version: 38.0.0 Beryl

Table of Contents

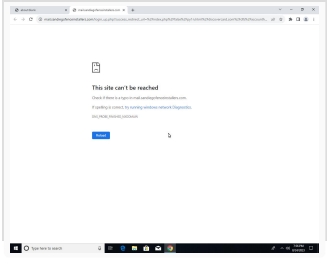
Windows Analysis Report

https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse..

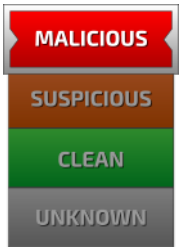
Overview

General Information

Sample URL:	https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=...m%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Fu
Analysis ID:	1296925
Infos:	



Detection

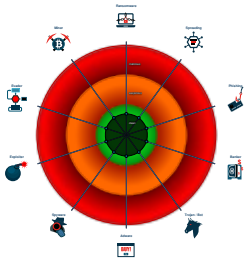


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Stores files to the Windows start me…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5164 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 8D1C4713ACB7CC2AAAEE4477C58A80BA)
  - chrome.exe (PID: 5472 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=2812 --field-trial-handle=2588,i,4458651840048700992,7296907126945281215,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 8D1C4713ACB7CC2AAAEE4477C58A80BA)
- chrome.exe (PID: 5936 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse%2Fpy1n.html%2Fdiscovercard.com%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Funfcu2.org%2Flogin1 MD5: 8D1C4713ACB7CC2AAAEE4477C58A80BA)
- **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

