ID: 800699
Sample Name: Remittance.htm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 18:21:36
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

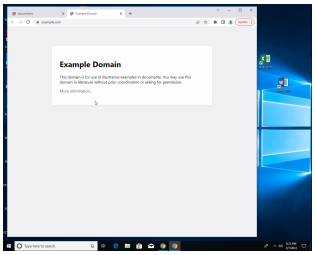
Windows Analysis Report

Remittance.htm

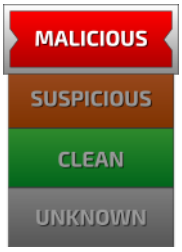
Overview

General Information

Sample Name:	Remittance.htm
Analysis ID:	800699
MD5:	39bb32548e89…
SHA1:	e70af8a69f739…
SHA256:	bf0f39c7f991c7…
Infos:	



Detection

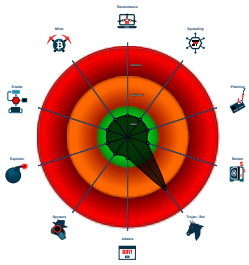


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Performs DNS queries to domains w…
- HTML document with suspicious na…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2528 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4492 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=1952 --field-trial-handle=1812,i,6925232024119698065,536351442840031,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4844 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Remittance.htm MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **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

Networking

Performs DNS queries to domains with low reputation

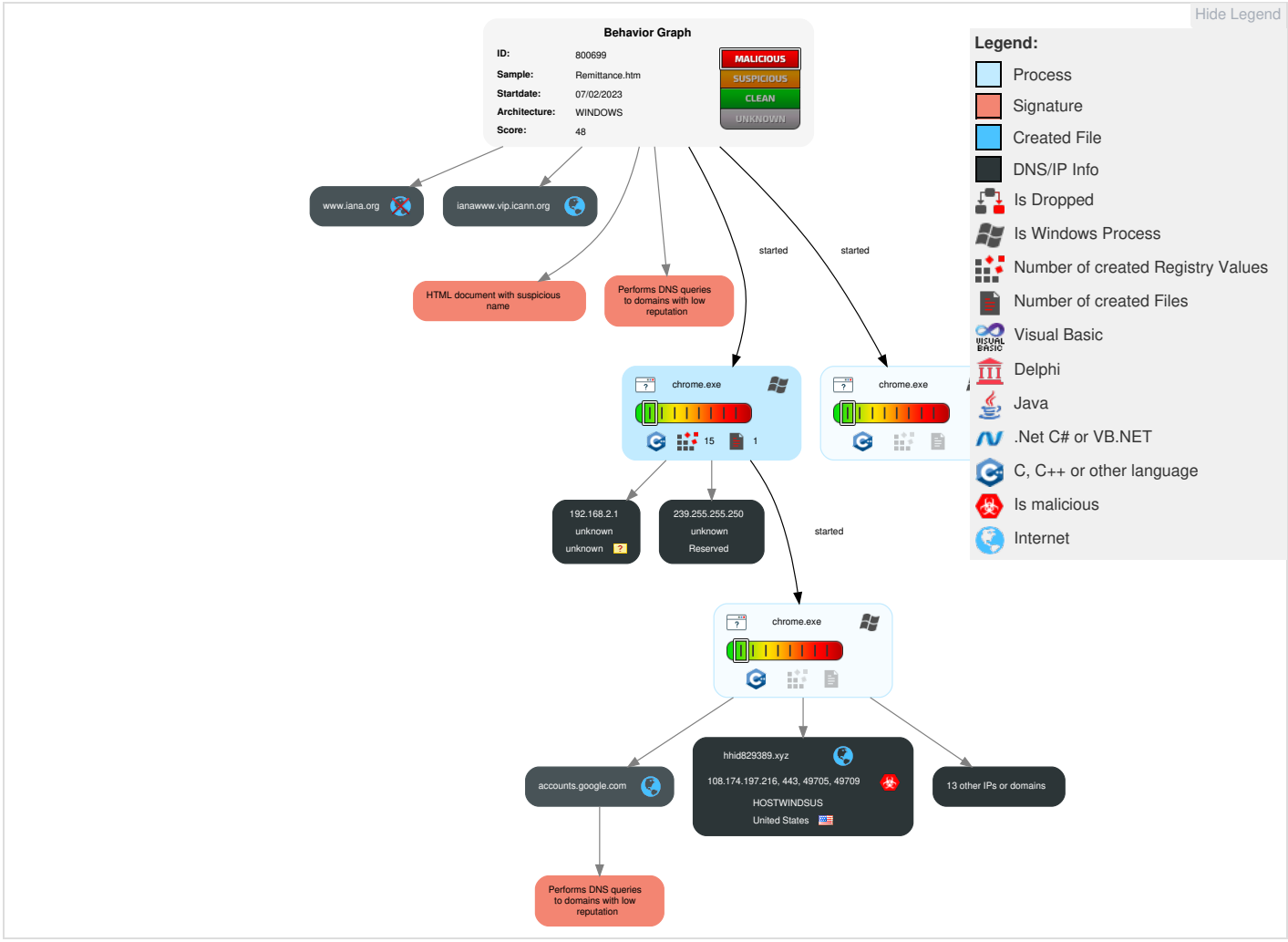
System Summary

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	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	5 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	6 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	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

