ID: 756306
Sample Name: NEW VOICEMAIL _MP3_.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 00:27:07
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

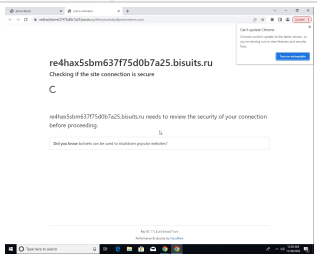
Windows Analysis Report

NEW VOICEMAIL _MP3_.html

Overview

General Information

Sample Name:	NEW VOICEMAIL _MP3_.html
Analysis ID:	756306
MD5:	29aad7a1fd0284..
SHA1:	18e6e964239d3e.
SHA256:	5afd73eb3bb765..
Infos:	



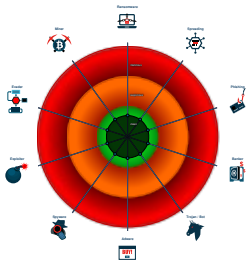
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML document with suspicious na…
- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2008 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5396 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=1980 --field-trial-handle=1776,i,9362262813609904554,7029340453842893064,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4304 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\NEW VOICEMAIL _MP3_.html 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

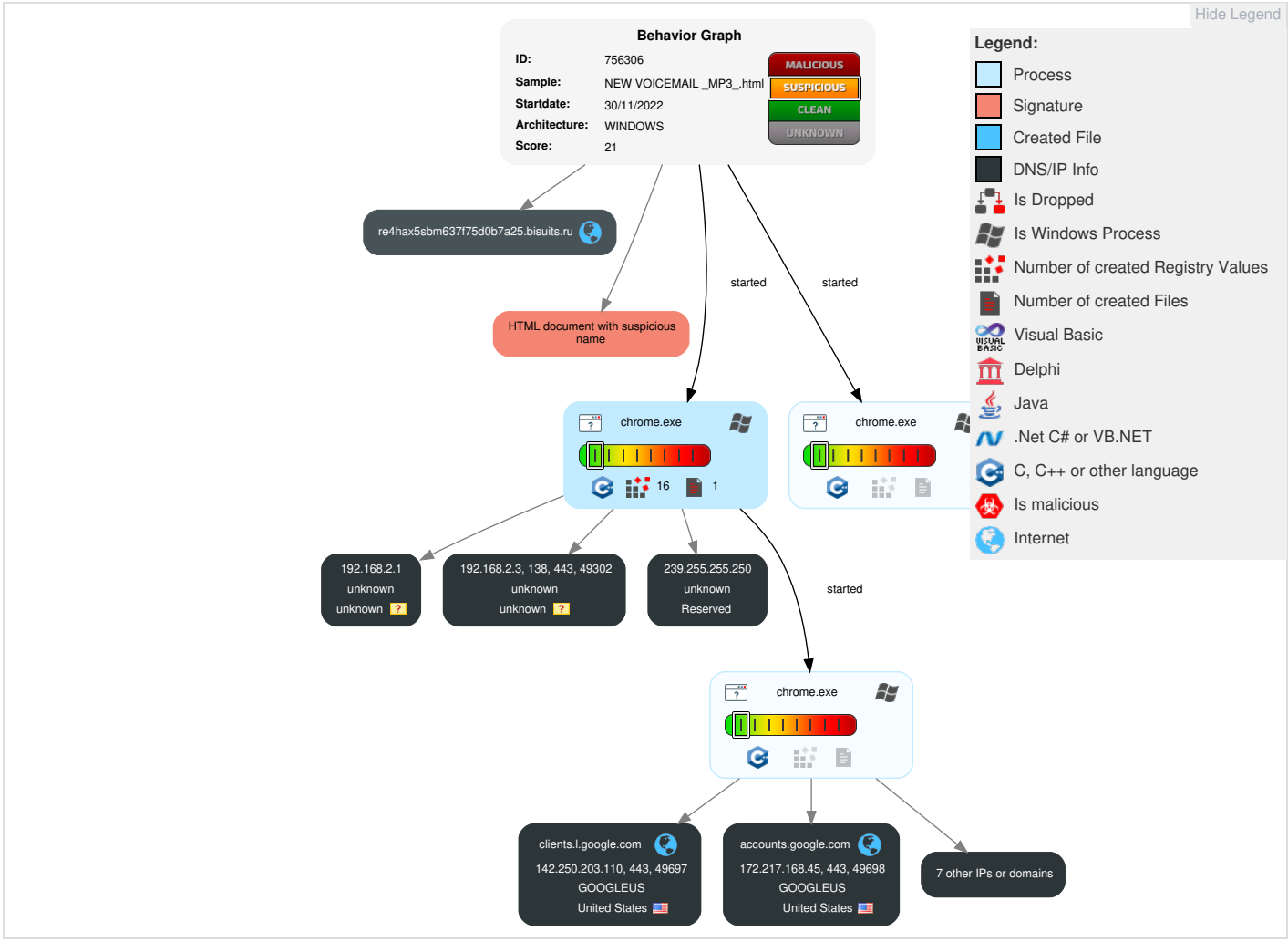
System Summary

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

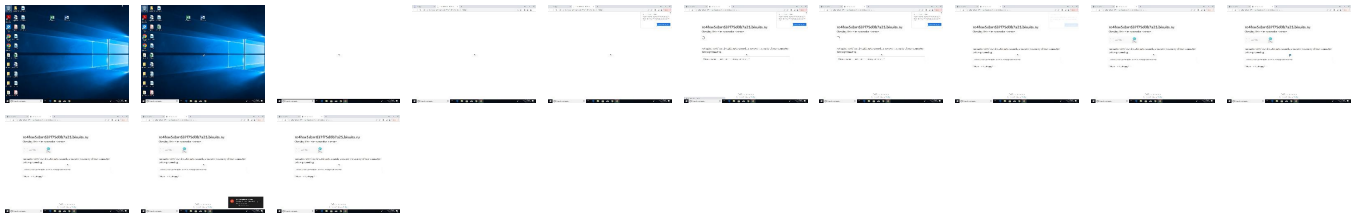
Behavior Graph

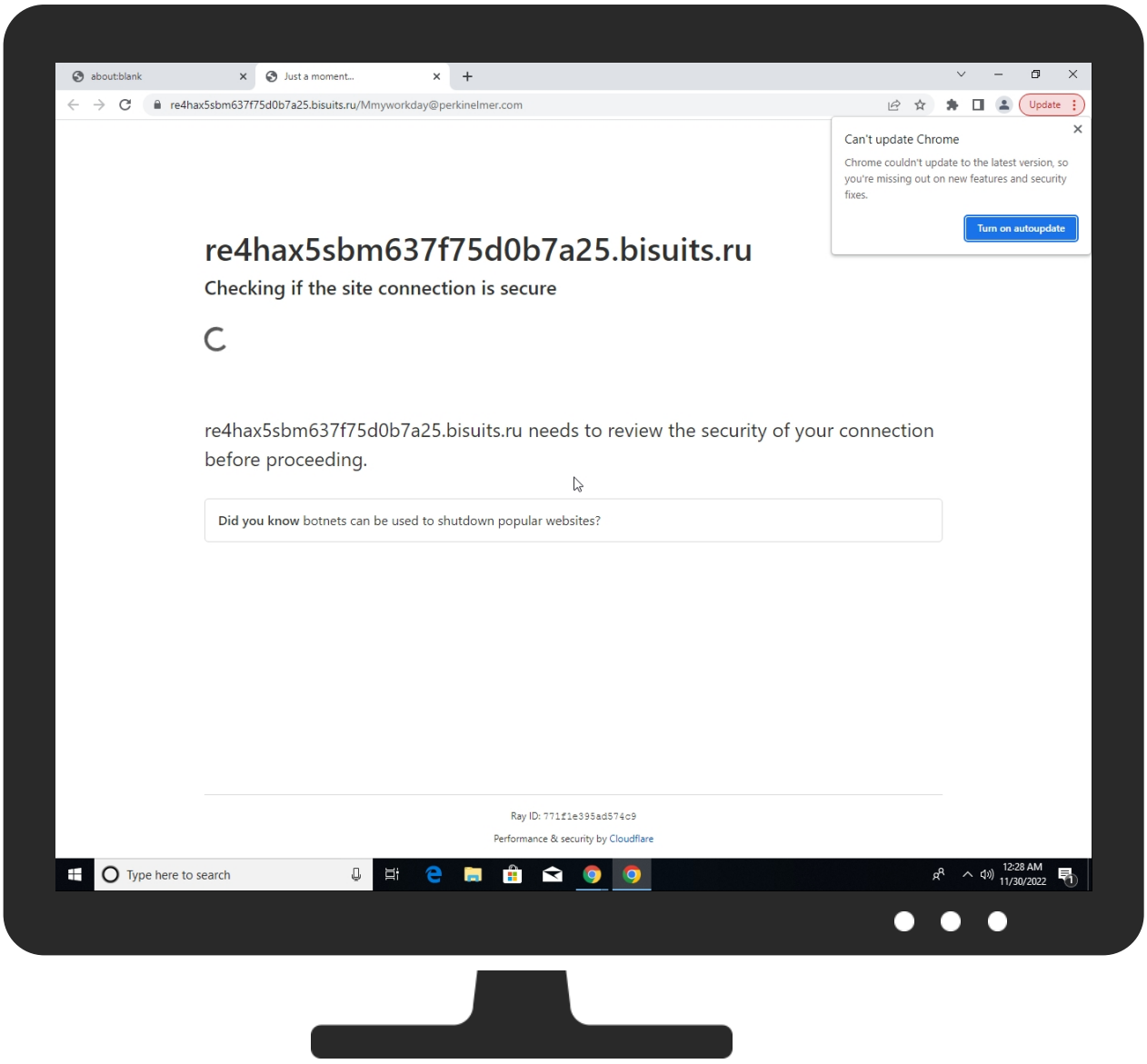


Screenshots

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://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=771f1e395ad574c9	0%	Avira URL Cloud	safe	
http://https://cloudflare.hcaptcha.com/checksiteconfig?v=d22dff0&host=re4hax5sbm637f75d0b7a25.bisuits.ru&sitekey=f9630567-8bfa-4fc9-8ee5-9c91c6276dff&sc=1&swa=1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/favicon.ico	0%	Avira URL Cloud	safe	
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/pat/771f1e395ad574c9/1669764490065/70c127170de94576b20f07b4248fb1f262d858ff026334d7edf50eeeb7d76436/_VQHvkJ6RIcB0xC	0%	Avira URL Cloud	safe	
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/img/771f1e395ad574c9/1669764490070/Fpo3sw4SytnVdaS	0%	Avira URL Cloud	safe	
http://https://cf-assets.hcaptcha.com/i/b4b4ffc/e	0%	Avira URL Cloud	safe	
http://https://cf-assets.hcaptcha.com/c/b4b4ffc/hsw.js	0%	Avira URL Cloud	safe	
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/flow/ov1/0.6395875432093886:1669759612:dbfPBAq4NWU--uGkziogIkMzGLFKirW4VMDN-_Huw28/771f1e395ad574c9/f6c7e8e13b37a36	0%	Avira URL Cloud	safe	
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/hcaptcha.js	0%	Avira URL Cloud	safe	
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/styles/challenges.css	0%	Avira URL Cloud	safe	
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1?ray=771f1e395ad574c9	0%	Avira URL Cloud	safe	
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/static/hcaptcha.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

