
**ID:** 876180
**Sample Name:** login.html
**Cookbook:**
defaultwindowsinteractivecookbook.jbs
**Time:** 13:07:21
**Date:** 26/05/2023
**Version:** 37.1.0 Beryl

# Table of Contents

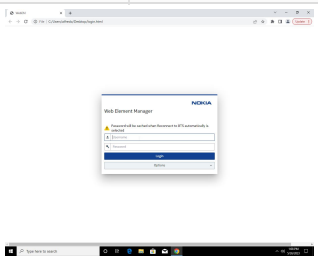
# Windows Analysis Report

## login.html

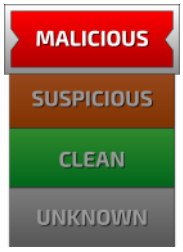
## Overview

### General Information

| | |
|---|---|
| Sample Name: | login.html |
| Analysis ID: | 876180 |
| MD5: | daccb43d7df16.. |
| SHA1: | ef1e463b2cff4c.. |
| SHA256: | f0a3bb7564922.. |
| Infos: | |



### Detection

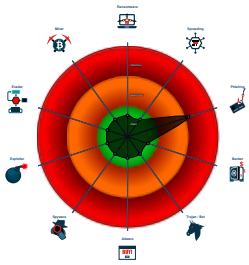



| | |
|---|---|
| Score: | 48 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### 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: 3564 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\login.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6928 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=2040 --field-trial-handle=1776,i,3959098085490163762,14531336400767641844,131072 --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

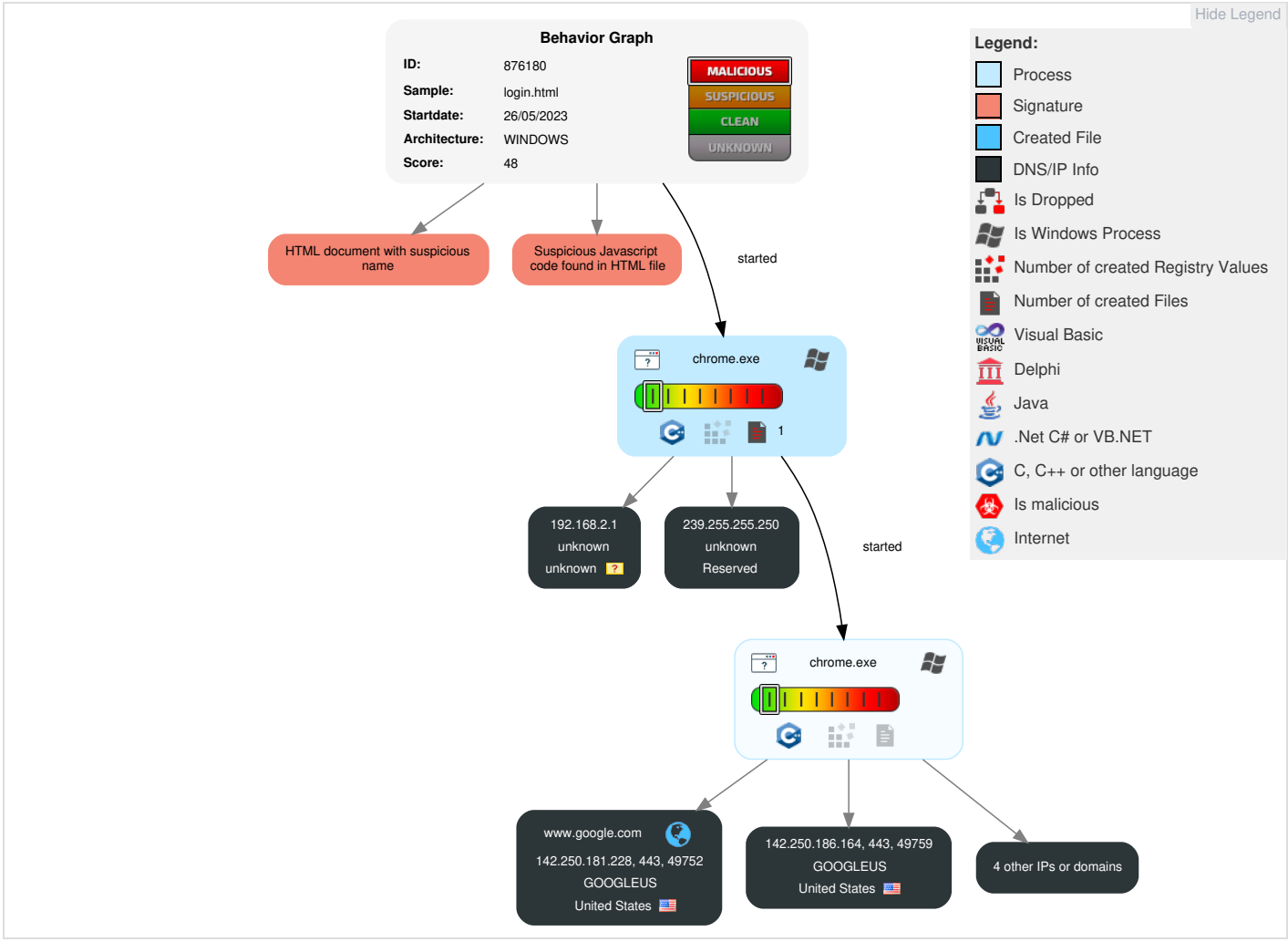
### System Summary

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 |

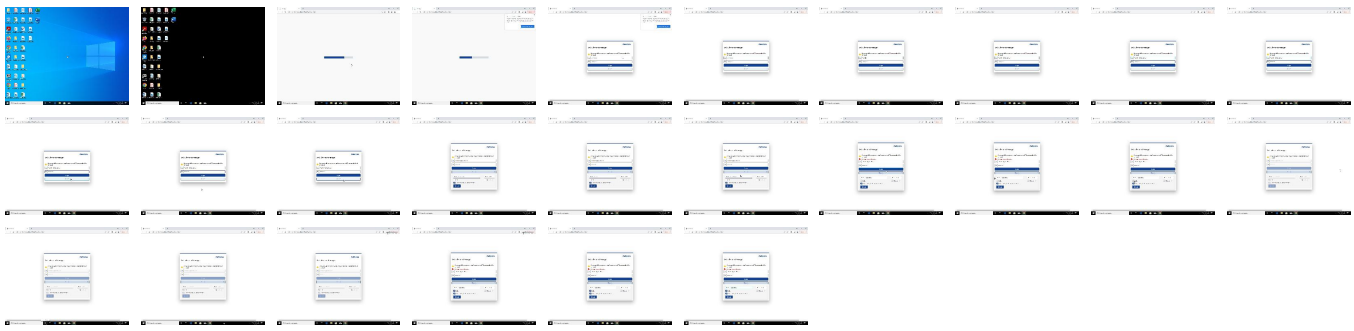
## Behavior Graph

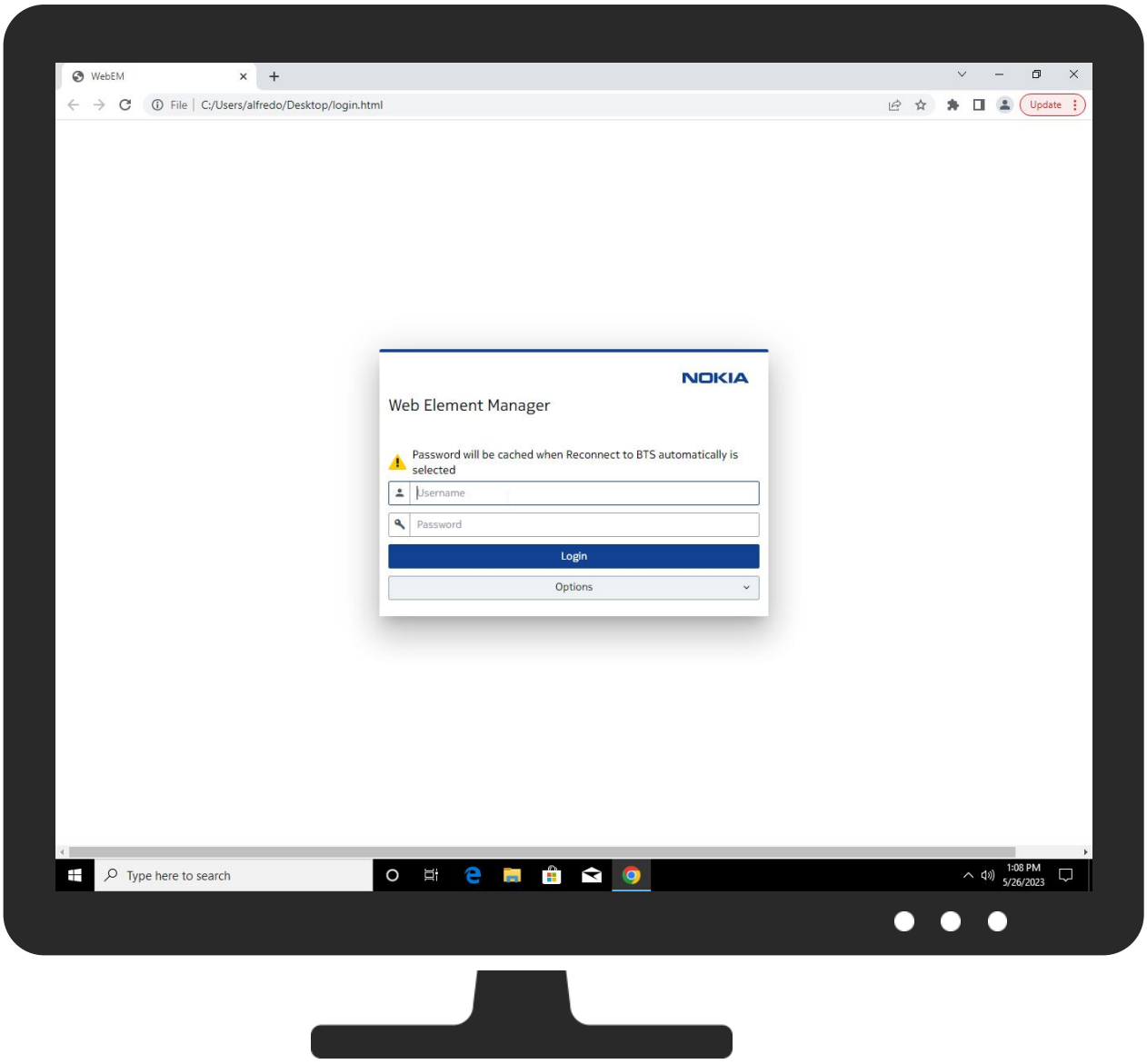



# Screenshots

## 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 | 216.58.212.173 | true | false | | high |
| www.google.com | 142.250.181.228 | true | false | | high |
| clients.l.google.com | 142.250.186.174 | true | false | | high |
| clients2.google.com | unknown | unknown | false | | high |

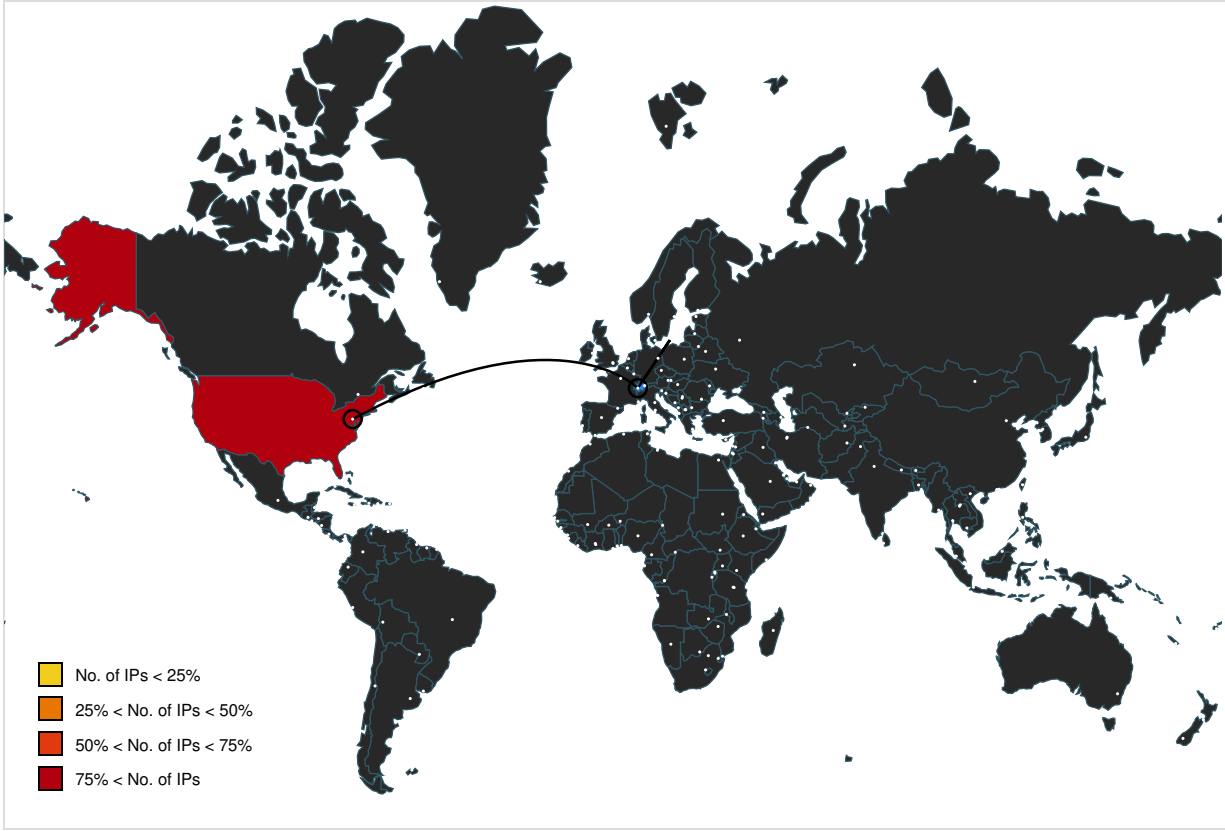
## Contacted URLs

| 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<br>• 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 |
|---|---|---|---|---|---|---|
| 239.255.255.250 | unknown | Reserved | ? | unknown | unknown | false |
| 142.250.181.228 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.186.174 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.186.164 | unknown | United States | | 15169 | GOOGLEUS | false |
| 216.58.212.173 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |

**Private**

| IP |
|---|
| 192.168.2.1 |
| 192.168.8.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.1.0 Beryl |
| Analysis ID: | 876180 |
| Start date and time: | 2023-05-26 13:07:21 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 4m 14s |
| 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: | 3 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |

| | |
|---|---|
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | login.html |
| Detection: | MAL |
| Classification: | mal48.phis.winHTML@24/0@6/7 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .html |

### Warnings

- Exclude process from analysis (whitelisted): svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, login.live.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

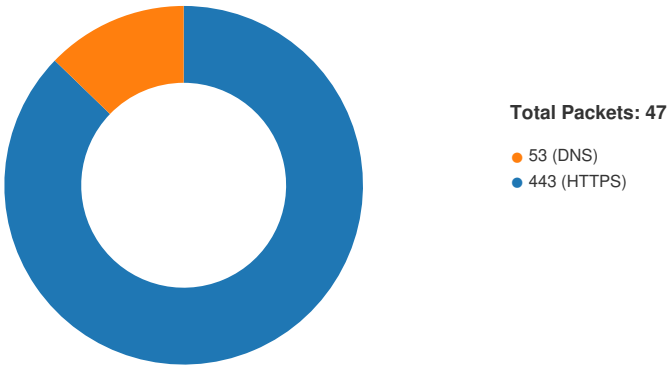
| | |
|---|---|
| File type: | HTML document, Unicode text, UTF-8 text, with very long lines (7825) |
| Entropy (8bit): | 5.840089611320105 |
| TrID: | • Atom web feed (35501/1) 20.76%<br>• HyperText Markup Language XML (18501/1) 10.82%<br>• Scalable Vector Graphics (18501/1) 10.82%<br>• Artificial Intelligence Markup Language (14501/1) 8.48%<br>• 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 13:07:51.400619030 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.400693893 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.400814056 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.418652058 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.418724060 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.420115948 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.420186996 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.420300961 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.420504093 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.420535088 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.533128023 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 26, 2023 13:07:51.538477898 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.538520098 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.539134979 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.539259911 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.539940119 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.540055990 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.567812920 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.612163067 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.696618080 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.696655035 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.701330900 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.701463938 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.849123001 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.849514961 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.850357056 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.850421906 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.851481915 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.851681948 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.851706982 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.851874113 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.883640051 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.883748055 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.883790016 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.883934975 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.884023905 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.884881020 CEST | 49748 | 443 | 192.168.2.3 | 142.250.186.174 |
| May 26, 2023 13:07:51.884927034 CEST | 443 | 49748 | 142.250.186.174 | 192.168.2.3 |
| May 26, 2023 13:07:51.891083002 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.906132936 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.906229019 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.906285048 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.906548023 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:51.906622887 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.907476902 CEST | 49750 | 443 | 192.168.2.3 | 216.58.212.173 |
| May 26, 2023 13:07:51.907510996 CEST | 443 | 49750 | 216.58.212.173 | 192.168.2.3 |
| May 26, 2023 13:07:55.313117981 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.313199043 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.313313007 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.313735962 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.313774109 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.386934996 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.387664080 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.387727976 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.388981104 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.389168978 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.391175032 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.391391039 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.573523998 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:07:55.573576927 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:07:55.674484015 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:08:05.358793974 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:08:05.358985901 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:08:05.359230042 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:08:06.161745071 CEST | 49752 | 443 | 192.168.2.3 | 142.250.181.228 |
| May 26, 2023 13:08:06.161793947 CEST | 443 | 49752 | 142.250.181.228 | 192.168.2.3 |
| May 26, 2023 13:08:35.555830002 CEST | 49755 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:08:35.555891037 CEST | 443 | 49755 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:08:35.556015015 CEST | 49755 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:08:35.568034887 CEST | 49755 | 443 | 192.168.2.3 | 192.168.8.1 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 26, 2023 13:08:35.568068981 CEST | 443 | 49755 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:08:35.568293095 CEST | 443 | 49755 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:08:42.017419100 CEST | 49756 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:08:42.017508984 CEST | 443 | 49756 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:08:42.017800093 CEST | 49756 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:08:42.018251896 CEST | 49756 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:08:42.018287897 CEST | 443 | 49756 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:08:55.361479998 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:08:55.361551046 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.361722946 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:08:55.362885952 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:08:55.362922907 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.422955990 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.423672915 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:08:55.423738003 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.424434900 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.425582886 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:08:55.425769091 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:08:55.466732979 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:09:05.423384905 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:09:05.423553944 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:09:05.423917055 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:09:06.164712906 CEST | 49759 | 443 | 192.168.2.3 | 142.250.186.164 |
| May 26, 2023 13:09:06.164767027 CEST | 443 | 49759 | 142.250.186.164 | 192.168.2.3 |
| May 26, 2023 13:09:12.021434069 CEST | 49756 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:09:12.062843084 CEST | 443 | 49756 | 192.168.8.1 | 192.168.2.3 |
| May 26, 2023 13:09:57.067023039 CEST | 49756 | 443 | 192.168.2.3 | 192.168.8.1 |
| May 26, 2023 13:09:57.067087889 CEST | 443 | 49756 | 192.168.8.1 | 192.168.2.3 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 26, 2023 13:07:51.363832951 CEST | 57319 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:07:51.364128113 CEST | 60671 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:07:51.380985975 CEST | 53 | 57319 | 1.1.1.1 | 192.168.2.3 |
| May 26, 2023 13:07:51.381026983 CEST | 53 | 60671 | 1.1.1.1 | 192.168.2.3 |
| May 26, 2023 13:07:55.273209095 CEST | 51601 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:07:55.290276051 CEST | 53 | 51601 | 1.1.1.1 | 192.168.2.3 |
| May 26, 2023 13:07:55.293823957 CEST | 58242 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:07:55.310697079 CEST | 53 | 58242 | 1.1.1.1 | 192.168.2.3 |
| May 26, 2023 13:08:55.321634054 CEST | 58921 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:08:55.338728905 CEST | 53 | 58921 | 1.1.1.1 | 192.168.2.3 |
| May 26, 2023 13:08:55.342730045 CEST | 60298 | 53 | 192.168.2.3 | 1.1.1.1 |
| May 26, 2023 13:08:55.359709024 CEST | 53 | 60298 | 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 13:07:51.363832951 CEST | 192.168.2.3 | 1.1.1.1 | 0x3006 | Standard query (0) | accounts.google.com | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:51.364128113 CEST | 192.168.2.3 | 1.1.1.1 | 0xdb94 | Standard query (0) | clients2.google.com | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:55.273209095 CEST | 192.168.2.3 | 1.1.1.1 | 0xe925 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:55.293823957 CEST | 192.168.2.3 | 1.1.1.1 | 0x1322 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:08:55.321634054 CEST | 192.168.2.3 | 1.1.1.1 | 0xcbee | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:08:55.342730045 CEST | 192.168.2.3 | 1.1.1.1 | 0x4804 | 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 13:07:51.380985975 CEST | 1.1.1.1 | 192.168.2.3 | 0x3006 | No error (0) | accounts.google.com | | 216.58.212.173 | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:51.381026983 CEST | 1.1.1.1 | 192.168.2.3 | 0xdb94 | No error (0) | clients2.google.com | clients.l.google.com | | CNAME (Canonical name) | IN (0x0001) | false |
| May 26, 2023 13:07:51.381026983 CEST | 1.1.1.1 | 192.168.2.3 | 0xdb94 | No error (0) | clients.l.google.com | | 142.250.186.174 | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:55.290276051 CEST | 1.1.1.1 | 192.168.2.3 | 0xe925 | No error (0) | www.google.com | | 142.250.181.228 | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:07:55.310697079 CEST | 1.1.1.1 | 192.168.2.3 | 0x1322 | No error (0) | www.google.com | | 142.250.181.228 | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:08:55.338728905 CEST | 1.1.1.1 | 192.168.2.3 | 0xcbee | No error (0) | www.google.com | | 142.250.184.196 | A (IP address) | IN (0x0001) | false |
| May 26, 2023 13:08:55.359709024 CEST | 1.1.1.1 | 192.168.2.3 | 0x4804 | No error (0) | www.google.com | | 142.250.186.164 | 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: 3564, Parent PID: 3840

#### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 13:07:48 |

| | |
|---|---|
| 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: **6928**, Parent PID: **3564**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 13:07:49 |
| 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=2040 --field-trial-handle=1776,i,3959098085490163762,14531336400767641844,131072 --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 |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Disassembly

**No disassembly**