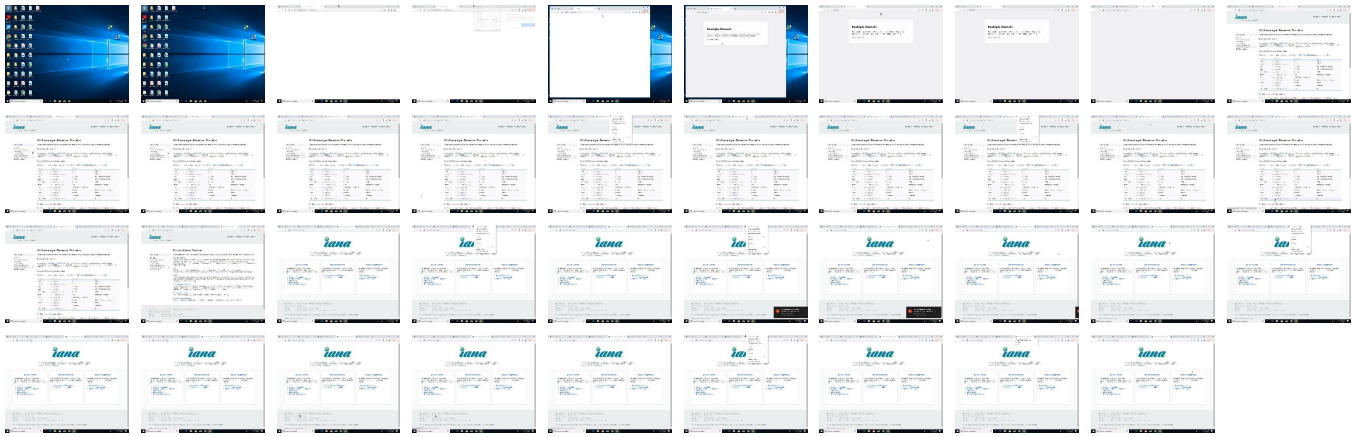
Behavior Graph

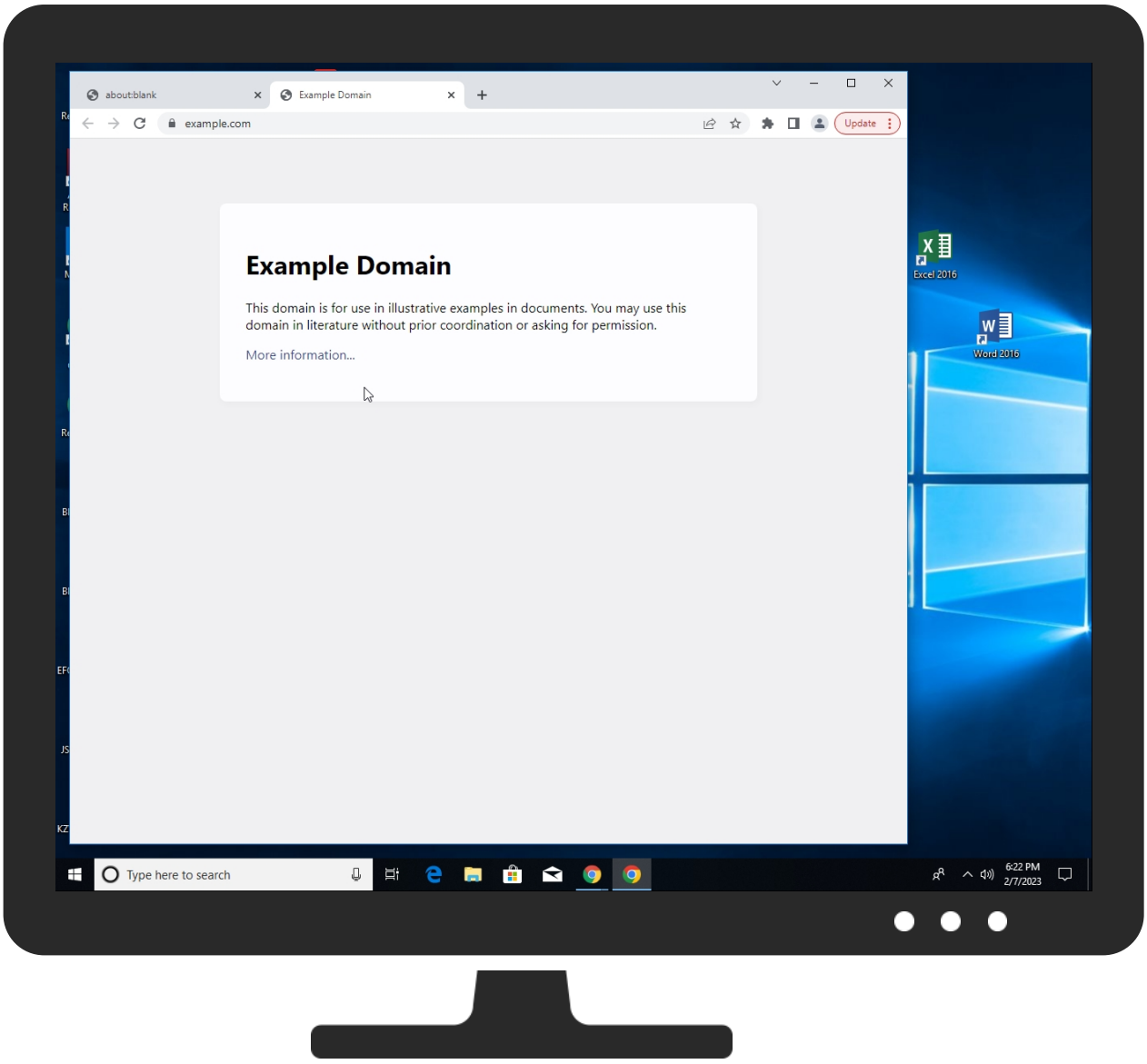


Screenshots

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://https://hhid829389.xyz/?aoul&qrc=glenn.walker	0%	Avira URL Cloud	safe	
http://https://hhid829389.xyz/?aoul&qrc=glenn.walker@cra-arc.gc.ca	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hhid829389.xyz	108.174.197.216	true	true		unknown
accounts.google.com	216.58.209.45	true	false		high
cse.google.com	142.250.180.174	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
example.com	93.184.216.34	true	false		high
ianawww.vip.icann.org	192.0.46.8	true	false		high
href.li	192.0.78.27	true	false		high
www.vip.icann.org	192.0.47.7	true	false		high
clients2.google.com	unknown	unknown	false		high
www.iana.org	unknown	unknown	false		high
pti.icann.org	unknown	unknown	false		high
www.icann.org	unknown	unknown	false		high