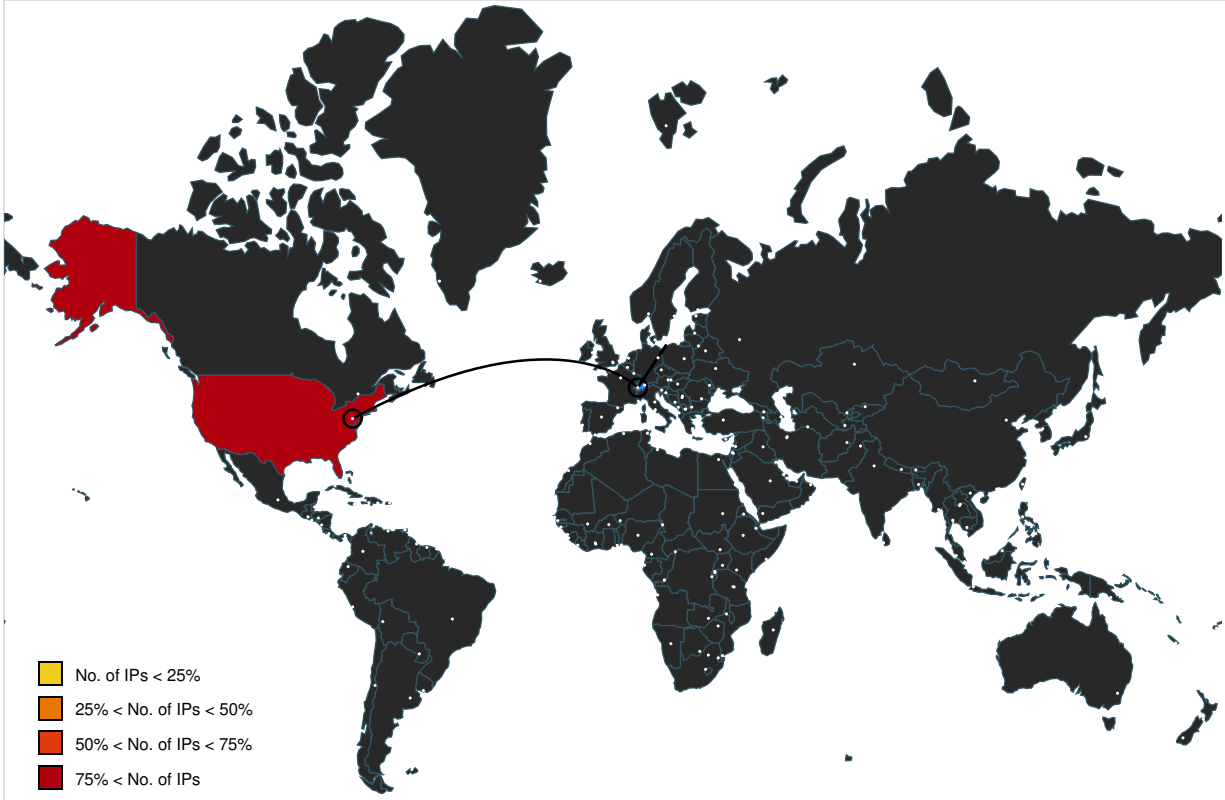
Name	IP	Active	Malicious	Antivirus Detection	Reputation
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	172.217.168.45	true	false		high
re4hax5sbm637f75d0b7a25.bisuits.ru	172.67.177.105	true	false		unknown
cf-assets.hcaptcha.com	104.18.23.122	true	false		unknown
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
cloudflare.hcaptcha.com	104.18.18.132	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=771f1e395ad574c9	false	• Avira URL Cloud: safe	unknown
http://https://cloudflare.hcaptcha.com/checksiteconfig?v=d22dff0&host=re4hax5sbm637f75d0b7a25.bisuits.ru&sitekey=f9630567-8bfa-4fc9-8ee5-9c91c6276dff&sc=1&swa=1	false	• Avira URL Cloud: safe	unknown
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/pat/771f1e395ad574c9/1669764490065/70c127170de94576b20f07b4248fb1f262d858ff026334d7edf50eeeb7d76436/_VQHvkJ6RIcB0xC	false	• Avira URL Cloud: safe	unknown
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/Mmyworkday@perkinelmer.com	false		unknown
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/static/hcaptcha.html#frame=checkbox&id=0m0rrtd2ktu&host=re4hax5sbm637f75d0b7a25.bisuits.ru&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=off&custom=false&endpoint=https%3A%2F%2Fcloudflare.hcaptcha.com&hl=en&assethost=https%3A%2F%2Fcf-assets.hcaptcha.com&imghost=https%3A%2F%2Fcf-imgs.hcaptcha.com&tplinks=on&sitekey=f9630567-8bfa-4fc9-8ee5-9c91c6276dff&theme=light&origin=https%3A%2F%2Fre4hax5sbm637f75d0b7a25.bisuits.ru	false		unknown
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/Mmyworkday@perkinelmer.com	false		unknown
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://cf-assets.hcaptcha.com/captcha/v1/d22dff0/static/hcaptcha.html#frame=challenge&id=0m0rrtd2ktu&host=re4hax5sbm637f75d0b7a25.bisuits.ru&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=off&custom=false&endpoint=https%3A%2F%2Fcloudflare.hcaptcha.com&hl=en&assethost=https%3A%2F%2Fcf-assets.hcaptcha.com&imghost=https%3A%2F%2Fcf-imgs.hcaptcha.com&tplinks=on&sitekey=f9630567-8bfa-4fc9-8ee5-9c91c6276dff&theme=light&origin=https%3A%2F%2Fre4hax5sbm637f75d0b7a25.bisuits.ru	false		unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/static/hcaptcha.html#frame=checkbox&id=1fz4ymj8jx8j&host=re4hax5sbm637f75d0b7a25.bisuits.ru&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=off&custom=false&endpoint=https%3A%2F%2Fcloudflare.hcaptcha.com&hl=en&assethost=https%3A%2F%2Fcf-assets.hcaptcha.com&imghost=https%3A%2F%2Fcf-imgs.hcaptcha.com&tplinks=on&sitekey=f9630567-8bfa-4fc9-8ee5-9c91c6276dff&theme=light&origin=https%3A%2F%2Fre4hax5sbm637f75d0b7a25.bisuits.ru	false		unknown
http://https://cf-assets.hcaptcha.com/i/b4b4ffc/e	false	• Avira URL Cloud: safe	unknown
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/img/771f1e395ad574c9/1669764490070/Fpo3sw4SytnVdaS	false	• Avira URL Cloud: safe	unknown
http://https://cf-assets.hcaptcha.com/c/b4b4ffc/hsw.js	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report/v3?s=xTET7Jah2R1LJd9k1OmByfSraqkqYwi8fa%2FYX0RDdE6mC5bct2gy0t9R5bmlJb2h%2Bs4NmTqZPEITfm6jYcEilGveZCY%2BuEg063Nd9fo9cuHk3ZV4%2BZxWxcFDL40H7oQlqu0S1Wm038AbyQYuRiyLGrQPQXOA	false		high
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/flow/ov1/0.6395875432093886:1669759612:dbfPBAq4NWU--uGkziogIkMzGLFKirW4VMDN-_Huw28/771f1e395ad574c9/f6c7e8e13b37a36	false	• Avira URL Cloud: safe	unknown
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/hcaptcha.js	false	• Avira URL Cloud: safe	unknown
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/styles/challenges.css	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report/v3?s=n0s3ihfFR8zpUNvsc1vNdKcV8%2BwZcGoGtktqUkoSavxUUForhD0amYKaIMBf4Yblk3faOZNu9S9YhZnDi8uR6eKzdhPTaGc9WuJID8%2BFCP5AjZObFb7d%2BYuvB4EBXFKNl4SdFB0XLJhDz8R7ZMfYhovr6kvl	false		high
http://https://re4hax5sbm637f75d0b7a25.bisuits.ru/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1?ray=771f1e395ad574c9	false	• Avira URL Cloud: safe	unknown
http://https://cf-assets.hcaptcha.com/captcha/v1/d22dff0/static/hcaptcha.html	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.23.122	cf-assets.hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	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
172.67.177.105	re4hax5sbm637f75d0b7a25.bisuits.ru	United States		13335	CLOUDFLARENETUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.18.132	cloudflare.hcaptcha.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756306
Start date and time:	2022-11-30 00:27:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW VOICEMAIL _MP3_.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:	18
Number of new started drivers analysed:	1
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:	SUS
Classification:	sus21.winHTML@30/0@10/11
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 • Browse: https://www.cloudflare.com/?utm_source=challenge&utm_campaign=m

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, qwavedrv.sys, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 172.217.168.10, 172.217.168.42, 172.217.168.74, 142.250.203.106
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.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

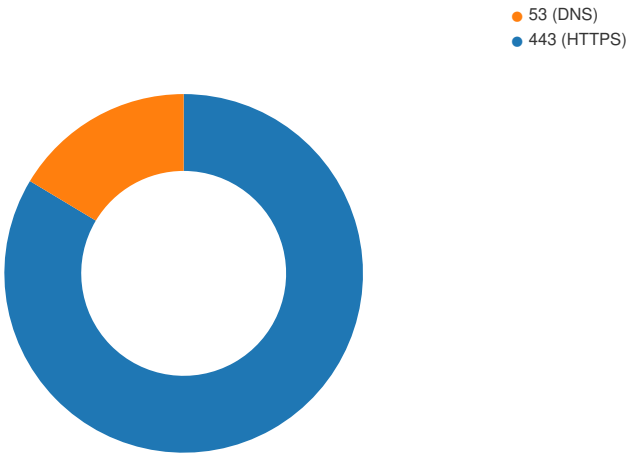
General

File type:	HTML document, ASCII text, with very long lines (30471), with CRLF line terminators
Entropy (8bit):	4.667094027005393
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	NEW VOICEMAIL _MP3_.html
File size:	30626
MD5:	29aad7a1fd02847a742991511818d9ca
SHA1:	18e6e964239d3eab2b684845d55f45c2cf1e458a
SHA256:	5afd73eb3bb765cf65f586dabb6810631a942aeb56d20a8ce6757a1aa0e25db4
SHA512:	8d20d5af483946d5524c4c39dde3f00728b4326cfb631be23e61f457f24ed9848ca581b541d7d075a6a301ecf445c2d699a54758223f77bd0f132a79ba2789e3
SSDEEP:	384:b8Qg6A5nbxsgUsz+zq6l7TCpH8X+tFEW9k71M5YxsxExO7GF37/ay0unIQy44v7B:oQg1sgztWG71SY2IL5/h0o0FYt8
TLSH:	95D223A07717CC524D7AE12FB59E9B66C9190B63CD5E84F633E1820C1BF0B325A825CE
File Content Preview:	<script>..let okay ="myworkday@perkinelmer.com";.... function rect() {... .. ..let m8Bx;!function(){const QaXH=Array.prototype.slice.call(arguments);return eval("(function sYJv(beRn){const DLTn=fjWn(beRn,vBJn(sYJv.toString()));try{let X8Ln=eval(

Network Behavior

Network Port Distribution

Total Packets: 61



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:27:58.444571018 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.444628000 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.444780111 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.445112944 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.445125103 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.511734962 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.512111902 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.512541056 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.512553930 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516519070 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516535997 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516562939 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516583920 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516633987 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516645908 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516706944 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516726971 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516747952 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516849995 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516865969 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516891003 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516925097 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.516931057 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.516963005 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.517163992 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.630098104 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.630182028 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.630201101 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.630247116 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.630286932 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.630302906 CET	443	49696	204.79.197.200	192.168.2.3
Nov 30, 2022 00:27:58.630319118 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:27:58.630438089 CET	49696	443	192.168.2.3	204.79.197.200
Nov 30, 2022 00:28:05.748049021 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.748102903 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.748222113 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.748859882 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.748886108 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.754858971 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:05.754945993 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:05.755047083 CET	49698	443	192.168.2.3	172.217.168.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:28:05.755403042 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:05.755419970 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:05.806772947 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.812022924 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.812060118 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.812717915 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.812828064 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.813546896 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:05.813616991 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:05.883163929 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:05.918404102 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:05.918447018 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:05.921372890 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:05.921468973 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.426573992 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.426616907 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.426728964 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.426749945 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.426922083 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:06.426965952 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.427035093 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.427109957 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.427179098 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:06.427197933 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.464634895 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.464734077 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:06.464768887 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.464787006 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.464838982 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:06.468149900 CET	49697	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:28:06.468208075 CET	443	49697	142.250.203.110	192.168.2.3
Nov 30, 2022 00:28:06.506948948 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.507239103 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.507268906 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.507349014 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:06.507407904 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.534051895 CET	49698	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:28:06.534090996 CET	443	49698	172.217.168.45	192.168.2.3
Nov 30, 2022 00:28:08.454121113 CET	49701	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.454196930 CET	443	49701	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.454282999 CET	49701	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.455014944 CET	49702	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.455079079 CET	443	49702	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.455172062 CET	49702	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.455369949 CET	49701	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.455399990 CET	443	49701	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.455585957 CET	49702	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.455624104 CET	443	49702	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.557035923 CET	443	49702	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.563673019 CET	443	49701	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.631887913 CET	49702	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.668797970 CET	49701	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.845809937 CET	49701	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.845874071 CET	443	49701	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.846355915 CET	49702	443	192.168.2.3	172.67.177.105
Nov 30, 2022 00:28:08.846405983 CET	443	49702	172.67.177.105	192.168.2.3
Nov 30, 2022 00:28:08.847389936 CET	49703	443	192.168.2.3	172.217.168.68
Nov 30, 2022 00:28:08.847445965 CET	443	49703	172.217.168.68	192.168.2.3
Nov 30, 2022 00:28:08.847529888 CET	49703	443	192.168.2.3	172.217.168.68

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:28:05.354523897 CET	49977	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:05.354964018 CET	57840	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:05.375597000 CET	53	49977	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:05.384494066 CET	53	57840	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:08.272850990 CET	49302	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:08.296752930 CET	53	49302	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:08.513886929 CET	53975	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:08.533364058 CET	53	53975	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:09.286120892 CET	60582	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:09.303678036 CET	53	60582	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:09.799643040 CET	57134	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:09.820872068 CET	53	57134	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:14.391242027 CET	55638	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:14.429902077 CET	53	55638	8.8.8.8	192.168.2.3
Nov 30, 2022 00:28:14.603430033 CET	57704	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:28:14.624385118 CET	53	57704	8.8.8.8	192.168.2.3
Nov 30, 2022 00:29:09.423382044 CET	65511	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:29:09.442065001 CET	53	65511	8.8.8.8	192.168.2.3
Nov 30, 2022 00:29:20.756680012 CET	138	138	192.168.2.3	192.168.2.255
Nov 30, 2022 00:30:08.617685080 CET	52079	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:30:08.637743950 CET	53	52079	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:28:05.354523897 CET	192.168.2.3	8.8.8.8	0xc837	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:05.354964018 CET	192.168.2.3	8.8.8.8	0x90b9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:08.272850990 CET	192.168.2.3	8.8.8.8	0x96b1	Standard query (0)	re4hax5sbm637f75d0b7a25.bisuits.ru	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:08.513886929 CET	192.168.2.3	8.8.8.8	0x90d6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:09.286120892 CET	192.168.2.3	8.8.8.8	0xed6f	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:09.799643040 CET	192.168.2.3	8.8.8.8	0x905	Standard query (0)	cloudflare.hcaptcha.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.391242027 CET	192.168.2.3	8.8.8.8	0x827b	Standard query (0)	re4hax5sbm637f75d0b7a25.bisuits.ru	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.603430033 CET	192.168.2.3	8.8.8.8	0x62e1	Standard query (0)	cf-assets.hcaptcha.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:29:09.423382044 CET	192.168.2.3	8.8.8.8	0x1913	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:30:08.617685080 CET	192.168.2.3	8.8.8.8	0x88ab	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 30, 2022 00:28:05.375597000 CET	8.8.8.8	192.168.2.3	0xc837	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:28:05.375597000 CET	8.8.8.8	192.168.2.3	0xc837	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:05.384494066 CET	8.8.8.8	192.168.2.3	0x90b9	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:08.296752930 CET	8.8.8.8	192.168.2.3	0x96b1	No error (0)	re4hax5sbm637f75d0b7a25.bisuits.ru		172.67.177.105	A (IP address)	IN (0x0001)	false