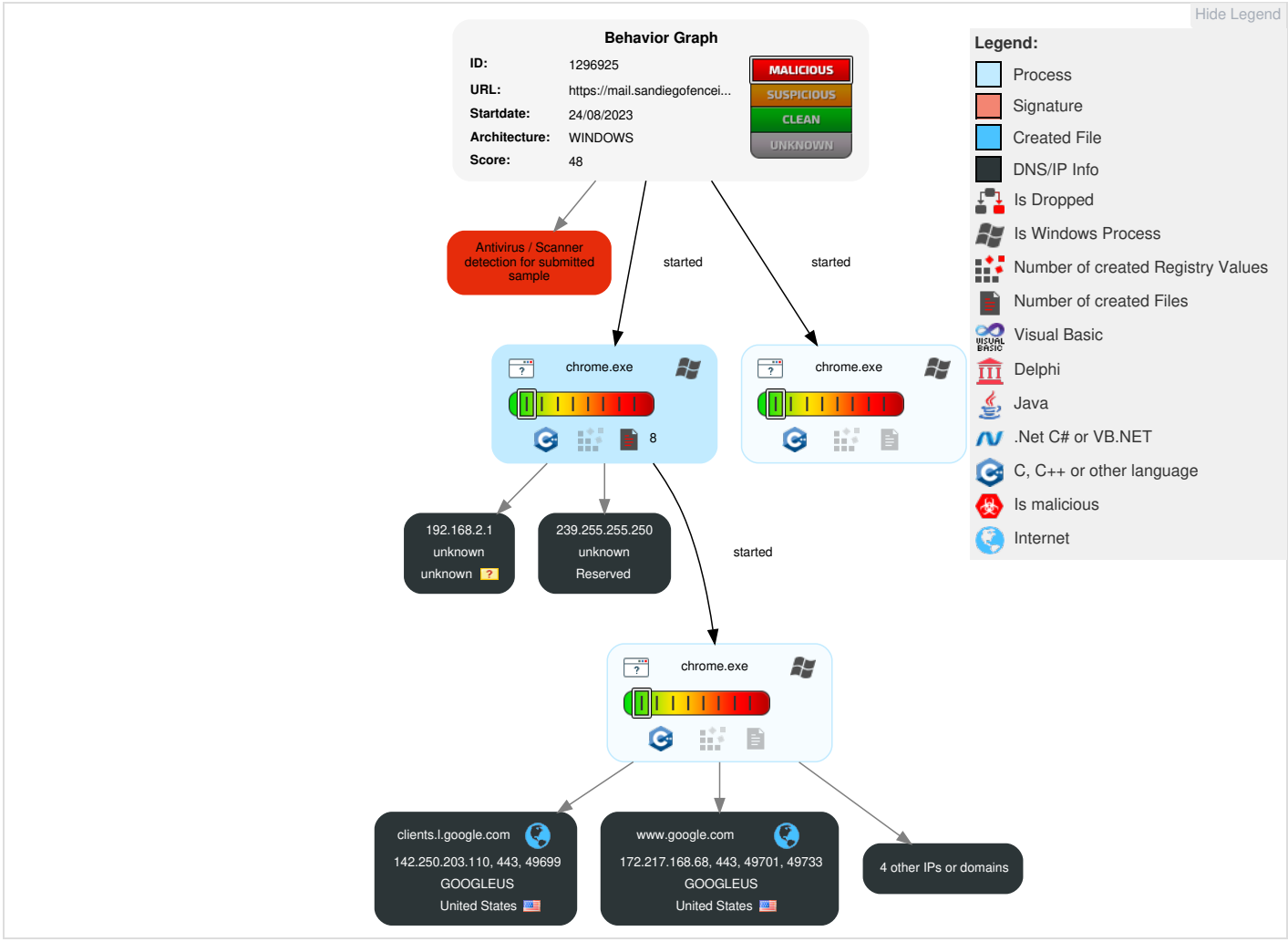
AV Detection

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	1 Registry Run Keys / Startup Folder	1 Process Injection	1 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	1 Registry Run Keys / Startup Folder	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