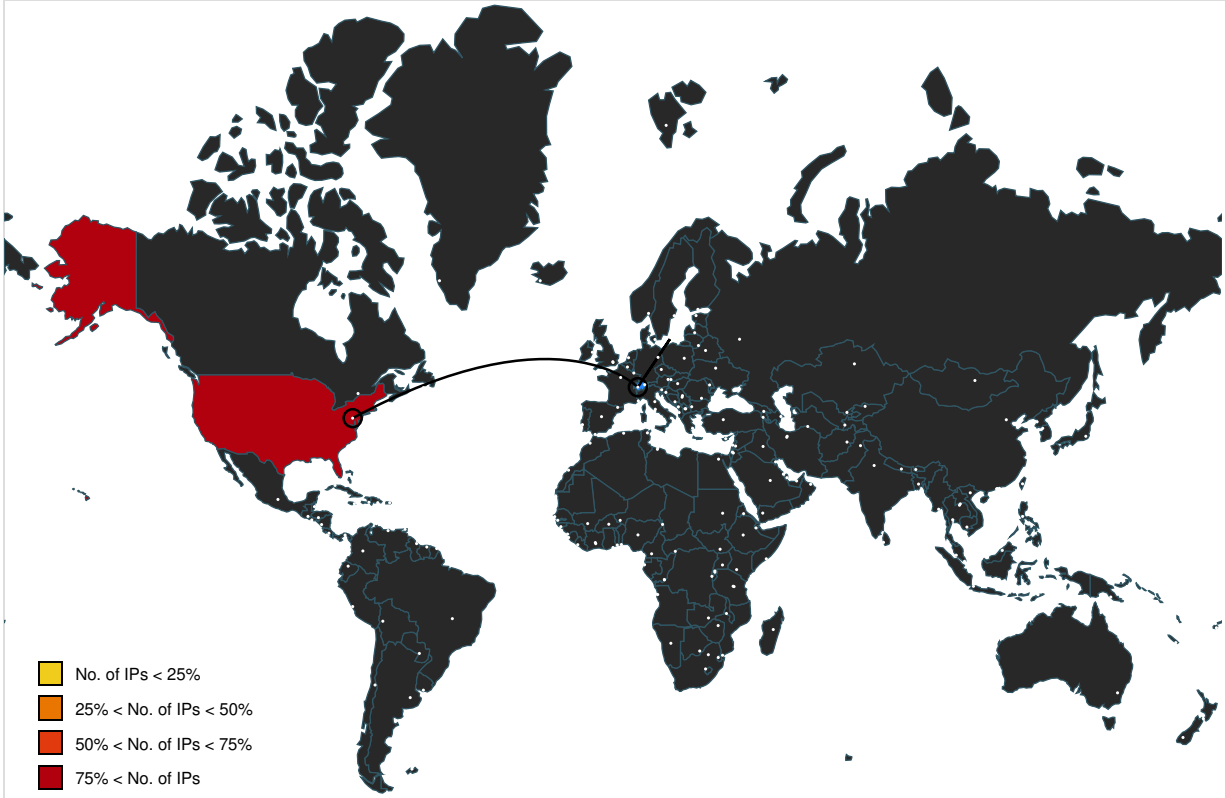
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.iana.org/_img/2022/fonts/SourceCodePro-Regular.woff	false		high
http://https://cse.google.com/cse.js?cx=010470622406686203020:boq_dnseony	false		high
http://https://www.iana.org/_img/2022/iana-logo-header.svg	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://www.iana.org/domains/reserved	false		high
http://https://www.google.com/sorry/index?continue=https://cse.google.com/cse.js%3Fcx%3D010470622406686203020:boq_dnseony&q=EgRUETQNGIOSip8GIjBwZeFx4kuwKO0Anr2hOl6B0Jhv87WwRGnV_yxI1B3AmVgNsivYUqSS_Jg7ekQ9qP0yAXI	false		high
http://https://www.iana.org/_img/bookmark_icon.ico	false		high
http://https://www.iana.org/_css/2022/iana_website.css	false		high
http://www.iana.org/_img/bookmark_icon.ico	false		high
http://www.iana.org/	false		high
http://www.iana.org/domains	false		high
http://www.iana.org/	false		high
http://https://www.iana.org/_img/2022/fonts/NotoSans-Bold.woff	false		high
http://www.iana.org/domains/reserved	false		high
http://https://example.com/	false		high
http://https://href.li/?https://example.com	false		high
http://https://www.iana.org/_js/iana.js	false		high
http://https://www.iana.org/_img/2022/fonts/NotoSans-Regular.woff	false		high
http://https://example.com/favicon.ico	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=104.0.5112.81&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://www.iana.org/_img/2022/iana-logo-header.svg	false		high
http://https://www.iana.org/domains/example	false		high
http://https://www.iana.org/_img/2015.1/iana-logo-homepage.svg	false		high
http://https://www.iana.org/_js/jquery.js	false		high
http://https://example.com/	false		high
http://https://hhid829389.xyz/?aoul&qrc=glenn.walker@cra-arc.gc.ca	false	• Avira URL Cloud: safe	unknown
http://www.iana.org/domains	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hhid829389.xyz/?aoul&qrc=glenn.walker	Remittance.htm	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.46.8	ianawww.vip.icann.org	United States		16876	ICANN-DCUS	false
93.184.216.34	example.com	European Union		15133	EDGECASTUS	false
108.174.197.216	hhid829389.xyz	United States		54290	HOSTWINDSUS	true
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
192.0.78.27	href.li	United States		2635	AUTOMATTICUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	cse.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800699
Start date and time:	2023-02-07 18:21:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	9
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:	Remittance.htm
Detection:	MAL
Classification:	mal48.troj.winHTM@35/0@17/10
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: .htm • Browse: https://www.iana.org/domains/example • Browse: http://www.iana.org/ • Browse: http://www.iana.org/domains

