ID: 876181
Sample Name: login.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 13:17:50
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

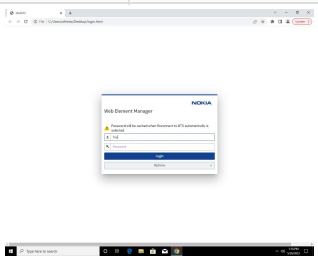
Windows Analysis Report

login.html

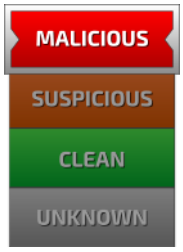
Overview

General Information

Sample Name:	login.html
Analysis ID:	876181
MD5:	daccb43d7df16..
SHA1:	ef1e463b2cff4c..
SHA256:	f0a3bb7564922..
Infos:	



Detection

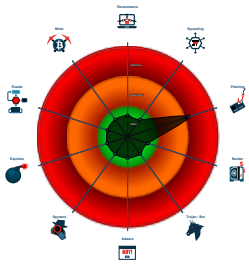


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Suspicious Javascript code found in…
- HTML document with suspicious na…
- HTML body contains password inpu…
- HTML body with high number of larg…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6556 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\login.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 1584 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=2036 --field-trial-handle=1772,i,15227930420298686886,3054010558266752575,131072 --disable-features =OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **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