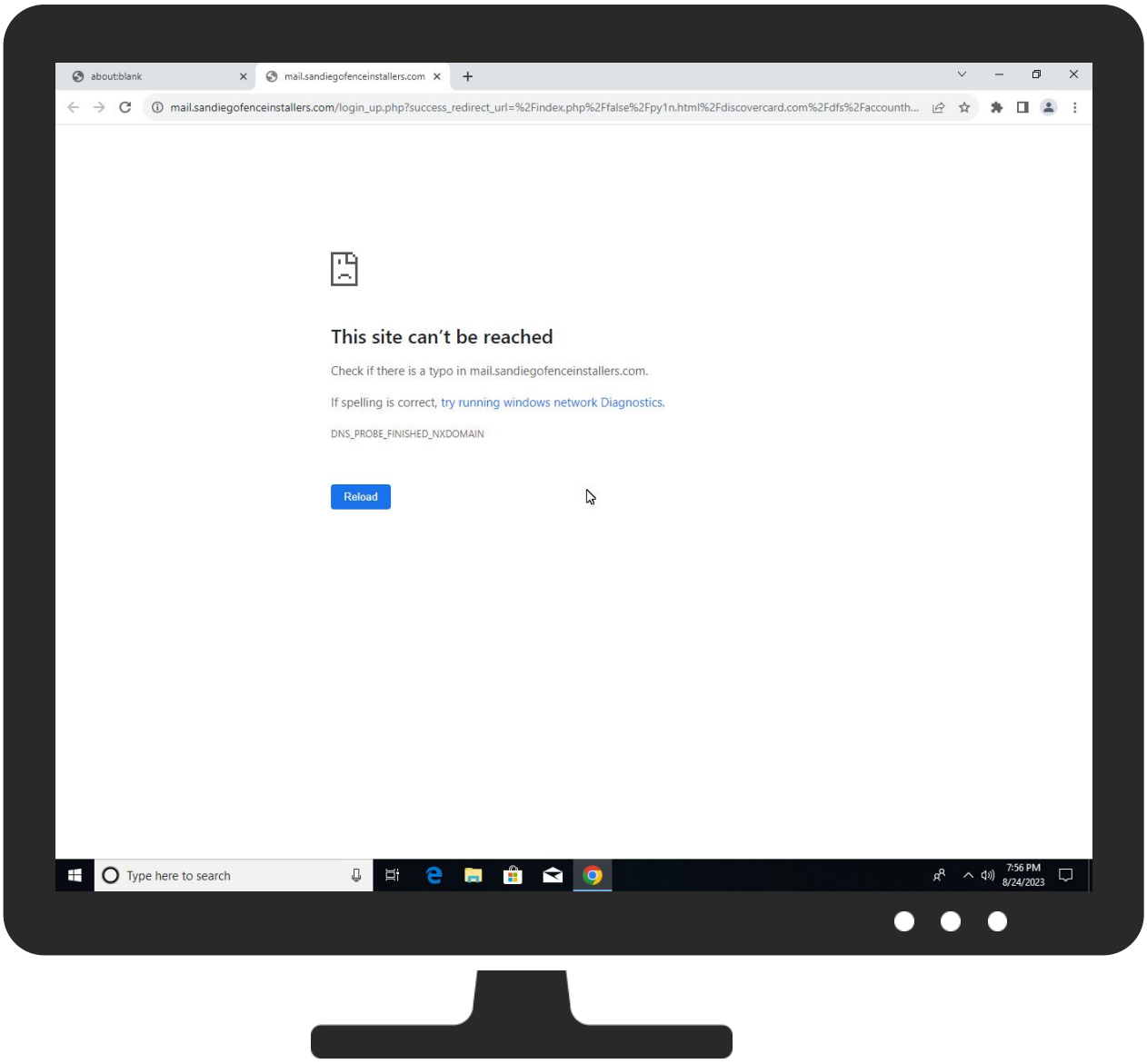
Behavior Graph



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://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse%2Fpy1n.html%2Fdiscovercard.com%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Funfcu2.org%2Flogin1	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

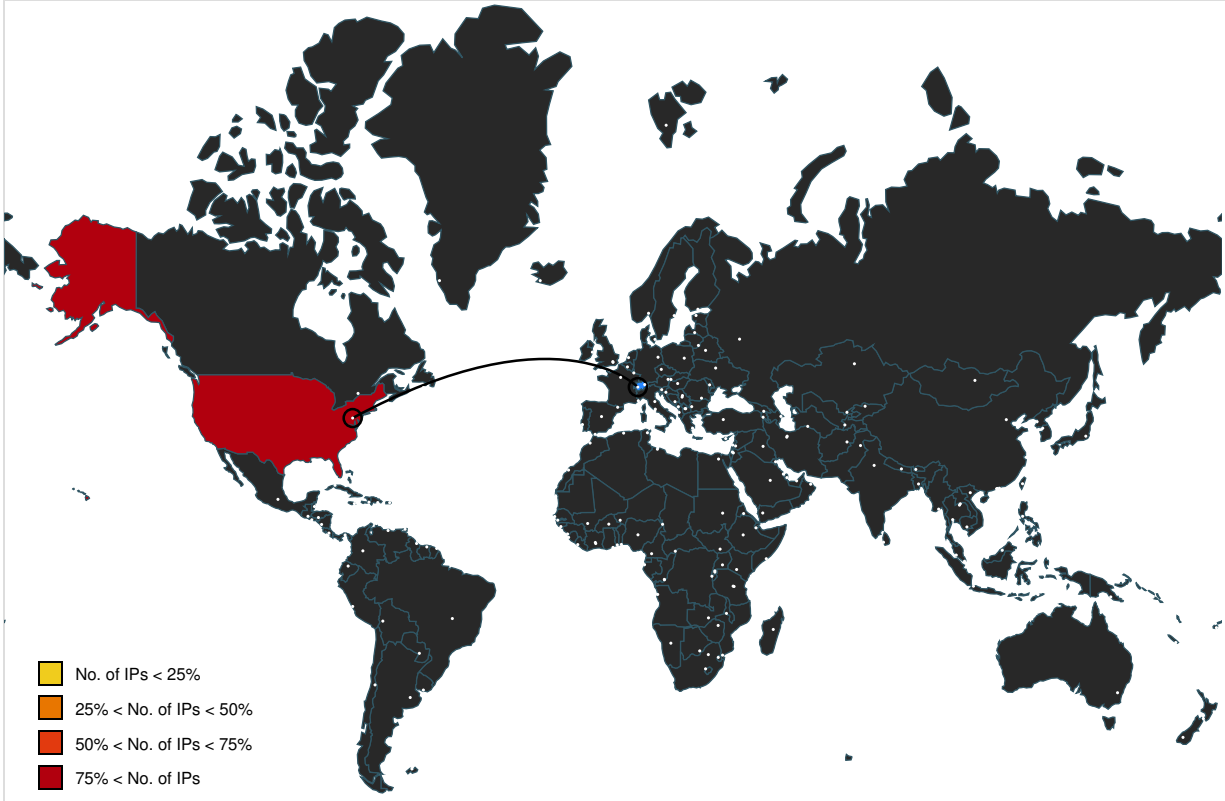
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	142.250.203.110	true	false		high
accounts.google.com	172.217.168.77	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
mail.sandiegofenceinstallers.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=115.0.5790.171&lang=en-GB&acceptformat=crx3,puff&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.77	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1296925
Start date and time:	2023-08-24 19:54:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse%2Fpy1n.html%2Fdiscovercard.com%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Funfcu2.org%2Flogin1
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:	18
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@26/6@23/5
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): dllhost.exe, BackgroundTransferHost.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, geover.prod.do.dsp.mp.microsoft.com, fs.microsoft.com, geo.prod.do.dsp.mp.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, eudb.ris.api.iris.microsoft.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, crl3.digicert.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse%2Fpy1n.html%2Fdiscovercard.com%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Funfcu2.org%2Flogin1

