ID: 876182
Sample Name: login.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 13:18:24
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

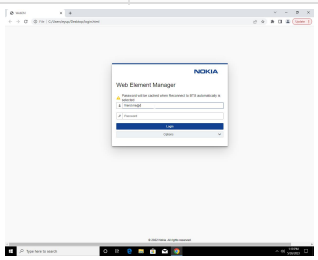
Windows Analysis Report

login.html

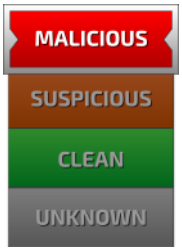
Overview

General Information

Sample Name:	login.html
Analysis ID:	876182
MD5:	2bed4e10b45a…
SHA1:	4a6d48cf4fcbd…
SHA256:	8144972cf5d53..
Infos:	



Detection

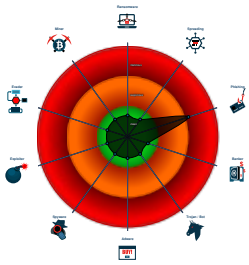


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 4916 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\login.html MD5: C817D9E0D995276EC89E4C89AFC19694)
  - chrome.exe (PID: 7176 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=2012 --field-trial-handle=2104,i,15377410011852329966,8301881256533976150,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: C817D9E0D995276EC89E4C89AFC19694)
- **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

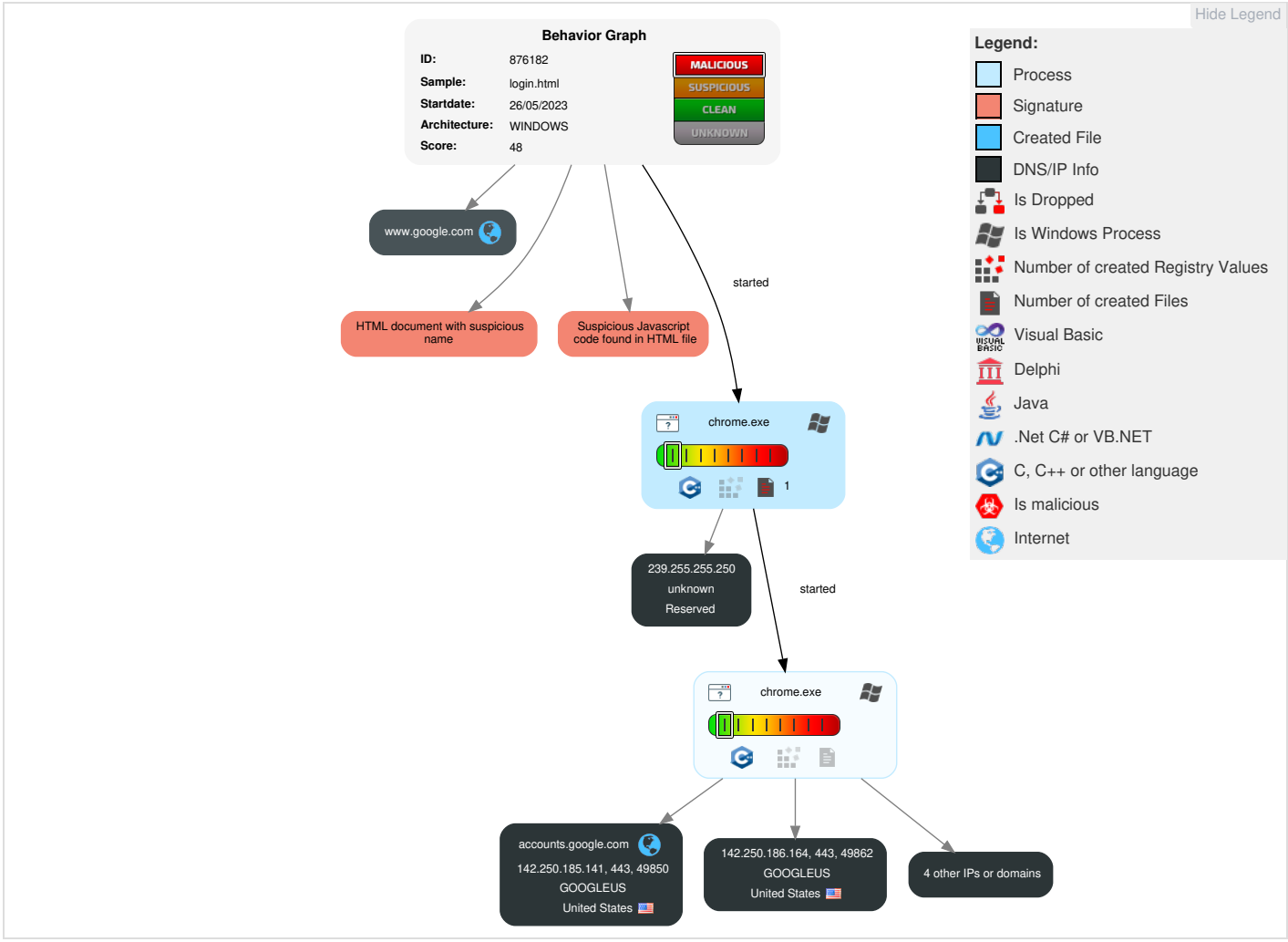
System Summary

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

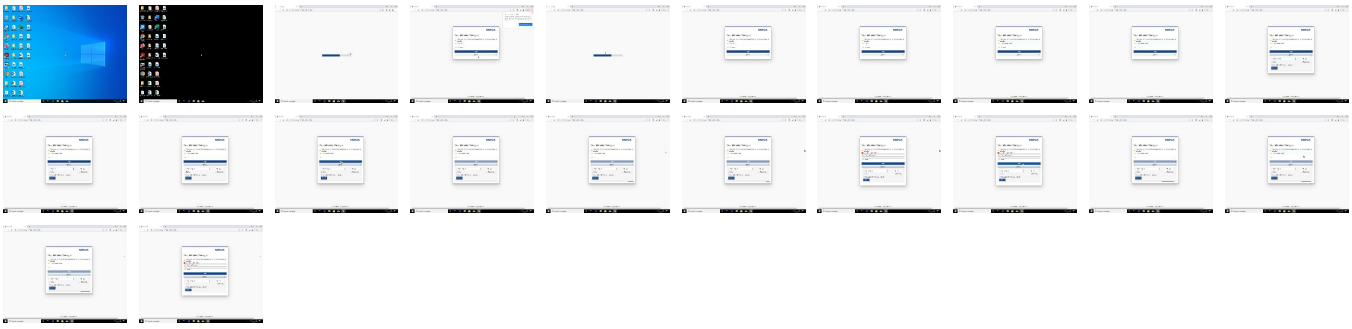
Behavior Graph

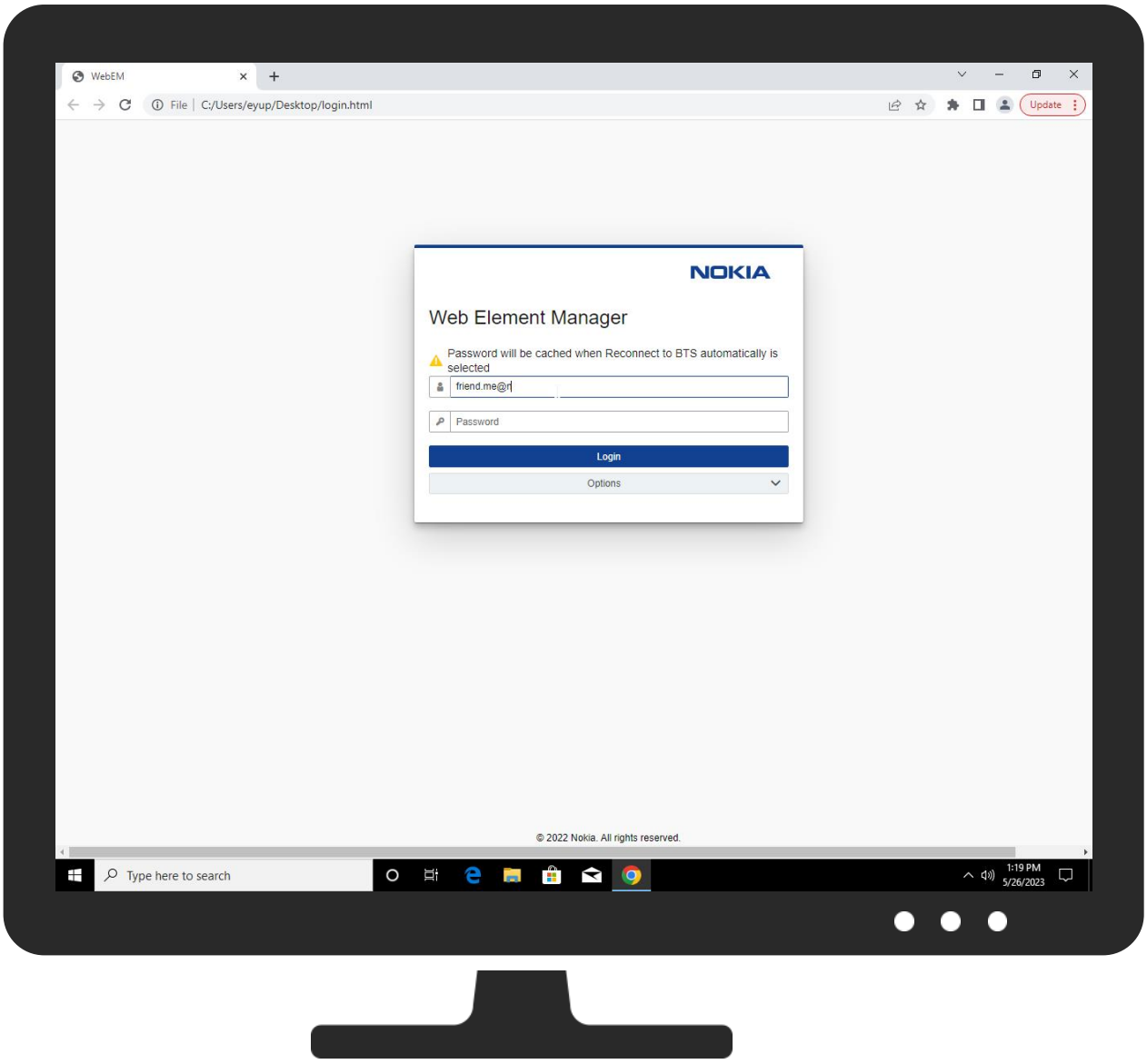


Screenshots

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	142.250.185.141	true	false		high
www.google.com	142.250.186.68	true	false		high
clients.l.google.com	142.250.186.46	true	false		high
clients2.google.com	unknown	unknown	false		high

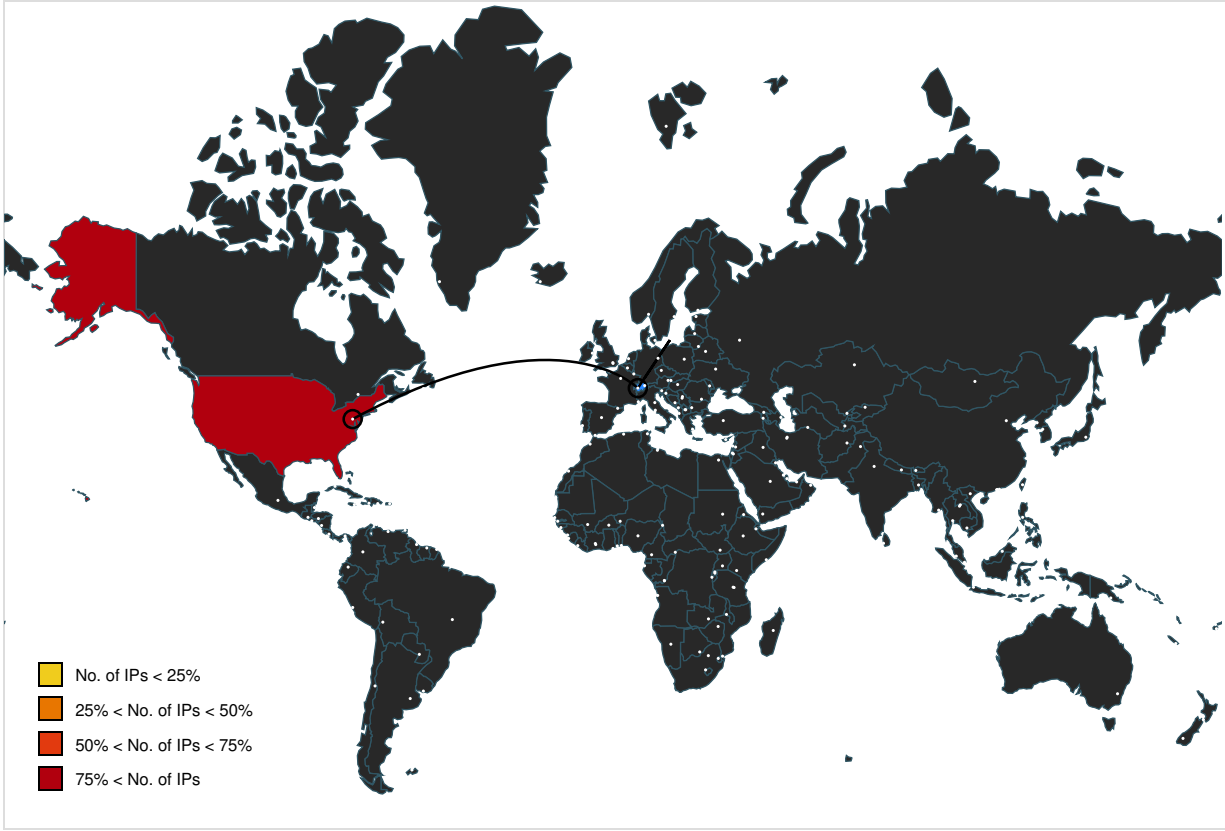
Contacted URLs

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=108.0.5359.125&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
file:///C:/Users/user/Desktop/login.html	true		low

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://developer.mozilla.org/en-US/docs/Web/CSS/CSS_animated_properties)	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
142.250.186.46	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.68	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.141	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.186.164	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.8.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876182
Start date and time:	2023-05-26 13:18:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
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:	7
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@23/0@5/6
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, SIHClient.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.131, 34.104.35.123, 142.250.181.227
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, login.live.com, slscr.update.microsoft.com, update.googleapis.com, clientservices.googleapis.com
- 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

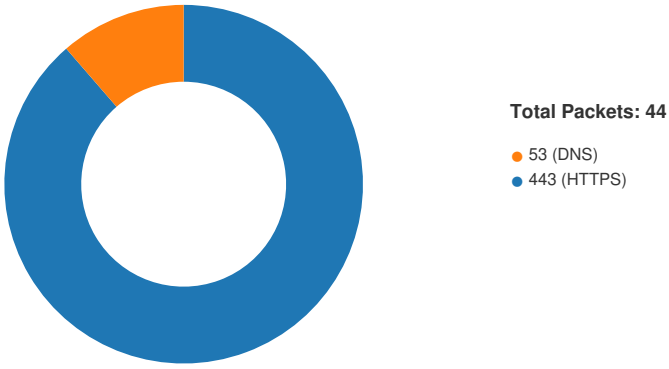
File type:	HTML document, Unicode text, UTF-8 text, with very long lines (11622)
Entropy (8bit):	5.751667127058019
TrID:	• Atom web feed (35501/1) 20.76% • HyperText Markup Language XML (18501/1) 10.82% • Scalable Vector Graphics (18501/1) 10.82% • Artificial Intelligence Markup Language (14501/1) 8.48% • Mathematical Markup Language (13501/1) 7.89%
File name:	login.html
File size:	3755553
MD5:	2bed4e10b45a42651153a0345ed603a7
SHA1:	4a6d48cf4fcbde75db9915f8eb549ee48b3ca29e
SHA256:	8144972cf5d537d3eacf74282e57912448d80c87589e263154dfe0ba58e4fa20
SHA512:	7a77042ce031cc71b9491b4bf60d122f91335100d85bd40b4f3a65af8f7d1ec6d3cb97377c9731eecd16a119257e3c3828acee88cad2471938d7cfd46ee20b35
SSDEEP:	49152:uPp1aRH1wQsPMXuDTrw5qe8DQxhcTzY4KHWOoQ70Otup26z/riwDKJYTcA2gP3k:OpLkyrA
TLSH:	2F067E963A91343103A299F690FF008AB33D7245B4094168F66CD8EA6F7D95892F7F7C
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:	173149cccc490307

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:18:59.844387054 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:18:59.844468117 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:18:59.844609976 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:18:59.846960068 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:18:59.847038031 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:18:59.847130060 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:18:59.847625017 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:18:59.847659111 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:18:59.848058939 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:18:59.848095894 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:18:59.989780903 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:18:59.990535975 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.031497002 CEST	49852	443	192.168.2.2	142.250.186.46

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:19:00.031553984 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.031687975 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.031712055 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.033008099 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.033138990 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.036307096 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.036379099 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.036433935 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.036484003 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.325939894 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.326293945 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.326325893 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.326380014 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.326533079 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.326967001 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.327003956 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.359334946 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.359492064 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.359553099 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.359610081 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.359684944 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.360611916 CEST	49852	443	192.168.2.2	142.250.186.46
May 26, 2023 13:19:00.360656023 CEST	443	49852	142.250.186.46	192.168.2.2
May 26, 2023 13:19:00.377911091 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.378175974 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.378213882 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.378252029 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:00.378338099 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.379918098 CEST	49850	443	192.168.2.2	142.250.185.141
May 26, 2023 13:19:00.379952908 CEST	443	49850	142.250.185.141	192.168.2.2
May 26, 2023 13:19:02.370265007 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.370313883 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.370397091 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.370906115 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.370918989 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.429876089 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.436201096 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.436228037 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.437647104 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.437747002 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.444185972 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.444372892 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.498837948 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:02.498878956 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:02.599832058 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:12.421078920 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:12.421207905 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:12.421291113 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:14.075465918 CEST	49855	443	192.168.2.2	142.250.186.68
May 26, 2023 13:19:14.075504065 CEST	443	49855	142.250.186.68	192.168.2.2
May 26, 2023 13:19:25.453273058 CEST	49859	443	192.168.2.2	192.168.8.1
May 26, 2023 13:19:25.453361034 CEST	443	49859	192.168.8.1	192.168.2.2
May 26, 2023 13:19:25.453769922 CEST	49859	443	192.168.2.2	192.168.8.1
May 26, 2023 13:19:25.454197884 CEST	49859	443	192.168.2.2	192.168.8.1
May 26, 2023 13:19:25.454231977 CEST	443	49859	192.168.8.1	192.168.2.2
May 26, 2023 13:19:55.463520050 CEST	49859	443	192.168.2.2	192.168.8.1
May 26, 2023 13:19:55.510864973 CEST	443	49859	192.168.8.1	192.168.2.2
May 26, 2023 13:20:02.418777943 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:02.418852091 CEST	443	49862	142.250.186.164	192.168.2.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:20:02.419004917 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:02.420104980 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:02.420140028 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:02.478332043 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:02.479784966 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:02.479832888 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:02.480539083 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:02.482117891 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:02.482266903 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:02.523160934 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:05.441783905 CEST	49863	443	192.168.2.2	192.168.8.1
May 26, 2023 13:20:05.441868067 CEST	443	49863	192.168.8.1	192.168.2.2
May 26, 2023 13:20:05.442111015 CEST	49863	443	192.168.2.2	192.168.8.1
May 26, 2023 13:20:05.442600012 CEST	49863	443	192.168.2.2	192.168.8.1
May 26, 2023 13:20:05.442636013 CEST	443	49863	192.168.8.1	192.168.2.2
May 26, 2023 13:20:12.517433882 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:12.517580032 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:12.517788887 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:12.858957052 CEST	49862	443	192.168.2.2	142.250.186.164
May 26, 2023 13:20:12.859014988 CEST	443	49862	142.250.186.164	192.168.2.2
May 26, 2023 13:20:35.454138994 CEST	49863	443	192.168.2.2	192.168.8.1
May 26, 2023 13:20:35.498845100 CEST	443	49863	192.168.8.1	192.168.2.2
May 26, 2023 13:20:40.518342972 CEST	49859	443	192.168.2.2	192.168.8.1
May 26, 2023 13:20:40.518381119 CEST	443	49859	192.168.8.1	192.168.2.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 13:18:59.727849007 CEST	52756	53	192.168.2.2	1.1.1.1
May 26, 2023 13:18:59.729933023 CEST	62881	53	192.168.2.2	1.1.1.1
May 26, 2023 13:18:59.744868040 CEST	53	52756	1.1.1.1	192.168.2.2
May 26, 2023 13:18:59.746738911 CEST	53	62881	1.1.1.1	192.168.2.2
May 26, 2023 13:19:02.338146925 CEST	65102	53	192.168.2.2	1.1.1.1
May 26, 2023 13:19:02.355225086 CEST	53	65102	1.1.1.1	192.168.2.2
May 26, 2023 13:20:02.398961067 CEST	55420	53	192.168.2.2	1.1.1.1
May 26, 2023 13:20:02.415838957 CEST	53	55420	1.1.1.1	192.168.2.2
May 26, 2023 13:21:02.464523077 CEST	55067	53	192.168.2.2	1.1.1.1
May 26, 2023 13:21:02.481475115 CEST	53	55067	1.1.1.1	192.168.2.2

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 13:18:59.727849007 CEST	192.168.2.2	1.1.1.1	0x7252	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:59.729933023 CEST	192.168.2.2	1.1.1.1	0x476c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:02.338146925 CEST	192.168.2.2	1.1.1.1	0xba3e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:20:02.398961067 CEST	192.168.2.2	1.1.1.1	0x17a8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 13:21:02.464523077 CEST	192.168.2.2	1.1.1.1	0x90c3	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 13:18:59.744868040 CEST	1.1.1.1	192.168.2.2	0x7252	No error (0)	accounts.google.com		142.250.185.141	A (IP address)	IN (0x0001)	false
May 26, 2023 13:18:59.746738911 CEST	1.1.1.1	192.168.2.2	0x476c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

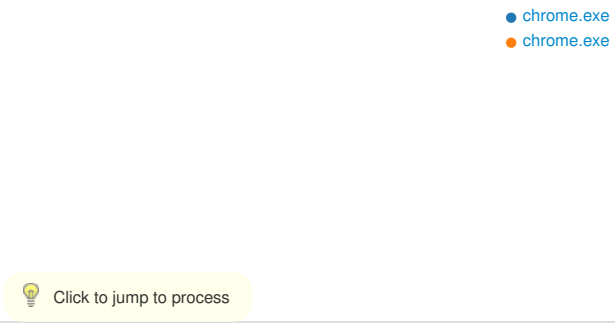
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 13:18:59.746738911 CEST	1.1.1.1	192.168.2.2	0x476c	No error (0)	clients.l.google.com		142.250.186.46	A (IP address)	IN (0x0001)	false
May 26, 2023 13:19:02.355225086 CEST	1.1.1.1	192.168.2.2	0xba3e	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
May 26, 2023 13:20:02.415838957 CEST	1.1.1.1	192.168.2.2	0x17a8	No error (0)	www.google.com		142.250.186.164	A (IP address)	IN (0x0001)	false
May 26, 2023 13:21:02.481475115 CEST	1.1.1.1	192.168.2.2	0x90c3	No error (0)	www.google.com		142.250.184.228	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4916**, Parent PID: **3164**

General	
Target ID:	0
Start time:	13:18:56
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:	0x7ff733a40000
File size:	3133720 bytes
MD5 hash:	C817D9E0D995276EC89E4C89AFC19694
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **7176**, Parent PID: **4916**

General

Target ID:	1
Start time:	13:18:57
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=2012 --field-trial-handle=2104,i,15377410011852329966,8301881256533976150,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff733a40000
File size:	3133720 bytes
MD5 hash:	C817D9E0D995276EC89E4C89AFC19694
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

Disassembly

No disassembly