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.163
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, edgedl.me.gvt1.com, login.live.com, tile-service.weather.microsoft.com, update.googleapis.com, ctldl.windowsupdate.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

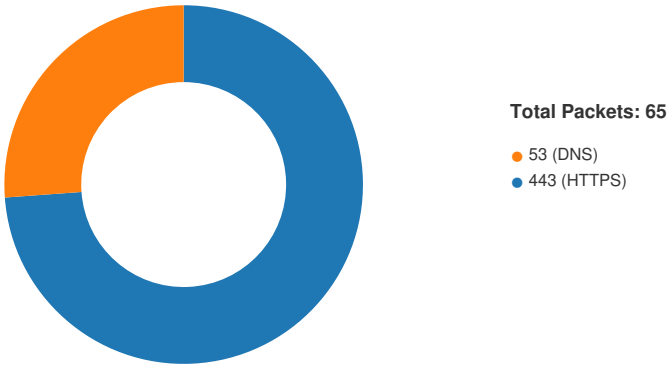
Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	5.255051358476731
TrID:	• HyperText Markup Language (15015/1) 100.00%
File name:	Remittance.htm
File size:	225
MD5:	39bb32548e89f58ceb6960e84791979e
SHA1:	e70af8a69f739dc0501013a1a9ebb5f4cef552e2
SHA256:	bf0f39c7f991c76bbd138e4d74dc9cc402aca673c5edd8b6005dc41faf739208
SHA512:	18764d29c900701e18f6d7b0cf3c9fd59c0cd1a0baab510062a28e91755b5503f1bd979e720d00524ffb0d1c213b30a36a89b22e152cdf9005f925fac4c621b4
SSDEEP:	6:h4QWqqMzSKcAIK7UK+oSPNKDVjgnEzcTi/MWXfGb:hPlzSb1K0NwVsEzcu/MWPGb
TLSH:	7AD0A7EB3C50DD056971ACF45C75E22C94B7B2C45E96E217D4C4792B15203B89D471CE
File Content Preview:	<!DOCTYPE html>..<html>..<body>..<script>..// Javascript URL redirection - generated by www.rapidtables.com..window.location.replace("https://hhid829389.xyz/?aoul&qrc=glenn.walker@cra-arc.gc.ca");..</script>..</body>..</html>

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:37.691319942 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.691380024 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:37.691392899 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:37.691487074 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:37.691525936 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.691601992 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:37.692004919 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.692030907 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:37.692116976 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.987829924 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:37.987891912 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:37.987996101 CET	49707	443	192.168.2.5	216.58.209.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:37.988661051 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.988682985 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:37.988743067 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.989568949 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.989614010 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:37.990034103 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.990087032 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:37.990170002 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.990416050 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:37.990466118 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:37.990911961 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.990940094 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:37.991348982 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:37.991374016 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:37.991632938 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:37.991652966 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:37.991877079 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:37.991902113 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.138591051 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.159660101 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.159723043 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.160851955 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.160969973 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.163341045 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.163414001 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.166472912 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.196099043 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.198189974 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.233935118 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.291367054 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.291383982 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.296061039 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.363872051 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.379285097 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.379317045 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.379832029 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:38.379885912 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.380006075 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:38.380048990 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.380188942 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.380203962 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.380378008 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.380405903 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.380817890 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.380866051 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.380903006 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.381345034 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.381370068 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.381409883 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:38.381949902 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.382010937 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.382051945 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:38.382292986 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:38.382379055 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:38.382539988 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.382594109 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:38.382613897 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.383281946 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.383364916 CET	49702	443	192.168.2.5	142.250.180.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:38.383384943 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:38.433386087 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.491400003 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:38.491403103 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:38.491410971 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:39.280591965 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:39.280657053 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:39.280733109 CET	49702	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:39.280792952 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:39.281105042 CET	443	49702	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:39.281104088 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:39.281294107 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:39.281342983 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:39.281559944 CET	49705	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:39.281610012 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:39.281779051 CET	49708	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:22:39.281809092 CET	443	49708	142.250.180.174	192.168.2.5
Feb 7, 2023 18:22:39.281836987 CET	443	49705	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:39.281837940 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:39.282054901 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:39.282099962 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:39.282169104 CET	49707	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:39.282188892 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:39.282314062 CET	443	49707	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:39.282712936 CET	443	49703	216.58.209.45	192.168.2.5
Feb 7, 2023 18:22:39.287015915 CET	49709	443	192.168.2.5	108.174.197.216
Feb 7, 2023 18:22:39.287077904 CET	443	49709	108.174.197.216	192.168.2.5
Feb 7, 2023 18:22:39.287311077 CET	49703	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:22:39.287374020 CET	443	49703	216.58.209.45	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:22:36.930655003 CET	49724	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:36.930768967 CET	61452	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:36.930810928 CET	65323	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:36.948674917 CET	53	49724	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:36.958616972 CET	53	61452	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:36.958682060 CET	53	65323	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:39.745507956 CET	55039	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:39.763851881 CET	53	55039	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:41.076035023 CET	59220	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:41.095607996 CET	53	59220	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:41.445427895 CET	55068	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:41.464953899 CET	53	55068	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:53.454372883 CET	56263	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:53.474816084 CET	53	56263	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:56.124258041 CET	64419	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:56.142252922 CET	53	64419	8.8.8.8	192.168.2.5
Feb 7, 2023 18:22:56.820790052 CET	61344	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:22:57.012938976 CET	53	61344	8.8.8.8	192.168.2.5
Feb 7, 2023 18:23:06.101645947 CET	60284	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:06.121783018 CET	53	60284	8.8.8.8	192.168.2.5
Feb 7, 2023 18:23:15.503917933 CET	53555	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:15.522234917 CET	53	53555	8.8.8.8	192.168.2.5
Feb 7, 2023 18:23:39.830362082 CET	58872	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:39.848680973 CET	53	58872	8.8.8.8	192.168.2.5
Feb 7, 2023 18:23:55.121695995 CET	51972	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:55.141412973 CET	53	51972	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:23:58.891067028 CET	55726	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:58.891454935 CET	57924	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:23:58.911197901 CET	53	57924	8.8.8.8	192.168.2.5
Feb 7, 2023 18:23:59.056502104 CET	53	55726	8.8.8.8	192.168.2.5
Feb 7, 2023 18:25:00.620471001 CET	61797	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:25:00.638747931 CET	53	61797	8.8.8.8	192.168.2.5
Feb 7, 2023 18:25:39.995788097 CET	52874	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:25:40.015918016 CET	53	52874	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
Feb 7, 2023 18:22:36.930655003 CET	192.168.2.5	8.8.8.8	0xe34e	Standard query (0)	hhid829389.xyz	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:36.930768967 CET	192.168.2.5	8.8.8.8	0x5cf3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:36.930810928 CET	192.168.2.5	8.8.8.8	0xe230	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:39.745507956 CET	192.168.2.5	8.8.8.8	0xe70	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:41.076035023 CET	192.168.2.5	8.8.8.8	0xd5cf	Standard query (0)	href.li	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:41.445427895 CET	192.168.2.5	8.8.8.8	0xd3a0	Standard query (0)	example.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:53.454372883 CET	192.168.2.5	8.8.8.8	0xd346	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:56.124258041 CET	192.168.2.5	8.8.8.8	0x7e39	Standard query (0)	www.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:56.820790052 CET	192.168.2.5	8.8.8.8	0x62e4	Standard query (0)	pti.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:06.101645947 CET	192.168.2.5	8.8.8.8	0x3186	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:15.503917933 CET	192.168.2.5	8.8.8.8	0xef68	Standard query (0)	cse.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:39.830362082 CET	192.168.2.5	8.8.8.8	0xc764	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:55.121695995 CET	192.168.2.5	8.8.8.8	0x4755	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:58.891067028 CET	192.168.2.5	8.8.8.8	0xe243	Standard query (0)	pti.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:58.891454935 CET	192.168.2.5	8.8.8.8	0xa7bb	Standard query (0)	www.icann.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:25:00.620471001 CET	192.168.2.5	8.8.8.8	0x10d3	Standard query (0)	www.iana.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:25:39.995788097 CET	192.168.2.5	8.8.8.8	0x7e89	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
Feb 7, 2023 18:22:36.948674917 CET	8.8.8.8	192.168.2.5	0xe34e	No error (0)	hhid829389.xyz		108.174.197.216	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:36.958616972 CET	8.8.8.8	192.168.2.5	0x5cf3	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:36.958682060 CET	8.8.8.8	192.168.2.5	0xe230	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:36.958682060 CET	8.8.8.8	192.168.2.5	0xe230	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:39.763851881 CET	8.8.8.8	192.168.2.5	0xe70	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:41.095607996 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	href.li		192.0.78.27	A (IP address)	IN (0x0001)	false

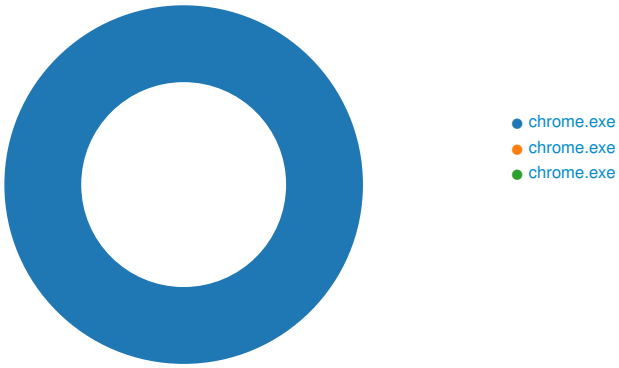
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:22:41.095607996 CET	8.8.8.8	192.168.2.5	0xd5cf	No error (0)	href.li		192.0.78.26	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:41.464953899 CET	8.8.8.8	192.168.2.5	0xd3a0	No error (0)	example.com		93.184.216.34	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:53.474816084 CET	8.8.8.8	192.168.2.5	0xd346	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:53.474816084 CET	8.8.8.8	192.168.2.5	0xd346	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:56.142252922 CET	8.8.8.8	192.168.2.5	0x7e39	No error (0)	www.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:56.142252922 CET	8.8.8.8	192.168.2.5	0x7e39	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:22:57.012938976 CET	8.8.8.8	192.168.2.5	0x62e4	No error (0)	pti.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:22:57.012938976 CET	8.8.8.8	192.168.2.5	0x62e4	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:06.121783018 CET	8.8.8.8	192.168.2.5	0x3186	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:06.121783018 CET	8.8.8.8	192.168.2.5	0x3186	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:15.522234917 CET	8.8.8.8	192.168.2.5	0xef68	No error (0)	cse.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:39.848680973 CET	8.8.8.8	192.168.2.5	0xc764	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:55.141412973 CET	8.8.8.8	192.168.2.5	0x4755	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:55.141412973 CET	8.8.8.8	192.168.2.5	0x4755	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:58.911197901 CET	8.8.8.8	192.168.2.5	0xa7bb	No error (0)	www.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:58.911197901 CET	8.8.8.8	192.168.2.5	0xa7bb	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:23:59.056502104 CET	8.8.8.8	192.168.2.5	0xe243	No error (0)	pti.icann.org	www.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:23:59.056502104 CET	8.8.8.8	192.168.2.5	0xe243	No error (0)	www.vip.icann.org		192.0.47.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:25:00.638747931 CET	8.8.8.8	192.168.2.5	0x10d3	No error (0)	www.iana.org	ianawww.vip.icann.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:25:00.638747931 CET	8.8.8.8	192.168.2.5	0x10d3	No error (0)	ianawww.vip.icann.org		192.0.46.8	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:25:40.015918016 CET	8.8.8.8	192.168.2.5	0x7e89	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- hhid829389.xyz
- accounts.google.com
- href.li
- example.com
- https:
  - www.iana.org
- cse.google.com
- www.google.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **2528**, Parent PID: **2868**

General

Target ID:	0
Start time:	18:22:32
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "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: **4492**, Parent PID: **2528**

General

Target ID:	1
Start time:	18:22:34
Start date:	07/02/2023
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=1952 --field-trial-handle=1812,i,6925232024119698065,536351442840031,131072 --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: **4844**, Parent PID: **2868**

General

Target ID:	2
Start time:	18:22:35
Start date:	07/02/2023
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\Remittance.htm
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