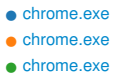
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:28:08.296752930 CET	8.8.8.8	192.168.2.3	0x96b1	No error (0)	re4hax5sbm637f75d0b7a25.bisuits.ru		104.21.43.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:08.533364058 CET	8.8.8.8	192.168.2.3	0x90d6	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:09.303678036 CET	8.8.8.8	192.168.2.3	0xed6f	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:09.820872068 CET	8.8.8.8	192.168.2.3	0x905	No error (0)	cloudflare.hcaptcha.com		104.18.18.132	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:09.820872068 CET	8.8.8.8	192.168.2.3	0x905	No error (0)	cloudflare.hcaptcha.com		104.18.19.132	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.429902077 CET	8.8.8.8	192.168.2.3	0x827b	No error (0)	re4hax5sbm637f75d0b7a25.bisuits.ru		172.67.177.105	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.429902077 CET	8.8.8.8	192.168.2.3	0x827b	No error (0)	re4hax5sbm637f75d0b7a25.bisuits.ru		104.21.43.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.624385118 CET	8.8.8.8	192.168.2.3	0x62e1	No error (0)	cf-assets.hcaptcha.com		104.18.23.122	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:28:14.624385118 CET	8.8.8.8	192.168.2.3	0x62e1	No error (0)	cf-assets.hcaptcha.com		104.18.22.122	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:29:09.442065001 CET	8.8.8.8	192.168.2.3	0x1913	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:30:08.637743950 CET	8.8.8.8	192.168.2.3	0x88ab	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false

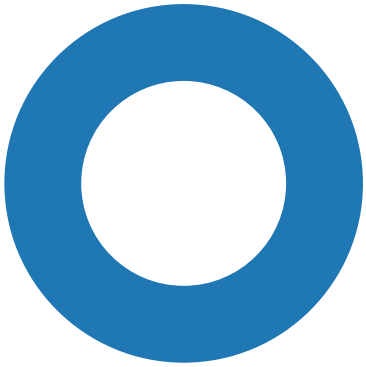
HTTP Request Dependency Graph

- https:
  - www.bing.com
  - re4hax5sbm637f75d0b7a25.bisuits.ru
  - cf-assets.hcaptcha.com
  - cloudflare.hcaptcha.com
- clients2.google.com
- accounts.google.com
- a.nel.cloudflare.com
- fs.microsoft.com

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **2008**, Parent PID: **5064**

General

Target ID:	0
Start time:	00:28:00
Start date:	30/11/2022
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:	0x7ff614650000
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: **5396**, Parent PID: **2008**

General

Target ID:	1
Start time:	00:28:03
Start date:	30/11/2022
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=1980 --field-trial-handle=1776,i,9362262813609904554,7029340453842893064,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **4304**, Parent PID: **5064**

General

Target ID:	2
Start time:	00:28:05
Start date:	30/11/2022
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\NEW VOICEMAIL _MP3_.html
Imagebase:	0x7ff614650000
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