Phishing

Suspicious Javascript code found in HTML file

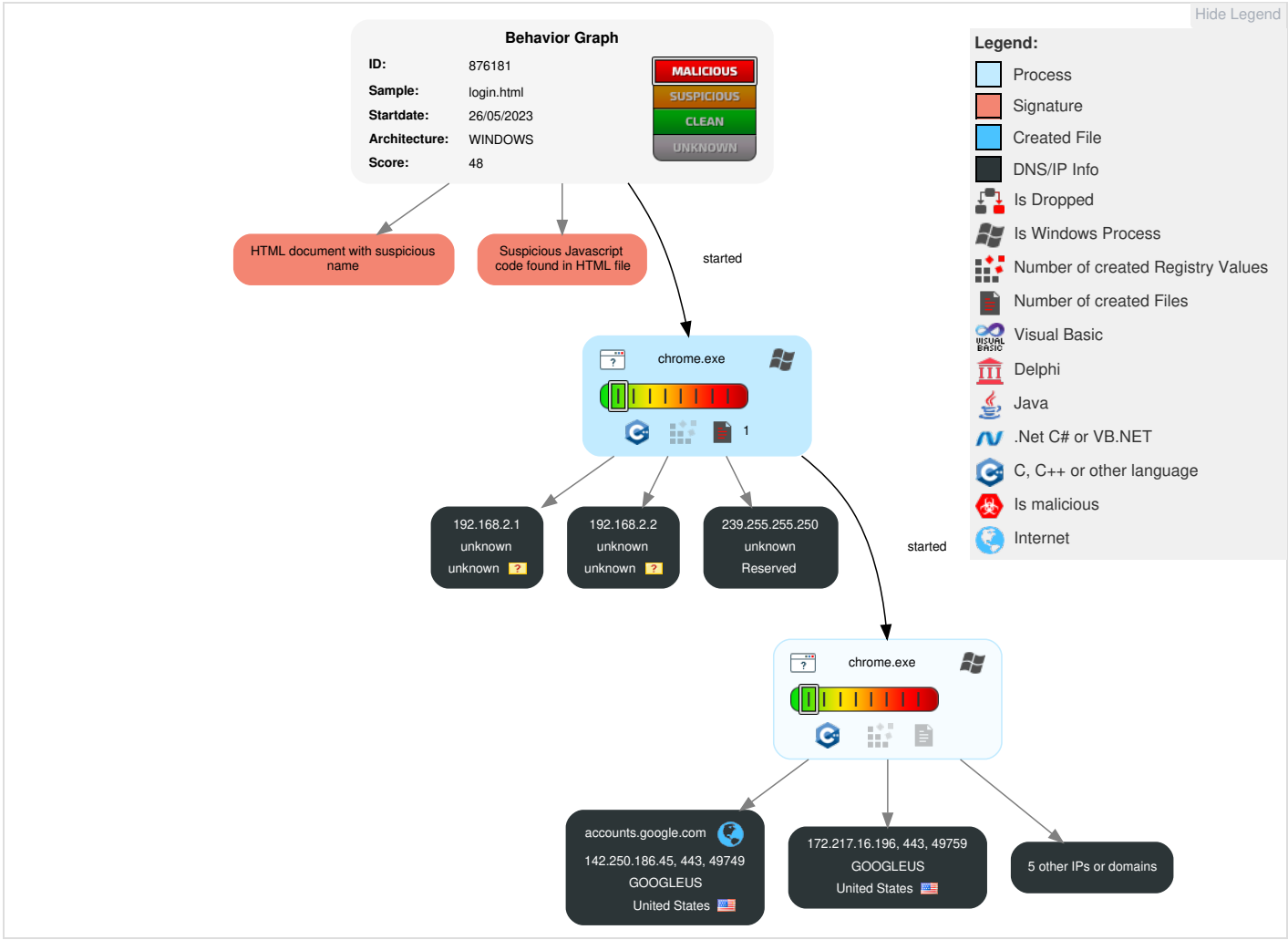
System Summary

HTML document with suspicious name

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	1 Extra Window Memory Injection	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)	1 Extra Window Memory Injection	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

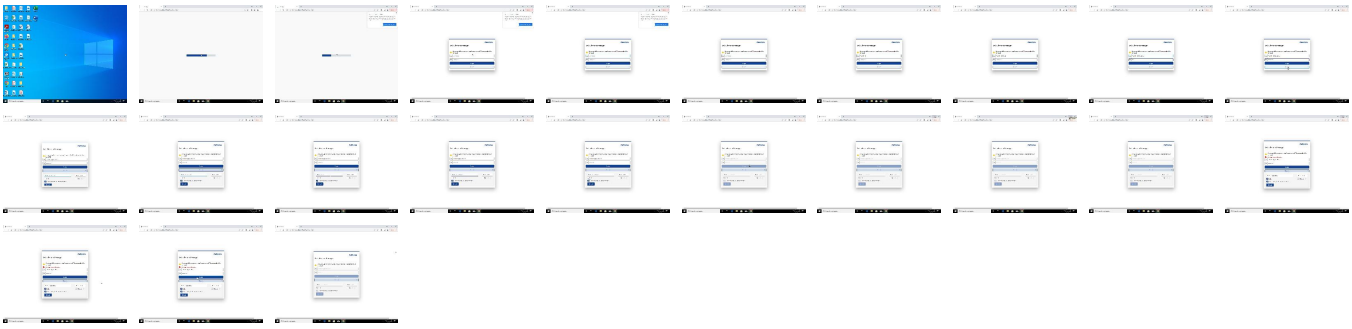
Behavior Graph

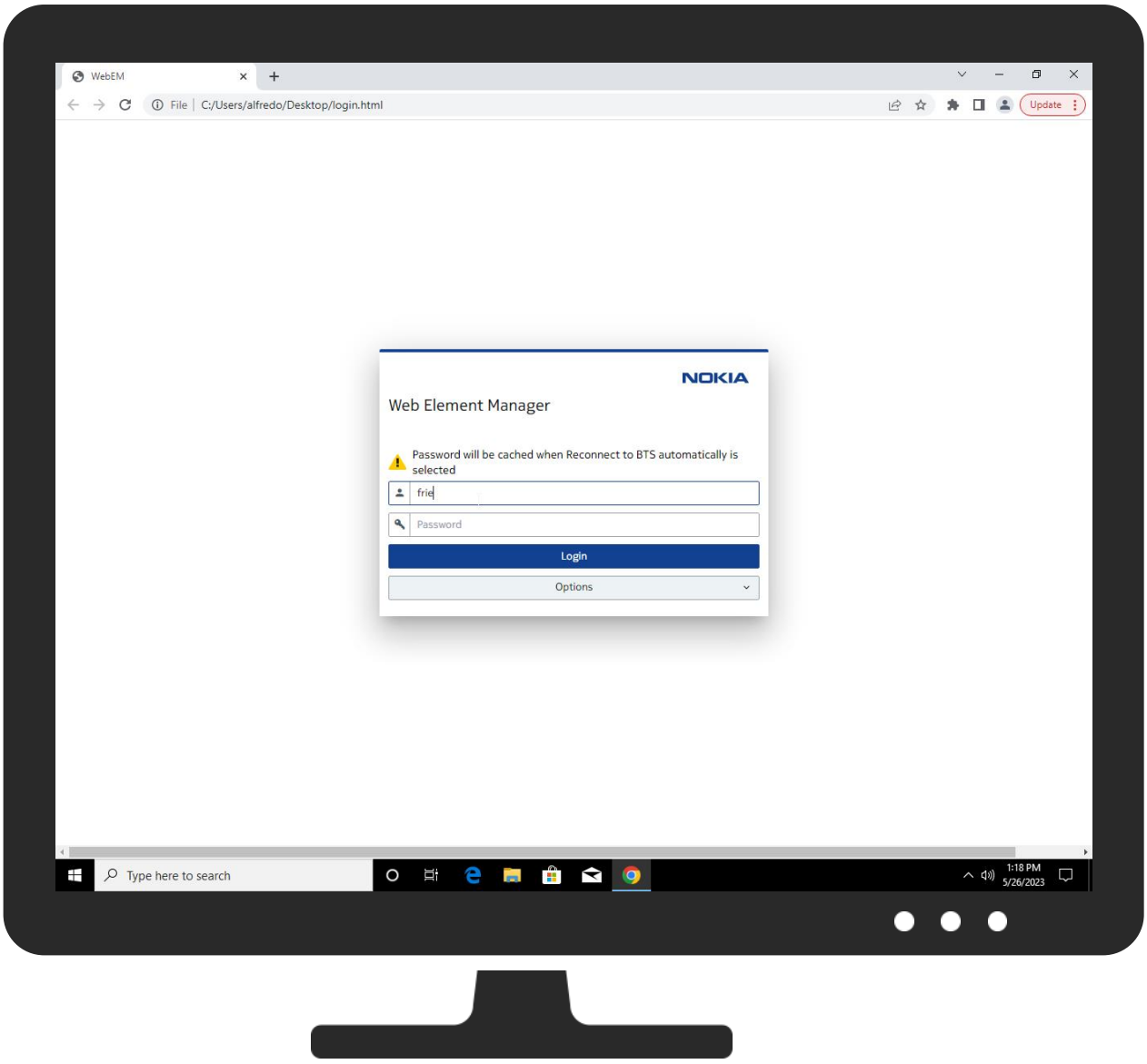


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.broofa.com	0%	URL Reputation	safe	
http://www.broofa.com	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://js.foundation/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.186.45	true	false		high
www.google.com	142.250.184.196	true	false		high
clients.l.google.com	216.58.212.174	true	false		high
clients2.google.com	unknown	unknown	false		high

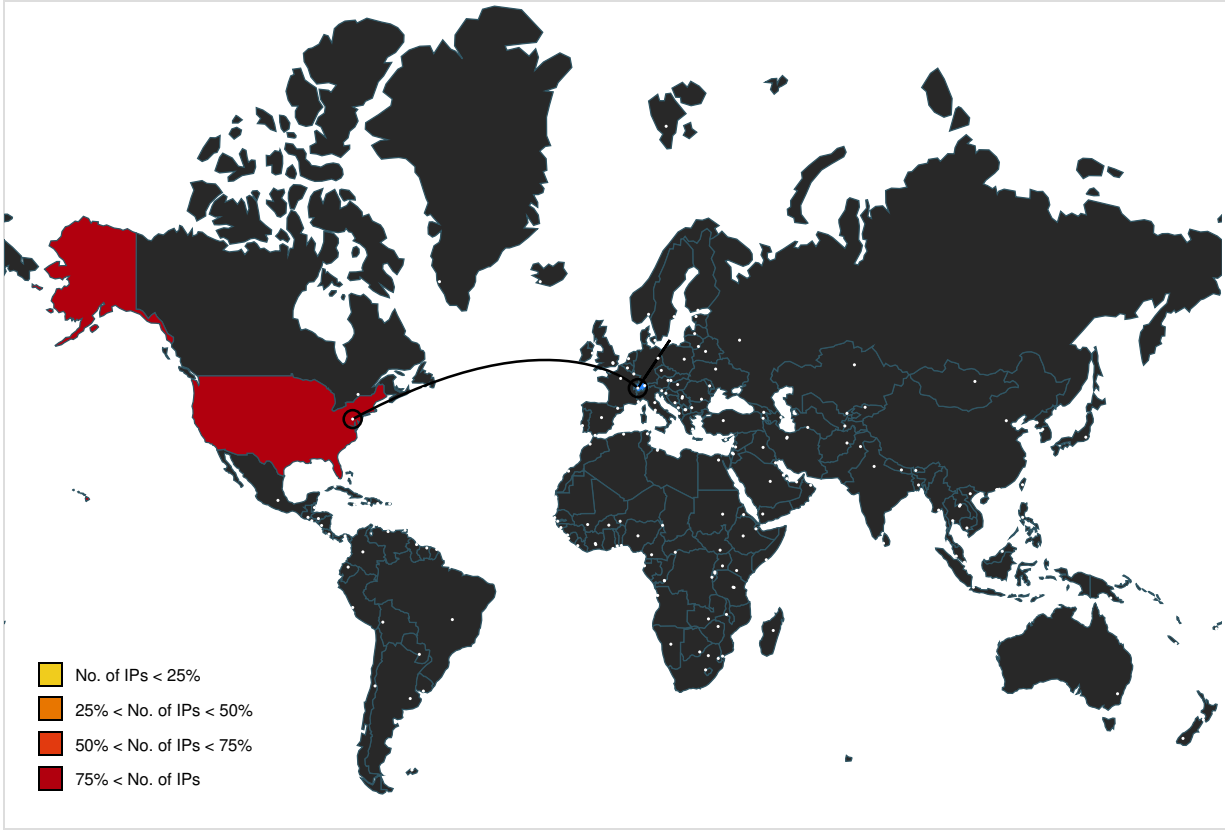
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/login.html	true		low
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	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=104.0.5112.102&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://underscorejs.org/LICENSE	login.html	false		high
http://www.apache.org/licenses/LICENSE-2.0	login.html	false		high
http://https://jquery.org/license	login.html	false		high
http://https://g.co/ng/security#xss)	login.html	false		high
http://www.broofa.com	login.html	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/dcodeIO/long.js	login.html	false		high
http://https://github.com/dcodeIO/protobuf.js	login.html	false		high
http://https://jquery.com/	login.html	false		high
http://https://angular.io/api/core/Component#animations).	login.html	false		high
http://https://angular.io/errors/$	login.html	false		high
http://https://angular.io/	login.html	false		high
http://https://lodash.com/	login.html	false		high
http://https://github.com/dcodeIO/bytebuffer.js	login.html	false		high
http://https://lodash.com/license	login.html	false		high
http://https://angular.io/license	login.html	false		high
http://https://openjsf.org/	login.html	false	• URL Reputation: safe	unknown
http://https://sizzlejs.com/	login.html	false		high
http://https://js.foundation/	login.html	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.212.164	unknown	United States		15169	GOOGLEUS	false
216.58.212.174	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.16.196	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.2
192.168.2.1
192.168.8.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876181
Start date and time:	2023-05-26 13:17:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	5
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
Sample file name:	login.html
Detection:	MAL
Classification:	mal48.phis.winHTML@24/0@6/8
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): HxTsr.exe, RuntimeBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.181.227, 34.104.35.123, 142.250.185.227
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, login.live.com, update.googleapis.com, clientservices.googleapis.com, cdn.onenote.net
- Not all processes where analyzed, report is missing behavior information

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

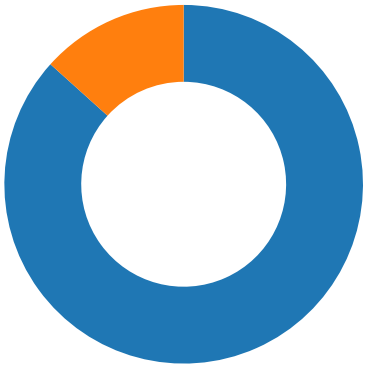
File type:	HTML document, Unicode text, UTF-8 text, with very long lines (7825)
Entropy (8bit):	5.840089611320105
TrID:	• Atom web feed (35501/1) 20.76% • HyperText Markup Language XML (18501/1) 10.82% • Scalable Vector Graphics (18501/1) 10.82% • Artificial Intelligence Markup Language (14501/1) 8.48% • Mathematical Markup Language (13501/1) 7.89%
File name:	login.html
File size:	5877035
MD5:	daccb43d7df16a5b00d0db1340b979ab
SHA1:	ef1e463b2cff4c9b8e5487422ae63ec15083bcbc
SHA256:	f0a3bb756492268062c421579e4115d2764a713e5b7cd2fc95a89c94814e6fc2
SHA512:	c310eee3cab573e728387b3a7a698e36e36ae3ba26c37d85961cd0d7dd96e1e312eb88a9fb014b8099e821b14c0b3b51653e5aed269503f00f261d05b8fe14a0
SSDEEP:	49152:2brAJ6aVxCVUuabZ2LTR17ATlxqiCLX8tfMEvCewKyZlUX7+dZdabAhawsKpg6za:JwwrctOT
TLSH:	1F466B737981247243A686E990EF1285BF3C3347D0054628F36CD9EE5BE9984D1A7BBC
File Content Preview:	<!doctype html> [if lt IE 7].<html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="en"> <![endif]--> [if IE 7].<html class="no-js lt-ie9 lt-ie8" lang="en"> <![endif]--> [if IE 8].<html class="no-js lt-ie9" lang="en"> <![endif]--> [if gt IE 8]>

File Icon

Icon Hash:	0f3149cc4c490307

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:18:19.049274921 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.049443960 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.049551964 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.053368092 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.053436995 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.103064060 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.103144884 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.103257895 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.103584051 CEST	49750	443	192.168.2.3	216.58.212.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:18:19.103621006 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.150820017 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.167960882 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.168047905 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.170989990 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.171118975 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.172354937 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.186816931 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.186856031 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.188234091 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.188468933 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.190368891 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.190493107 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.505518913 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.505951881 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.506926060 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.507004023 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.507209063 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.507611036 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.507841110 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.507882118 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.538070917 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.538244009 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.538295984 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.538394928 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.538547039 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.539030075 CEST	49750	443	192.168.2.3	216.58.212.174
May 26, 2023 13:18:19.539067984 CEST	443	49750	216.58.212.174	192.168.2.3
May 26, 2023 13:18:19.567183971 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.591365099 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.591702938 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:19.591830969 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.593846083 CEST	49749	443	192.168.2.3	142.250.186.45
May 26, 2023 13:18:19.593898058 CEST	443	49749	142.250.186.45	192.168.2.3
May 26, 2023 13:18:22.844258070 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.844336033 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.844451904 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.845412970 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.845443010 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.914408922 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.914860010 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.914885998 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.916234016 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.916428089 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.919033051 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.919131994 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:22.979422092 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:22.979477882 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:23.177371025 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:32.902923107 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:32.903064013 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:32.903162003 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:33.457587957 CEST	49752	443	192.168.2.3	216.58.212.164
May 26, 2023 13:18:33.457644939 CEST	443	49752	216.58.212.164	192.168.2.3
May 26, 2023 13:18:49.135298014 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 13:18:49.135365963 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 13:18:49.135622978 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 13:18:49.136478901 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 13:18:49.136503935 CEST	443	49755	192.168.8.1	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:19:19.140274048 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 13:19:19.186825037 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 13:19:22.894849062 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:22.894946098 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:22.895067930 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:22.895514011 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:22.895553112 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:22.956020117 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:22.962094069 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:22.962141037 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:22.963306904 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:22.963895082 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:22.964273930 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:23.004708052 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:32.976198912 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:32.976371050 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:32.976562977 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:33.808655024 CEST	49759	443	192.168.2.3	172.217.16.196
May 26, 2023 13:19:33.808713913 CEST	443	49759	172.217.16.196	192.168.2.3
May 26, 2023 13:19:56.780175924 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 13:19:56.780307055 CEST	443	49761	192.168.8.1	192.168.2.3
May 26, 2023 13:19:56.780524969 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 13:19:56.781084061 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 13:19:56.781121016 CEST	443	49761	192.168.8.1	192.168.2.3
May 26, 2023 13:20:04.193053961 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 13:20:04.193088055 CEST	443	49755	192.168.8.1	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:18:18.913467884 CEST	58615	53	192.168.2.3	1.1.1.1
May 26, 2023 13:18:18.914005995 CEST	52026	53	192.168.2.3	1.1.1.1
May 26, 2023 13:18:18.930218935 CEST	53	58615	1.1.1.1	192.168.2.3
May 26, 2023 13:18:18.930712938 CEST	53	52026	1.1.1.1	192.168.2.3
May 26, 2023 13:18:22.794048071 CEST	59318	53	192.168.2.3	1.1.1.1
May 26, 2023 13:18:22.810914993 CEST	53	59318	1.1.1.1	192.168.2.3
May 26, 2023 13:18:22.820312977 CEST	59520	53	192.168.2.3	1.1.1.1
May 26, 2023 13:18:22.836958885 CEST	53	59520	1.1.1.1	192.168.2.3
May 26, 2023 13:19:22.854386091 CEST	60556	53	192.168.2.3	1.1.1.1
May 26, 2023 13:19:22.871488094 CEST	53	60556	1.1.1.1	192.168.2.3
May 26, 2023 13:19:22.876698971 CEST	55131	53	192.168.2.3	1.1.1.1
May 26, 2023 13:19:22.893430948 CEST	53	55131	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 13:18:18.913467884 CEST	192.168.2.3	1.1.1.1	0xd5c9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:18.914005995 CEST	192.168.2.3	1.1.1.1	0x75b8	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:22.794048071 CEST	192.168.2.3	1.1.1.1	0x367f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:22.820312977 CEST	192.168.2.3	1.1.1.1	0x58f4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:22.854386091 CEST	192.168.2.3	1.1.1.1	0xae09	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:22.876698971 CEST	192.168.2.3	1.1.1.1	0x2807	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

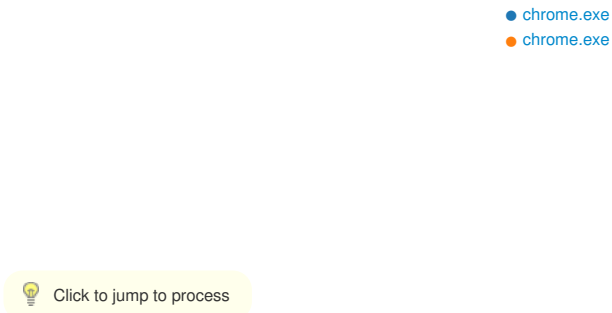
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 13:18:18.930218935 CEST	1.1.1.1	192.168.2.3	0xd5c9	No error (0)	accounts.google.com		142.250.186.45	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:18.930712938 CEST	1.1.1.1	192.168.2.3	0x75b8	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 13:18:18.930712938 CEST	1.1.1.1	192.168.2.3	0x75b8	No error (0)	clients.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:22.810914993 CEST	1.1.1.1	192.168.2.3	0x367f	No error (0)	www.google.com		142.250.184.196	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:22.836958885 CEST	1.1.1.1	192.168.2.3	0x58f4	No error (0)	www.google.com		216.58.212.164	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:22.871488094 CEST	1.1.1.1	192.168.2.3	0xae09	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:22.893430948 CEST	1.1.1.1	192.168.2.3	0x2807	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6556, Parent PID: 3840

General

Target ID:	0
Start time:	13:18:16
Start date:	26/05/2023

Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\login.html
Imagebase:	0x7ff70f0c0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Analysis Process: chrome.exe PID: **1584**, Parent PID: **6556**

General

Target ID:	1
Start time:	13:18:17
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2036 --field-trial-handle=1772,i,15227930420298686886,3054010558266752575,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff70f0c0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Disassembly

No disassembly