ID: 715090
Sample Name: phish5.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 16:11:41
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

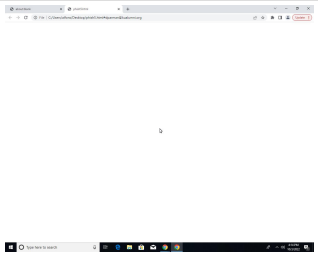
Windows Analysis Report

phish5.html

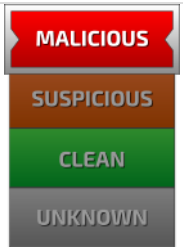
Overview

General Information

Sample Name:	phish5.html
Analysis ID:	715090
MD5:	74de36a50b1610.
SHA1:	713b974c200b71..
SHA256:	dd6727b26d5ba4.
Infos:	



Detection



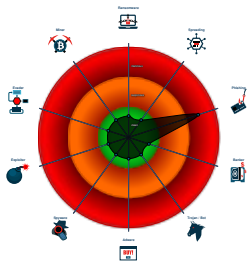
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1092 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6028 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=1856 --field-trial-handle=1872,i,12175141778944238973,2527083511056561703,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6212 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\phish5.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
phish5.html	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x156:$c8: while(!![]) • 0x175:$d1: parseInt(_0x483f24(0x177))/0x1+-parseInt(_0x483f24(0x169))/0x2+parseInt(_0x483f24(0x171))/0x3+-parseInt(_0x483f24(0x175))/0x4+parseInt(_0x483f24(0x163))/0x5+-parseInt(_0x483f24(0x16f))/0x6*(• 0x195:$d1: parseInt(_0x483f24(0x169))/0x2+parseInt(_0x483f24(0x171))/0x3+-parseInt(_0x483f24(0x175))/0x4+parseInt(_0x483f24(0x163))/0x5+-parseInt(_0x483f24(0x16f))/0x6*(parseInt(_0x483f24(0x16a))/0x7)+
phish5.html	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Source	Rule	Description	Author	Strings
phish5.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

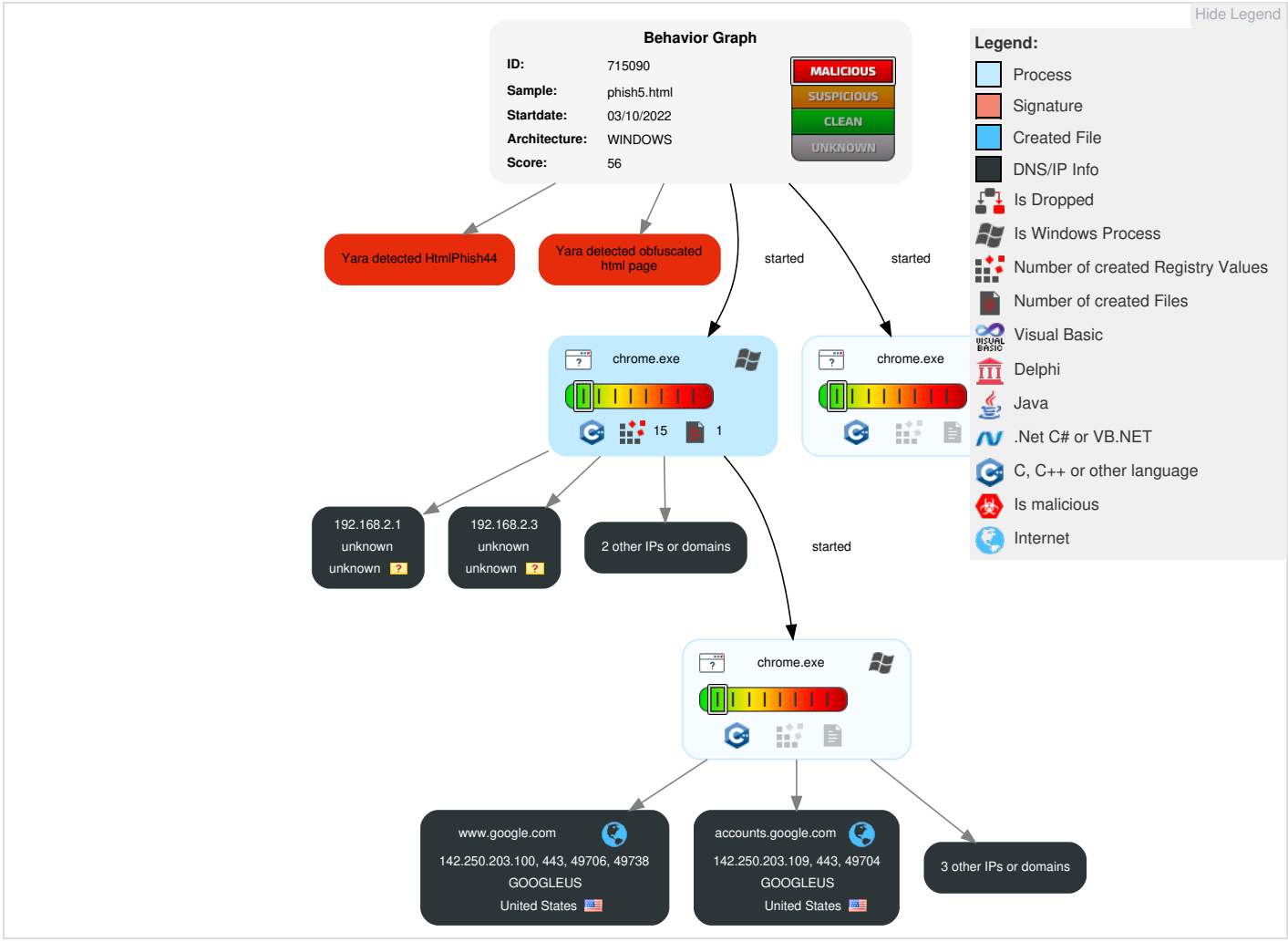
Yara detected HtmlPhish44

Yara detected obfuscated html page

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

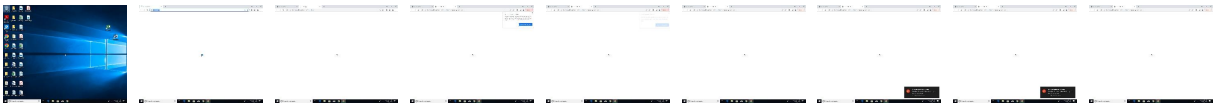
Behavior Graph

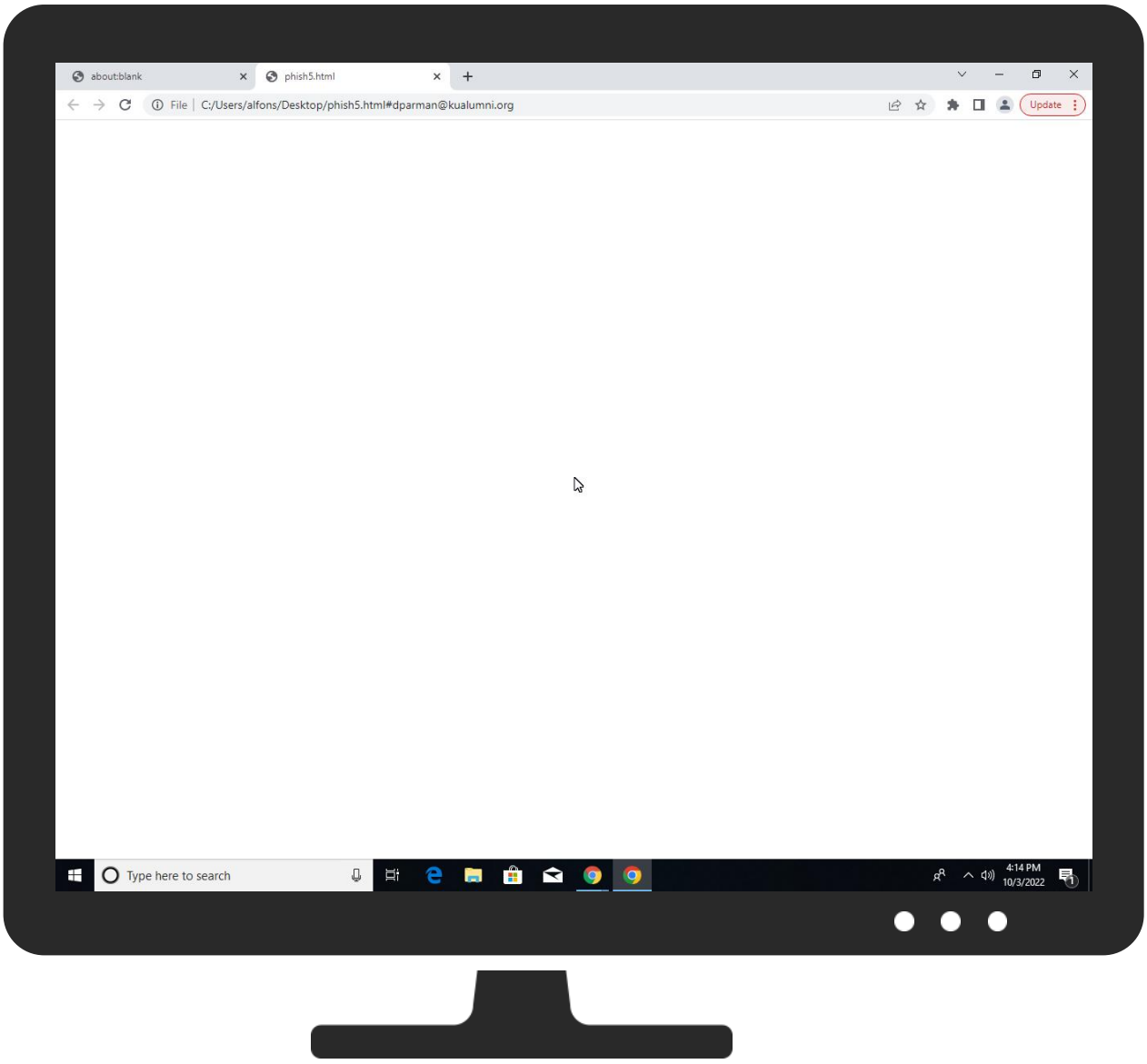


Screenshots

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
phish5.html	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

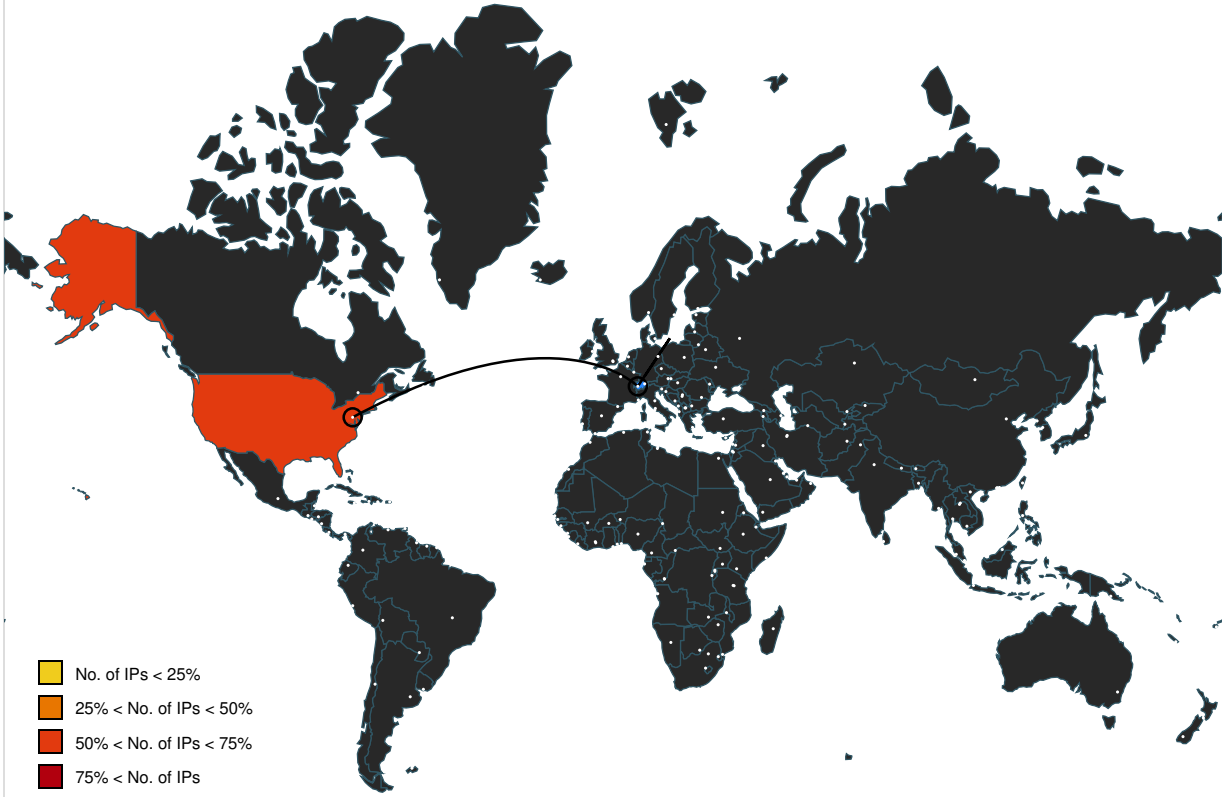
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	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://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1
192.168.2.6

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715090
Start date and time:	2022-10-03 16:11:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	phish5.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	22
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:	mal56.phis.winHTML@28/0@4/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, login.live.com, unitedstand.z13.web.core.windows.net, update.googleapis.com, clientservices.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.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

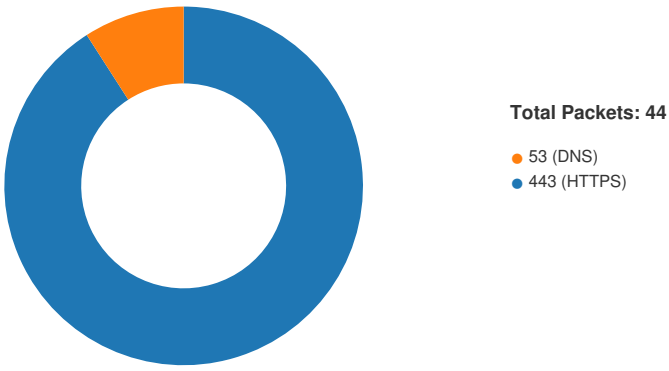
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (4733)
Entropy (8bit):	4.837047507026479
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	phish5.html
File size:	4925
MD5:	74de36a50b1610945743af5960e7f7ca
SHA1:	713b974c200b71a3657334f6079994355594e740
SHA256:	dd6727b26d5ba4a05f7bca42c4e73ba88fa75b709c255e4f8a7d79b99d86f91c
SHA512:	8017ca2fd18c5e7120a3b1e36966cdced4a09d2ff143df8803531d079cd892576eb9aae3c7cbc8017f65f2c99eaaf651e4ed22b0793a28d131b670d436a24714
SSDEEP:	96:/wNPvtA8MwTlN6f9jjOpJSfyQlfzUUm8qYPYzD0gcYnThF70gR6UMp:/wNXtnTlN6fljOpjhqYPYkgcYnThZRMp
TLSH:	A4A1D0C47FA8F11B079E4E5BFA17A9CFE07A59A7A8C822038214F94C29F4509C5EDC31
File Content Preview:	<script language=javascript>function _0x3f84(_0x396e53,_0x4f6a6b){var _0x18e8bd=_0x3b38();return _0x3f84=function(_0x5defaf,_0x1c9ef8){_0x5defaf=_0x5defaf-0x160;var _0x381c3f=_0x18e8bd[_0x5defaf];return _0x381c3f;},_0x3f84(_0x396e53,_0x4f6a6b);}var _0x1fa

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:12:44.243736982 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.243802071 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.243879080 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.245635033 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.245675087 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.247466087 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.247519970 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.247594118 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.248356104 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.248369932 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.314558983 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.315404892 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.315440893 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.321605921 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.322150946 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.322191000 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.323621988 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.323704958 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.323971033 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.324064016 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.325544119 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.325618029 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.629371881 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.629435062 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.629520893 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.630042076 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.630075932 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.688890934 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.689404964 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.689450026 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.690691948 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.690844059 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.717225075 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.717255116 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.717500925 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.717709064 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.717724085 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.719017982 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:44.719048023 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.719162941 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.719329119 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.719358921 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.719548941 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.720216990 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.720237017 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.772097111 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.772353888 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.772357941 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.772407055 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.775171995 CEST	49704	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:12:44.775196075 CEST	443	49704	142.250.203.109	192.168.2.5
Oct 3, 2022 16:12:44.778407097 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.778506041 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.778549910 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.778594017 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.778646946 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.784818888 CEST	49706	443	192.168.2.5	142.250.203.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:12:44.784848928 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:44.788872957 CEST	49703	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:12:44.788914919 CEST	443	49703	142.250.203.110	192.168.2.5
Oct 3, 2022 16:12:44.886545897 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:54.707730055 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:54.707885981 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:12:54.708005905 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:56.901563883 CEST	49706	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:12:56.901619911 CEST	443	49706	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.670897961 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:44.670974970 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.671107054 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:44.671591997 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:44.671636105 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.730684996 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.731359959 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:44.731395960 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.732283115 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.733226061 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:44.733263969 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.733418941 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:44.785068989 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:13:54.747488022 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:54.747586012 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:13:54.747659922 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:14:39.760118008 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:14:39.760179996 CEST	443	49738	142.250.203.100	192.168.2.5
Oct 3, 2022 16:15:24.790247917 CEST	49738	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:15:24.790292978 CEST	443	49738	142.250.203.100	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:12:44.007019997 CEST	49177	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:12:44.009830952 CEST	49724	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:12:44.035144091 CEST	53	49177	8.8.8.8	192.168.2.5
Oct 3, 2022 16:12:44.035681009 CEST	53	49724	8.8.8.8	192.168.2.5
Oct 3, 2022 16:12:44.280880928 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 16:12:44.608181000 CEST	63446	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:12:44.625714064 CEST	53	63446	8.8.8.8	192.168.2.5
Oct 3, 2022 16:13:44.648781061 CEST	49769	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:13:44.668303013 CEST	53	49769	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:12:44.007019997 CEST	192.168.2.5	8.8.8.8	0xc56e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:12:44.009830952 CEST	192.168.2.5	8.8.8.8	0xa9ed	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:12:44.608181000 CEST	192.168.2.5	8.8.8.8	0xe53c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:44.648781061 CEST	192.168.2.5	8.8.8.8	0x1e42	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
Oct 3, 2022 16:12:44.035144091 CEST	8.8.8.8	192.168.2.5	0xc56e	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:12:44.035681009 CEST	8.8.8.8	192.168.2.5	0xa9ed	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:12:44.035681009 CEST	8.8.8.8	192.168.2.5	0xa9ed	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:12:44.625714064 CEST	8.8.8.8	192.168.2.5	0xe53c	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:44.668303013 CEST	8.8.8.8	192.168.2.5	0x1e42	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49704	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:12:44 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:12:44 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-10-03 14:12:44 UTC	1	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 14:12:44 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-23sxJ0elPG1dCqbgBV-FuA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 14:12:44 UTC	2	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]

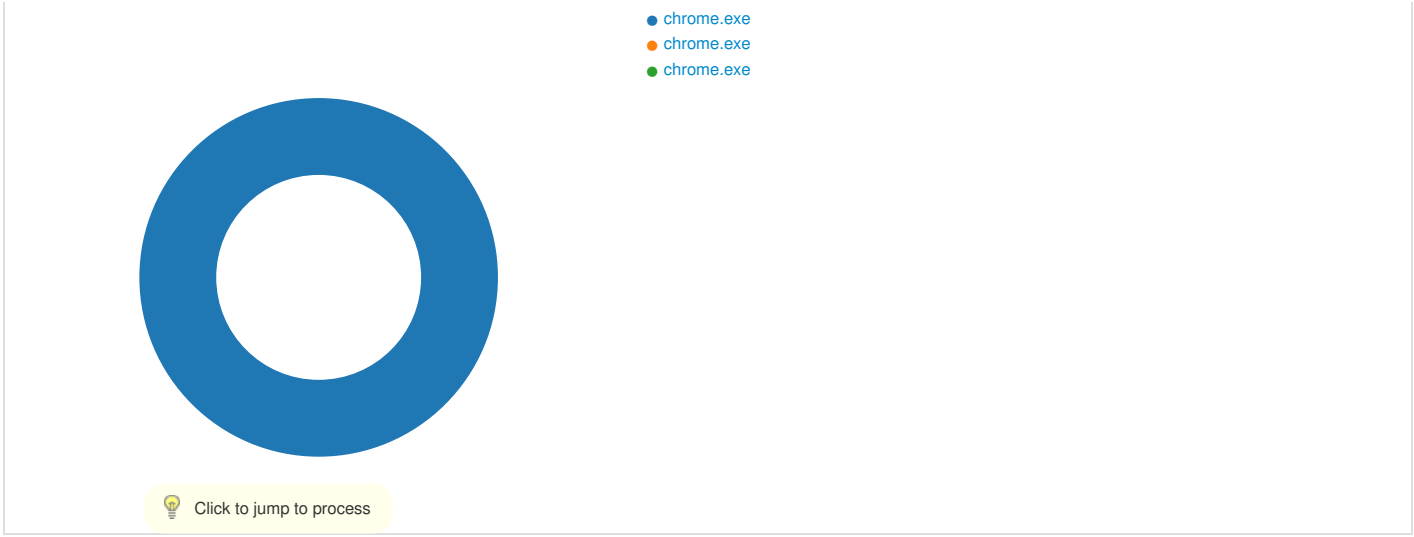
Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:12:44 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49703	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:12:44 UTC	0	OUT	GET /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 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:12:44 UTC	2	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-IZZMqyBYPtXpKig3re2OPw' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 14:12:44 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 25964 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 14:12:44 UTC	3	IN	Data Raw: 32 63 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 35 39 36 34 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="25964"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 14:12:44 UTC	4	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgm ieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a 4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 14:12:44 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 1092, Parent PID: 2860

General

Target ID:	0
Start time:	16:12:38
Start date:	03/10/2022
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:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 6028, Parent PID: 1092

General

Target ID:	1
Start time:	16:12:39
Start date:	03/10/2022
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=1856 --field-trial-handle=1872,i,12175141778944238973,252708351105656170 3,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: **6212**, Parent PID: **2860**

General

Target ID:	2
Start time:	16:12:40
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\phish5.html
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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