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Docs.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2675
Entropy (8bit):	4.007260914312631
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA1o9ehwiZUklqehDBA3:8JTXRu0
MD5:	F89E794712FBC3FDB2662D011BFB1499
SHA1:	77E64DADCAEF4F698D436BC5231A9CBDF62DFEF0
SHA-256:	1330865DEC91D4FCA1A30D227583D0955323F462FA93BB988726038A48044723
SHA-512:	31DDFF63D71735695C55A0D193F576E0D91EA4E74B95C8BFEEACB18C96F9A3DA57A6BFBD09329F1FF241E0622C8352183813B6A3BA235EC25247449075DF71C3
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....,V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h.r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Gmail.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2677
Entropy (8bit):	4.024747132109703
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA1t9eh/iZUkAQkqehEBA2:8JTXRK9QN
MD5:	1AEA5612DEECC3F2561447B4B4F6ECF4
SHA1:	28899BF346DF9DFF657C9B64AD88624EC451F001
SHA-256:	C7755D40925E73C034CE662E4B71D3812E5EFD4E2ECBF0A9CA8F7C2460BB94F4
SHA-512:	D968C2F5249C370D078EEB579A89FFF142587003BB2014D7885110BF844EF8FF2FEDDD828AF58F68B8EC69FAA681D82455D03C9661E1D0425D85CEFC959FD87
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....,V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h.r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Google Drive.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2691
Entropy (8bit):	4.037217293964395
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA14J9eh7sFiZUkmgqeh7suBABX:8JTXRUnA
MD5:	AEEFACADB40D10043C10F990652E5C0F
SHA1:	EB355FD9CDE1880C44357B0B1C832A336C454D62
SHA-256:	D022CC03E7DC073FF148E03D2285CEA0518B4E4E37D4C812900887B6F08957D7
SHA-512:	297FCED5E614EEB7E5F17912639FD7306AD8DA5FB2F181E62873435E5DC2B1A034FB4E1E2D965A2D9B8B71EB885488E3DEE54C3422F6A5542B77A3386FD4A84 3
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l. e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h. r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e. _.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l. e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Sheets.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2679
Entropy (8bit):	4.022570982288567
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA1u9ehDiZUkwqehIBAR:8JTXRX2
MD5:	BECA0F68E829779199F82EBC1EB8B76B
SHA1:	8DB55DBFC03D51054C974F44FD166A3BD057C2B9
SHA-256:	D42902BA680DFD2F1ABB3C1DC48A1B555E481B4CE77CF0EC6A7EDB810BADCAF9
SHA-512:	15B977A7E8C902FE701B0863B71EF1A181C8D3568375E27A48072180C14DB2EE76B8807B3FD9A66E522A02F5A4A7222651B27EACD94E7114B63AE9E192FD69E1
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l. e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h. r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e. _.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l. e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Slides.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2679
Entropy (8bit):	4.010808466195076
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA1c9ehBiZUk1W1qehqBAC:8JTXR39K
MD5:	B9F2936701C4933B0D379B29E9A7E7D5
SHA1:	F018781D48E844E4E6EC52E2BDA53A133288FB61
SHA-256:	45A2A1F5A802A59A6FF69C14EBAA7E4EBD6E83112BDBCE6C404911F7ACDCCC08
SHA-512:	99787F16D8FA761A29DA5FB5DFECD3107598D9275EA240C19F28AF269D53ABA821839D2ACB0713EFB5E9FD312090EAB28A5E9771BA0D0E11004F58ED8E97CF 1
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l. e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h. r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e. _.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l. e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\YouTube.lnk

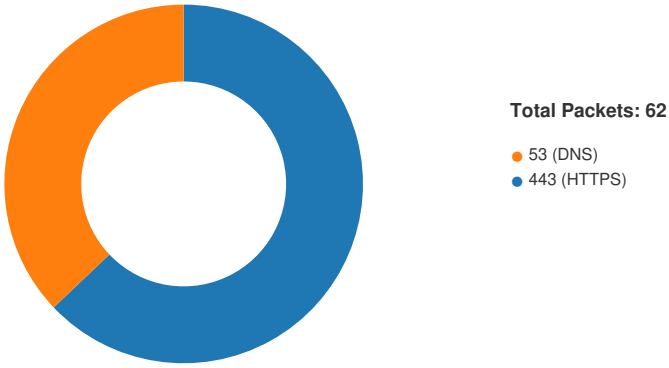
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Sep 30 06:28:28 2020, mtime=Thu Aug 10 09:45:23 2023, atime=Tue Aug 1 18:57:01 2023, length=1158936, window=hide
Category:	dropped
Size (bytes):	2681
Entropy (8bit):	4.025997287023558
Encrypted:	false
SSDEEP:	48:8JTcd9bORmH2idAKZdA1duTn9ehOuTbbiZUk5OjqehOuTbABAyT+:8JTXRgTqTbxWOvTbAPT
MD5:	7FC955EAC109DD3BF2C641B74C239AFE
SHA1:	124014CCCF0EF4CA41FA478BE83C64E37FC0F7AF
SHA-256:	C3BBE95275CA812F029F850BDD4A701DE40C68F48511B85F96FDDA34E408A4C4
SHA-512:	09544D5B1F8AD730C9ABFB78033A5B8F6FE2C34D7FE2766B04D789D53D2E88CBBBE7D2BDAA58EF2341A7FC5719073CA61D5D0D7621593CE453A36827B2F677C6
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....b.J.....w.....,V.....1....P.O. .:i.....+00.../C:\.....1.....W.U..PROGRA~1..t.....L..W.....E.....J.....P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....>Q.;..Google..>.....>Q.;.W.....G.o.o.g.l.e.....T.1.....W.U..Chrome..>.....>Q.;.W.....c.>.C.h.r.o.m.e.....`.1.....W.U..APPLIC~1..H.....>Q.;.W.....A.A.p.p.l.i.c.a.t.i.o.n.....n.2.....W!. .CHROME~1.EXE..R.....>Q.;.W.U.....}.....h.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....}\.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.F

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 24, 2023 19:55:43.272048950 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.272094965 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.272238970 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.278661013 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.278709888 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.285154104 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.285213947 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.285300970 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.300944090 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.300986052 CEST	443	49699	142.250.203.110	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 24, 2023 19:55:43.374636889 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.379035950 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.396414042 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.396464109 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.396583080 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.396615028 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.397726059 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.397916079 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.400037050 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.400279999 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.400470972 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.400587082 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.411048889 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.411361933 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.414484978 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.414525986 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.414845943 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.415066004 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.415436029 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.415473938 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.449373960 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.449471951 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.449506998 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.449600935 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.449682951 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.463841915 CEST	49699	443	192.168.2.4	142.250.203.110
Aug 24, 2023 19:55:43.463892937 CEST	443	49699	142.250.203.110	192.168.2.4
Aug 24, 2023 19:55:43.471487045 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.471667051 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.471702099 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.471740961 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:43.471811056 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.480424881 CEST	49698	443	192.168.2.4	172.217.168.77
Aug 24, 2023 19:55:43.480458021 CEST	443	49698	172.217.168.77	192.168.2.4
Aug 24, 2023 19:55:45.776206017 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.776258945 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.776357889 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.776896954 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.776932955 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.832093000 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.834053040 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.834115028 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.835616112 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.835745096 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.839303970 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.839565992 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:45.979052067 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:45.979095936 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:46.082629919 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:55.813098907 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:55.813198090 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:55:55.813333035 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:58.430896044 CEST	49701	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:55:58.430934906 CEST	443	49701	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:45.873914957 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:45.873964071 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:45.874064922 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:45.874588013 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:45.874610901 CEST	443	49733	172.217.168.68	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 24, 2023 19:56:48.494669914 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:48.495296001 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:48.495340109 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:48.496139050 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:48.496824980 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:48.496987104 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:48.540262938 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:56:58.552169085 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:58.552306890 CEST	443	49733	172.217.168.68	192.168.2.4
Aug 24, 2023 19:56:58.552408934 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:57:00.646816015 CEST	49733	443	192.168.2.4	172.217.168.68
Aug 24, 2023 19:57:00.646857977 CEST	443	49733	172.217.168.68	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 24, 2023 19:55:43.165520906 CEST	63315	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.165896893 CEST	62265	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.166512966 CEST	60838	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.167280912 CEST	53819	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.190660954 CEST	53	60838	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.202553988 CEST	53	63315	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.205363035 CEST	53	53819	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.211195946 CEST	53	62265	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.214791059 CEST	53	51816	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.761799097 CEST	49785	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.762279987 CEST	63872	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:43.903652906 CEST	53	49817	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:43.968375921 CEST	53	49785	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:44.106445074 CEST	62550	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:44.292721987 CEST	53	62550	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:45.716069937 CEST	64803	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:45.718527079 CEST	54388	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:45.728313923 CEST	64522	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:45.728740931 CEST	53653	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:45.736471891 CEST	53	64803	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:45.748250008 CEST	53	54388	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:45.752182961 CEST	53	53653	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:45.770896912 CEST	53	64522	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:46.725970984 CEST	52086	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:46.726480961 CEST	64196	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:46.959121943 CEST	53	52086	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:47.011681080 CEST	55398	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:47.040098906 CEST	53	55398	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:48.790116072 CEST	53	63872	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:51.741915941 CEST	53	64196	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:52.126959085 CEST	61330	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:52.127614975 CEST	60926	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:52.320254087 CEST	53	61330	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:52.363343954 CEST	49247	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:55:52.391532898 CEST	53	49247	8.8.8.8	192.168.2.4
Aug 24, 2023 19:55:57.154635906 CEST	53	60926	8.8.8.8	192.168.2.4
Aug 24, 2023 19:56:22.445149899 CEST	63494	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:56:22.445710897 CEST	57902	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:56:23.467422009 CEST	61038	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:56:23.468245029 CEST	61960	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:56:23.765650988 CEST	53	61038	8.8.8.8	192.168.2.4
Aug 24, 2023 19:56:23.845350981 CEST	53014	53	192.168.2.4	8.8.8.8
Aug 24, 2023 19:56:25.001065969 CEST	53014	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 24, 2023 19:56:25.038093090 CEST	53	53014	8.8.8.8	192.168.2.4
Aug 24, 2023 19:56:57.392524004 CEST	53	62204	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 24, 2023 19:55:43.903860092 CEST	192.168.2.4	8.8.8.8	d02f	(Port unreachable)	Destination Unreachable
Aug 24, 2023 19:55:48.791524887 CEST	192.168.2.4	8.8.8.8	d004	(Port unreachable)	Destination Unreachable
Aug 24, 2023 19:55:51.742080927 CEST	192.168.2.4	8.8.8.8	d004	(Port unreachable)	Destination Unreachable
Aug 24, 2023 19:55:57.154798031 CEST	192.168.2.4	8.8.8.8	d004	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Aug 24, 2023 19:55:43.165520906 CEST	192.168.2.4	8.8.8.8	0xdf3c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:43.165896893 CEST	192.168.2.4	8.8.8.8	0xd10a	Standard query (0)	clients2.google.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:43.166512966 CEST	192.168.2.4	8.8.8.8	0x2005	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:43.167280912 CEST	192.168.2.4	8.8.8.8	0x9edd	Standard query (0)	accounts.google.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:43.761799097 CEST	192.168.2.4	8.8.8.8	0xf970	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:43.762279987 CEST	192.168.2.4	8.8.8.8	0x6567	Standard query (0)	mail.sandiegofenceinstallers.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:44.106445074 CEST	192.168.2.4	8.8.8.8	0x45eb	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.716069937 CEST	192.168.2.4	8.8.8.8	0xe8ba	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.718527079 CEST	192.168.2.4	8.8.8.8	0xd474	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.728313923 CEST	192.168.2.4	8.8.8.8	0x7004	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.728740931 CEST	192.168.2.4	8.8.8.8	0x123b	Standard query (0)	www.google.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:46.725970984 CEST	192.168.2.4	8.8.8.8	0xc910	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:46.726480961 CEST	192.168.2.4	8.8.8.8	0xc8af	Standard query (0)	mail.sandiegofenceinstallers.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:47.011681080 CEST	192.168.2.4	8.8.8.8	0xafd0	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:52.126959085 CEST	192.168.2.4	8.8.8.8	0xb981	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:52.127614975 CEST	192.168.2.4	8.8.8.8	0xe0b1	Standard query (0)	mail.sandiegofenceinstallers.com	65	IN (0x0001)	false
Aug 24, 2023 19:55:52.363343954 CEST	192.168.2.4	8.8.8.8	0xe2	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:56:22.445149899 CEST	192.168.2.4	8.8.8.8	0x238a	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:56:22.445710897 CEST	192.168.2.4	8.8.8.8	0xcf4	Standard query (0)	mail.sandiegofenceinstallers.com	65	IN (0x0001)	false
Aug 24, 2023 19:56:23.467422009 CEST	192.168.2.4	8.8.8.8	0x905	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Aug 24, 2023 19:56:23.468245029 CEST	192.168.2.4	8.8.8.8	0x5508	Standard query (0)	mail.sandiegofenceinstallers.com	65	IN (0x0001)	false
Aug 24, 2023 19:56:23.845350981 CEST	192.168.2.4	8.8.8.8	0xe69e	Standard query (0)	mail.sandiegofenceinstallers.com	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:56:25.001065969 CEST	192.168.2.4	8.8.8.8	0xe69e	Standard query (0)	mail.sandiegofenceinstallers.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
Aug 24, 2023 19:55:43.190660954 CEST	8.8.8.8	192.168.2.4	0x2005	No error (0)	accounts.google.com		172.217.168.77	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:43.202553988 CEST	8.8.8.8	192.168.2.4	0xdf3c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Aug 24, 2023 19:55:43.202553988 CEST	8.8.8.8	192.168.2.4	0xdf3c	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:43.211195946 CEST	8.8.8.8	192.168.2.4	0xd10a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Aug 24, 2023 19:55:45.736471891 CEST	8.8.8.8	192.168.2.4	0xe8ba	No error (0)	google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.748250008 CEST	8.8.8.8	192.168.2.4	0xd474	No error (0)	google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:45.752182961 CEST	8.8.8.8	192.168.2.4	0x123b	No error (0)	www.google.com			65	IN (0x0001)	false
Aug 24, 2023 19:55:45.770896912 CEST	8.8.8.8	192.168.2.4	0x7004	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Aug 24, 2023 19:55:48.790116072 CEST	8.8.8.8	192.168.2.4	0x6567	Server failure (2)	mail.sandiegofenceinstallers.com	none	none	65	IN (0x0001)	false
Aug 24, 2023 19:55:51.741915941 CEST	8.8.8.8	192.168.2.4	0xc8af	Server failure (2)	mail.sandiegofenceinstallers.com	none	none	65	IN (0x0001)	false
Aug 24, 2023 19:55:57.154635906 CEST	8.8.8.8	192.168.2.4	0xe0b1	Server failure (2)	mail.sandiegofenceinstallers.com	none	none	65	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: 5164, Parent PID: 4732

General

Target ID:	1
Start time:	19:55:38
Start date:	24/08/2023
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:	0x7ff7c94b0000
File size:	3'219'224 bytes
MD5 hash:	8D1C4713ACB7CC2AAAEE4477C58A80BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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

Analysis Process: chrome.exe PID: 5472, Parent PID: 5164

General

Target ID:	3
Start time:	19:55:40
Start date:	24/08/2023
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=2812 --field-trial-handle=2588,i,4458651840048700992,7296907126945281215,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c94b0000
File size:	3'219'224 bytes
MD5 hash:	8D1C4713ACB7CC2AAAEE4477C58A80BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 5936, Parent PID: 4732

General	
Target ID:	4
Start time:	19:55:42
Start date:	24/08/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://mail.sandiegofenceinstallers.com/login_up.php?success_redirect_url=%2Findex.php%2Ffalse%2Fpy1n.html%2Fdiscovercard.com%2Fdfs%2Faccounthome%2Fsummary%2F-www.schwab.com%2Fsecure.accurint.com%2Funfcu2.org%2Flogin1
Imagebase:	0x7ff7c94b0000
File size:	3'219'224 bytes
MD5 hash:	8D1C4713ACB7CC2AAAEE4477C58A80BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly