ID: 756253
Sample Name:
Paid_invoice.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 21:57:04
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

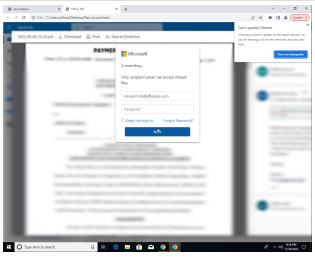
Windows Analysis Report

Paid_invoice.html

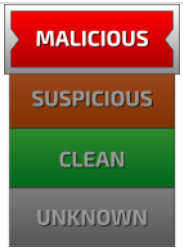
Overview

General Information

Sample Name:	Paid_invoice.html
Analysis ID:	756253
MD5:	388cd3eda11c1e..
SHA1:	fc6c35aaefc9671..
SHA256:	0b81b708477c44..
Infos:	



Detection



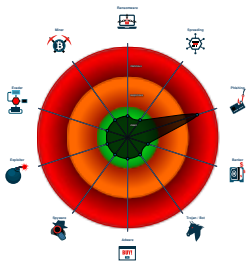
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- HTML document with suspicious title
- HTML document with suspicious na…
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- Invalid 'forgot password' link found
- HTML body contains low number of …
- IP address seen in connection with …
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5044 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5776 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=1756 --field-trial-handle=1648,i,9583188458170825095,14417365062387772299,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6244 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Paid_invoice.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Paid_invoice.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
84167.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

System Summary

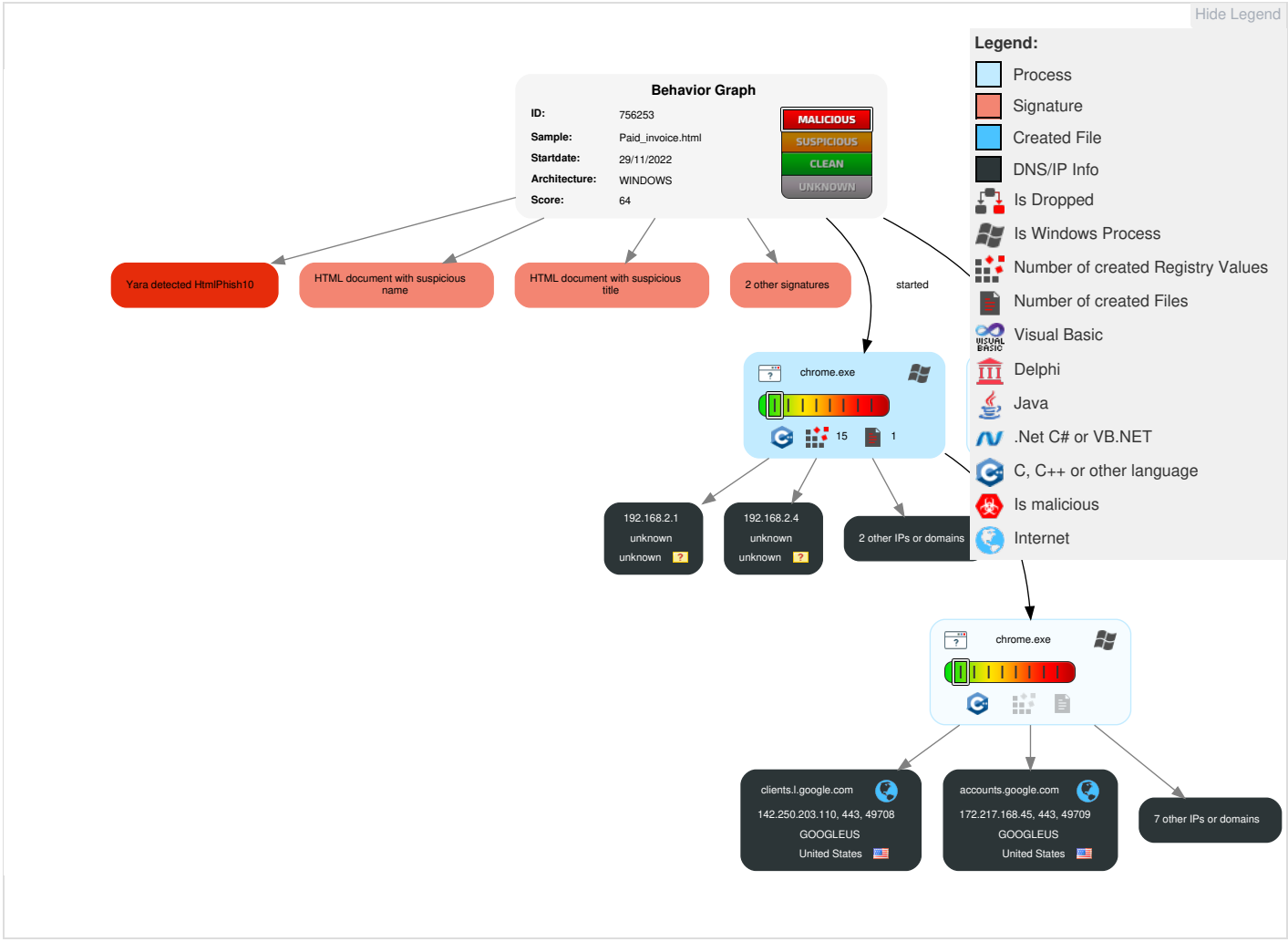
HTML document with suspicious title

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	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

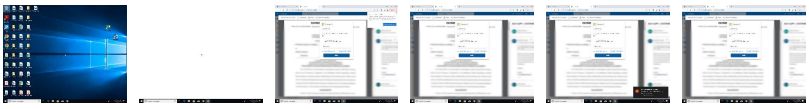
Behavior Graph

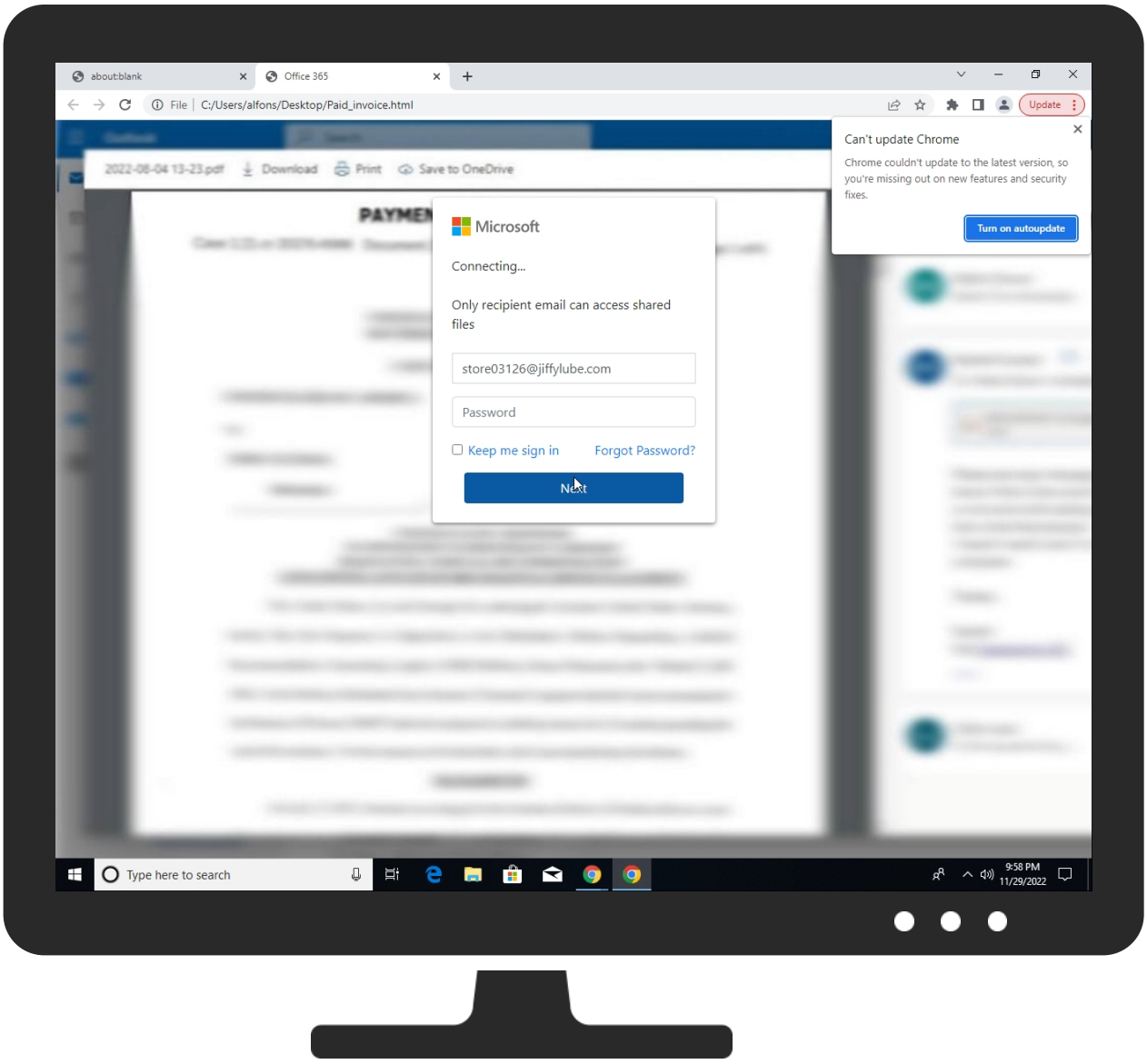


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

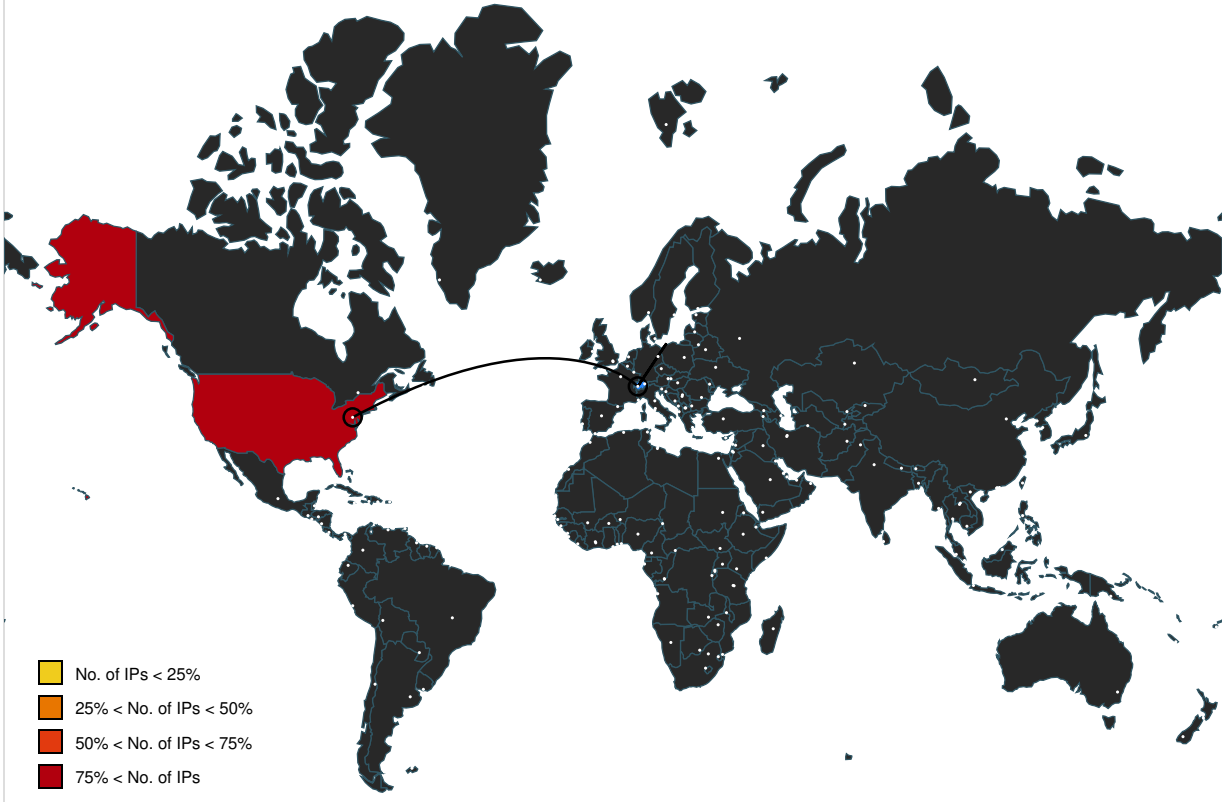
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	false		high
file:///C:/Users/user/Desktop/Paid_invoice.html	true		low
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	Paid_invoice.html	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756253
Start date and time:	2022-11-29 21:57:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Paid_invoice.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winHTML@28/0@8/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 69.16.175.42, 69.16.175.10, 142.250.203.106, 34.104.35.123
- Excluded domains from analysis (whitelisted): client.wns.windows.com, cds.s5x3j6q5.hwcdn.net, edgedl.me.gvt1.com, ajax.googleapis.com, update.googleapis.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

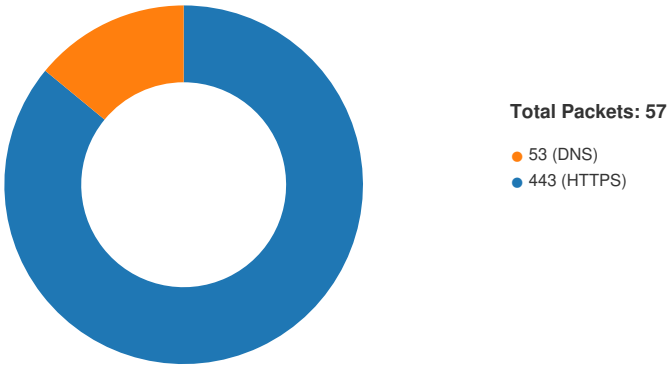
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (62367), with CRLF line terminators
Entropy (8bit):	6.141867962985458
TrID:	• HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11001/1) 18.97%
File name:	Paid_invoice.html
File size:	78674
MD5:	388cd3eda11c1e4a18b95934c94e4751
SHA1:	fc6c35aaefc9671149387530a875c2e2a350a5d2
SHA256:	0b81b708477c44bb04dd7bb0ed927d4ce8a3c7d9e11882542ab84f89bd167bb1
SHA512:	54599e09c1afad9771d473bd5e52cdeb5d29fa0be335116464db82364187a399444581aeb0d6d34c18775beb8f931765deeb221bd0dad4e6f739c56455d20f4d
SSDEEP:	1536:6oDLblS0ldSbAWeOuuRisEflunmYs4yMZ5NsOSdPzsGEJa:6o/blZuRGH1Merwa
TLSH:	C1739DB4D3809917085C1F53F62AB9ADFE2D41E389C0978F725C7A4EDBF5216A046633
File Content Preview:	<html lang="en">....<head>.. <meta http-equiv="x-ua-compatible" content="EmulateIE9">.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. <link rel="stylesheet" href="https://maxc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:57:56.942137957 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:56.942197084 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:56.942315102 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:56.942790985 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:56.942820072 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.010298014 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.023806095 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.023866892 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.024668932 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.024770021 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.025784016 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.025876045 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.134499073 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.134557009 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.134654045 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.135030985 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.135092974 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.218238115 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.218663931 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.218710899 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.220546961 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.220649004 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.417860031 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.417886972 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.418237925 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.418584108 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.418618917 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.418858051 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.419173956 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.419198990 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.419708967 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.419730902 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.456307888 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.456458092 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.456511974 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.456758976 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.456849098 CET	49708	443	192.168.2.5	142.250.203.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:57:57.460422039 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.465223074 CET	49708	443	192.168.2.5	142.250.203.110
Nov 29, 2022 21:57:57.465277910 CET	443	49708	142.250.203.110	192.168.2.5
Nov 29, 2022 21:57:57.493501902 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.493872881 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:57.493973970 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.509069920 CET	49709	443	192.168.2.5	172.217.168.45
Nov 29, 2022 21:57:57.509088993 CET	443	49709	172.217.168.45	192.168.2.5
Nov 29, 2022 21:57:59.205550909 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.205616951 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.205744028 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.288131952 CET	49713	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.288213968 CET	443	49713	104.17.24.14	192.168.2.5
Nov 29, 2022 21:57:59.288300037 CET	49713	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.300245047 CET	49715	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.300309896 CET	443	49715	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.300394058 CET	49715	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.300575018 CET	49716	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.300612926 CET	443	49716	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.300690889 CET	49716	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.301100969 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.301177025 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.301862001 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.301940918 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.302035093 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.302679062 CET	49719	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.302722931 CET	443	49719	104.17.24.14	192.168.2.5
Nov 29, 2022 21:57:59.302795887 CET	49719	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.303651094 CET	49713	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.303688049 CET	443	49713	104.17.24.14	192.168.2.5
Nov 29, 2022 21:57:59.304414034 CET	49715	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.304441929 CET	443	49715	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.304712057 CET	49716	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.304739952 CET	443	49716	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.304944992 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.304997921 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.309693098 CET	49719	443	192.168.2.5	104.17.24.14
Nov 29, 2022 21:57:59.309726000 CET	443	49719	104.17.24.14	192.168.2.5
Nov 29, 2022 21:57:59.510745049 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.511288881 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.511338949 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.513060093 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.513261080 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.532004118 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.533544064 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.533590078 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.536725044 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.536830902 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.547540903 CET	443	49716	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.572252035 CET	49716	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.572288990 CET	443	49716	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.572520018 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.572575092 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.573031902 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.573493004 CET	49711	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.573554993 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.573827982 CET	49717	443	192.168.2.5	104.18.11.207
Nov 29, 2022 21:57:59.573865891 CET	443	49717	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.573880911 CET	49711	443	192.168.2.5	104.18.11.207

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:57:59.573889971 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.573909044 CET	443	49711	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.575622082 CET	443	49716	104.18.11.207	192.168.2.5
Nov 29, 2022 21:57:59.575694084 CET	49716	443	192.168.2.5	104.18.11.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:57:56.825531960 CET	65323	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:56.827173948 CET	51484	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:56.853432894 CET	53	51484	8.8.8.8	192.168.2.5
Nov 29, 2022 21:57:56.853494883 CET	53	65323	8.8.8.8	192.168.2.5
Nov 29, 2022 21:57:58.987894058 CET	55039	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:58.991000891 CET	60975	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:59.002558947 CET	59220	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:59.010333061 CET	53	55039	8.8.8.8	192.168.2.5
Nov 29, 2022 21:57:59.021431923 CET	56682	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:57:59.024481058 CET	53	59220	8.8.8.8	192.168.2.5
Nov 29, 2022 21:57:59.044281960 CET	53	56682	8.8.8.8	192.168.2.5
Nov 29, 2022 21:58:00.655205965 CET	58581	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:58:00.673170090 CET	53	58581	8.8.8.8	192.168.2.5
Nov 29, 2022 21:59:00.716061115 CET	53555	53	192.168.2.5	8.8.8.8
Nov 29, 2022 21:59:00.733777046 CET	53	53555	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 21:57:56.825531960 CET	192.168.2.5	8.8.8.8	0xdf57	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:56.827173948 CET	192.168.2.5	8.8.8.8	0xffe3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:58.987894058 CET	192.168.2.5	8.8.8.8	0x2da3	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:58.991000891 CET	192.168.2.5	8.8.8.8	0xb143	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.002558947 CET	192.168.2.5	8.8.8.8	0x632a	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.021431923 CET	192.168.2.5	8.8.8.8	0xeecc	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:58:00.655205965 CET	192.168.2.5	8.8.8.8	0x40b1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:59:00.716061115 CET	192.168.2.5	8.8.8.8	0xc040	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
Nov 29, 2022 21:57:56.853432894 CET	8.8.8.8	192.168.2.5	0xffe3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:57:56.853432894 CET	8.8.8.8	192.168.2.5	0xffe3	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:56.853494883 CET	8.8.8.8	192.168.2.5	0xdf57	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.009727001 CET	8.8.8.8	192.168.2.5	0xb143	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:57:59.010333061 CET	8.8.8.8	192.168.2.5	0x2da3	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.010333061 CET	8.8.8.8	192.168.2.5	0x2da3	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false

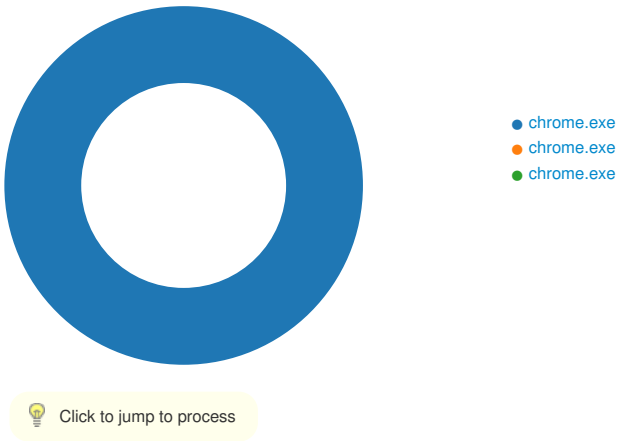
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 21:57:59.024481058 CET	8.8.8.8	192.168.2.5	0x632a	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.024481058 CET	8.8.8.8	192.168.2.5	0x632a	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.044281960 CET	8.8.8.8	192.168.2.5	0xeecc	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:57:59.044281960 CET	8.8.8.8	192.168.2.5	0xeecc	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:58:00.673170090 CET	8.8.8.8	192.168.2.5	0x40b1	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:59:00.733777046 CET	8.8.8.8	192.168.2.5	0xc040	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- maxcdn.bootstrapcdn.com
- stackpath.bootstrapcdn.com
- cdnjs.cloudflare.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5044, Parent PID: 160

General

Target ID:	2
Start time:	21:57:53
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5776**, Parent PID: **5044**

General

Target ID:	3
Start time:	21:57:54
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1756 --field-trial-handle=1648,i,9583188458170825095,14417365062387772299,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6244**, Parent PID: **160**

General

Target ID:	4

Start time:	21:57:55
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Paid_invoice.html
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly