



ID: 876177
Sample Name: login.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 12:48:32
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report login.html 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Phishing 4
System Summary 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
Public IPs 8
Private 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
UDP Packets 12
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: chrome.exePID: 5996, Parent PID: 3840 13
General 13
File Activities 14
Analysis Process: chrome.exePID: 2480, Parent PID: 5996 14
General 14
File Activities 14
Disassembly 14

Copyright Joe Security LLC 2023

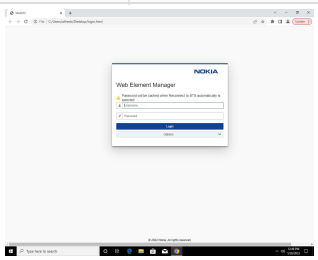
Windows Analysis Report

login.html

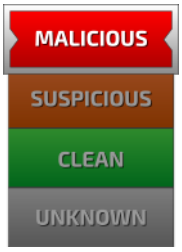
Overview

General Information

Sample Name:	login.html
Analysis ID:	876177
MD5:	2bed4e10b45a…
SHA1:	4a6d48cf4fcbd…
SHA256:	8144972cf5d53..
Infos:	



Detection

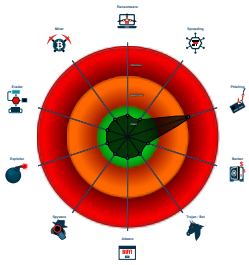


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 5996 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\login.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2480 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=1768,i,8600265007674146631,948493388715969417,131072 --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

Copyright Joe Security LLC 2023

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Suspicious Javascript code found in HTML file

System Summary

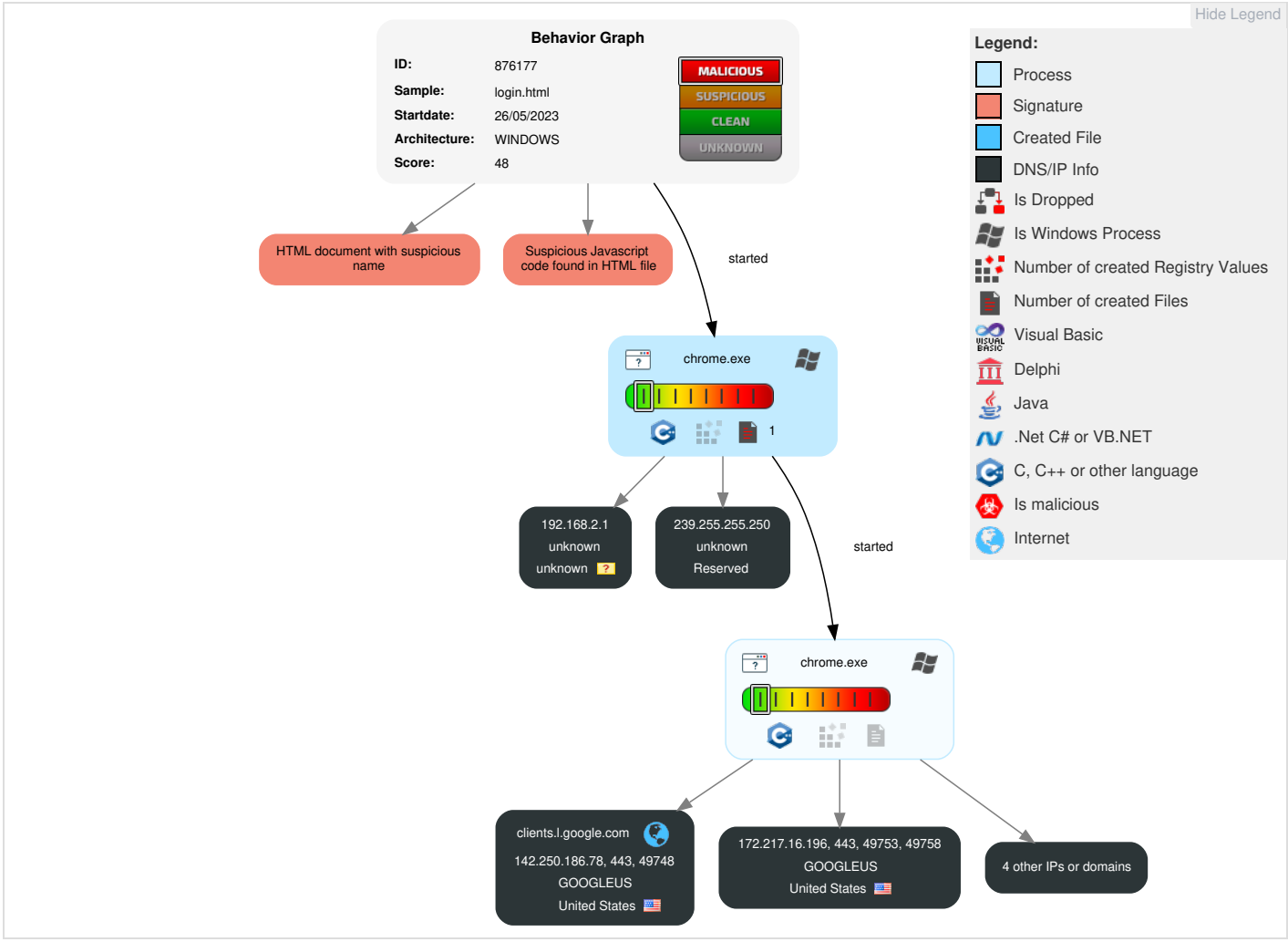


HTML document with suspicious name

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

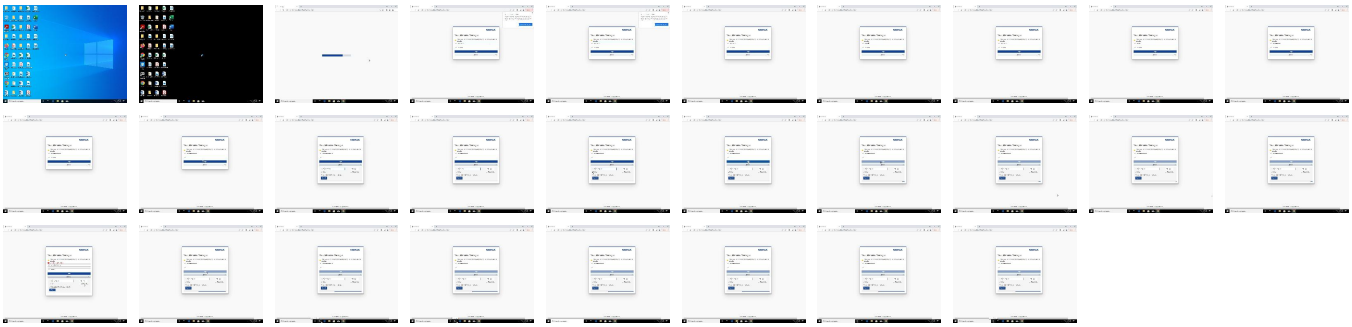
Behavior Graph

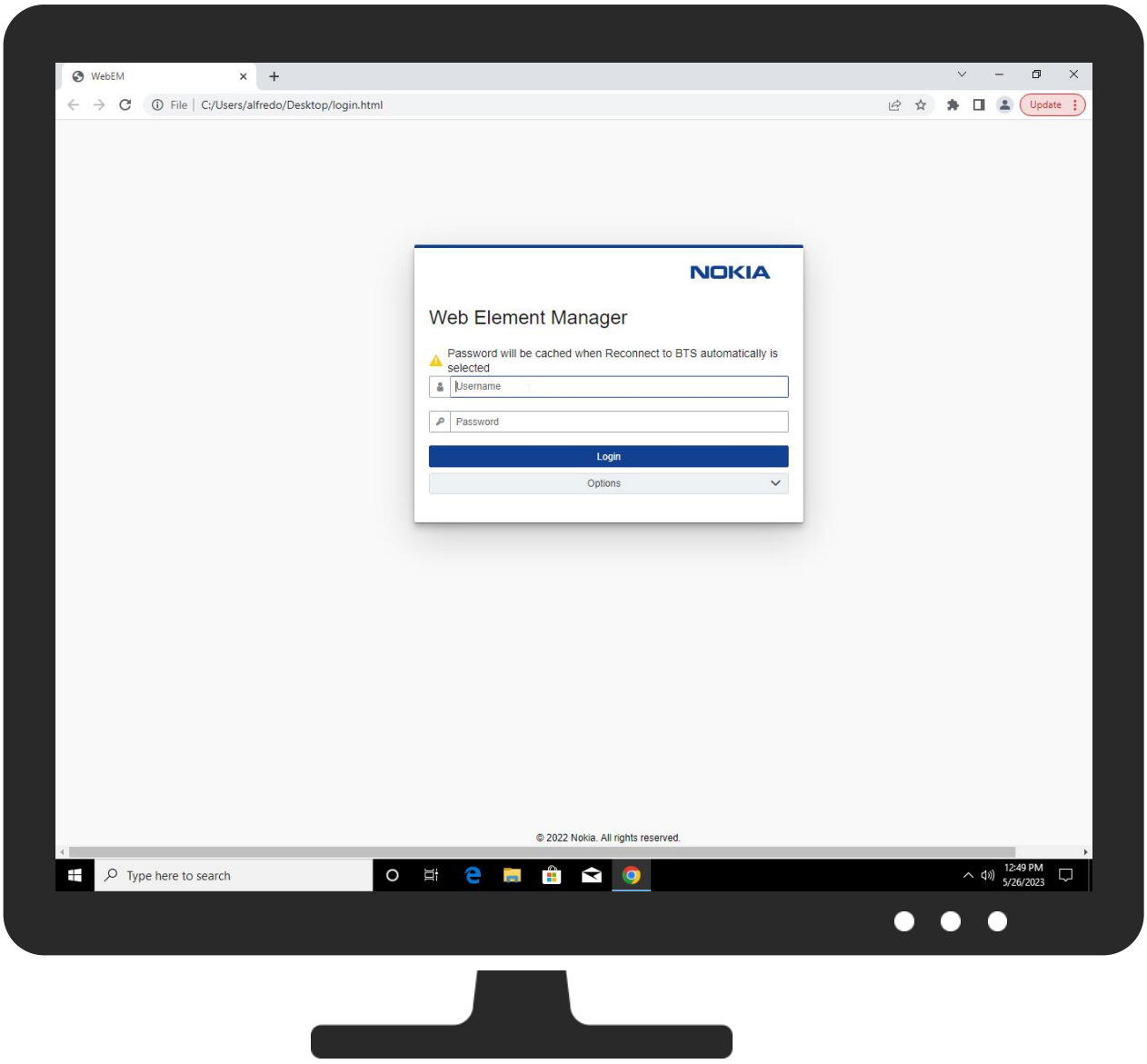


Screenshots

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	142.250.186.132	true	false		high
clients.l.google.com	142.250.186.78	true	false		high
clients2.google.com	unknown	unknown	false		high

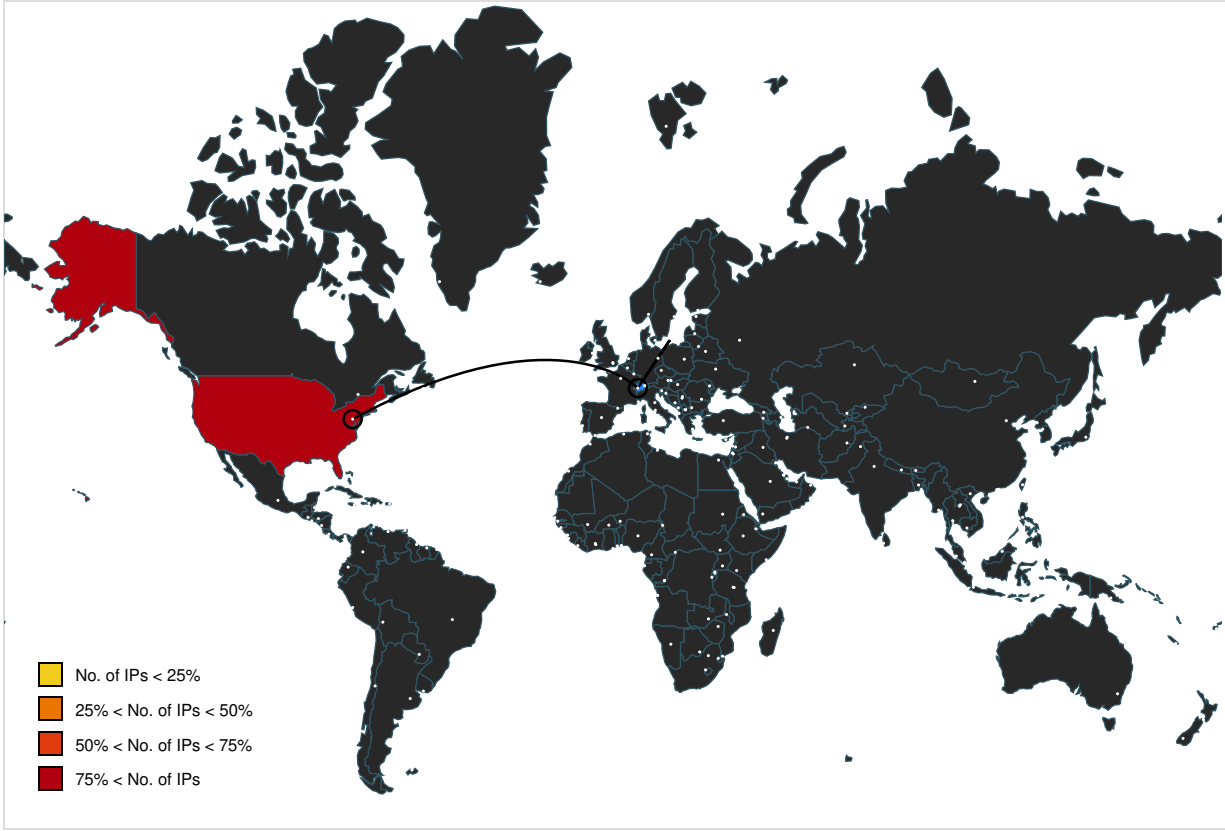
Contacted URLs

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://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
142.250.186.78	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.212.173	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.16.196	unknown	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:	876177
Start date and time:	2023-05-26 12:48:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 12s
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 • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Copyright Joe Security LLC 2023

Analysis stop reason:	Timeout
Sample file name:	login.html
Detection:	MAL
Classification:	mal48.phis.winHTML@25/0@4/6
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): svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.186.99, 34.104.35.123, 142.250.186.131, 142.250.185.99
- 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 (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]>

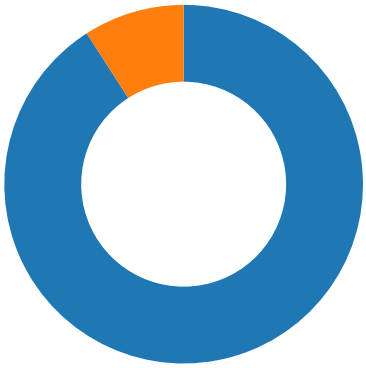
File Icon



Icon Hash:	0f3149cc4c490307

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:49:02.255598068 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.255651951 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.255744934 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.257782936 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.257813931 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.350594044 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.381902933 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.381932020 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.383001089 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.383121967 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.384526014 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.384643078 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.589541912 CEST	49750	443	192.168.2.3	216.58.212.173

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:49:02.589601040 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.589740038 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.590147018 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.590173960 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.654774904 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.655159950 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.655203104 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.656642914 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.656842947 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.657035112 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.657394886 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.659028053 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.659075975 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.659333944 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.659452915 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.659599066 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.659631014 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.691893101 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.692056894 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.692100048 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.692230940 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.692312002 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.696649075 CEST	49748	443	192.168.2.3	142.250.186.78
May 26, 2023 12:49:02.696677923 CEST	443	49748	142.250.186.78	192.168.2.3
May 26, 2023 12:49:02.699656963 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.703792095 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.703922987 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.703949928 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.704127073 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:02.704211950 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.711453915 CEST	49750	443	192.168.2.3	216.58.212.173
May 26, 2023 12:49:02.711483002 CEST	443	49750	216.58.212.173	192.168.2.3
May 26, 2023 12:49:06.090440989 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.090502024 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.090682030 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.090941906 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.090964079 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.157744884 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.158298016 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.158329010 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.159666061 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.159775972 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.161794901 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.162014961 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.278032064 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:06.278079033 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:06.477984905 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:16.134865999 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:16.135051966 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:16.135164022 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:17.780543089 CEST	49753	443	192.168.2.3	172.217.16.196
May 26, 2023 12:49:17.780605078 CEST	443	49753	172.217.16.196	192.168.2.3
May 26, 2023 12:49:42.981910944 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 12:49:42.981992006 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 12:49:42.982146978 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 12:49:42.982590914 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 12:49:42.982625008 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 12:50:06.059665918 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:06.059755087 CEST	443	49758	172.217.16.196	192.168.2.3

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:50:06.059856892 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:06.060497046 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:06.060530901 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:06.123642921 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:06.124099970 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:06.124136925 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:06.125256062 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:06.125715971 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:06.125926971 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:06.166124105 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:12.985914946 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 12:50:13.026911020 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 12:50:16.108927011 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:16.109030008 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:16.109113932 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:17.788781881 CEST	49758	443	192.168.2.3	172.217.16.196
May 26, 2023 12:50:17.788840055 CEST	443	49758	172.217.16.196	192.168.2.3
May 26, 2023 12:50:36.352571964 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 12:50:36.352627993 CEST	443	49761	192.168.8.1	192.168.2.3
May 26, 2023 12:50:36.352768898 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 12:50:36.353543043 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 12:50:36.353576899 CEST	443	49761	192.168.8.1	192.168.2.3
May 26, 2023 12:50:58.031704903 CEST	49755	443	192.168.2.3	192.168.8.1
May 26, 2023 12:50:58.031749964 CEST	443	49755	192.168.8.1	192.168.2.3
May 26, 2023 12:51:06.356529951 CEST	49761	443	192.168.2.3	192.168.8.1
May 26, 2023 12:51:06.398828983 CEST	443	49761	192.168.8.1	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:49:02.194981098 CEST	51048	53	192.168.2.3	1.1.1.1
May 26, 2023 12:49:02.211862087 CEST	53	51048	1.1.1.1	192.168.2.3
May 26, 2023 12:49:02.516541958 CEST	61310	53	192.168.2.3	1.1.1.1
May 26, 2023 12:49:02.533519030 CEST	53	61310	1.1.1.1	192.168.2.3
May 26, 2023 12:49:06.002515078 CEST	56799	53	192.168.2.3	1.1.1.1
May 26, 2023 12:49:06.019246101 CEST	53	56799	1.1.1.1	192.168.2.3
May 26, 2023 12:49:06.056133032 CEST	54134	53	192.168.2.3	1.1.1.1
May 26, 2023 12:49:06.072896004 CEST	53	54134	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 12:49:02.194981098 CEST	192.168.2.3	1.1.1.1	0xdd6b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:49:02.516541958 CEST	192.168.2.3	1.1.1.1	0xfdbf	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:49:06.002515078 CEST	192.168.2.3	1.1.1.1	0x92d4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:49:06.056133032 CEST	192.168.2.3	1.1.1.1	0x8539	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 12:49:02.211862087 CEST	1.1.1.1	192.168.2.3	0xdd6b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 12:49:02.211862087 CEST	1.1.1.1	192.168.2.3	0xdd6b	No error (0)	clients.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2023

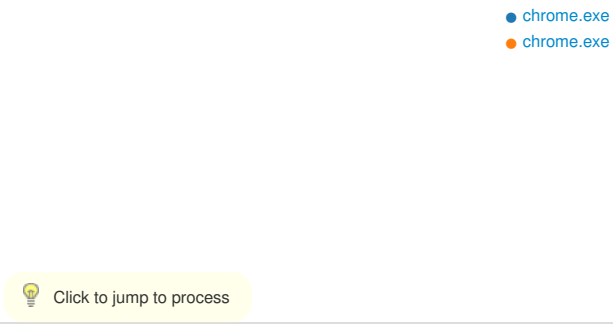
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 12:49:02.533519030 CEST	1.1.1.1	192.168.2.3	0xfdbf	No error (0)	accounts.google.com		216.58.212.173	A (IP address)	IN (0x0001)	false
May 26, 2023 12:49:06.019246101 CEST	1.1.1.1	192.168.2.3	0x92d4	No error (0)	www.google.com		142.250.186.132	A (IP address)	IN (0x0001)	false
May 26, 2023 12:49:06.072896004 CEST	1.1.1.1	192.168.2.3	0x8539	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: **5996**, Parent PID: **3840**

General

Target ID:	0
Start time:	12:48:58
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

Copyright Joe Security LLC 2023

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: **2480**, Parent PID: **5996**

General

Target ID:	1
Start time:	12:49:00
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=1768,i,8600265007674146631,948493388715969417,131072 --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

Copyright Joe Security LLC 2023