ID: 756327
Sample Name: NEW VOICEMAIL _MP3_11232022 20736 a.m..html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 01:28:30
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

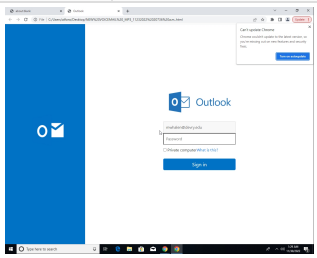
Windows Analysis Report

NEW VOICEMAIL _MP3_11232022 20736 a.m..html

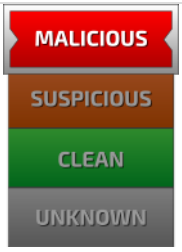
Overview

General Information

Sample Name:	NEW VOICEMAIL _MP3_11232022 20736 a.m..html
Analysis ID:	756327
MD5:	f0ad6b867b30da..
SHA1:	5ac910e6b2b263..
SHA256:	1c7686885d0544..
Infos:	



Detection



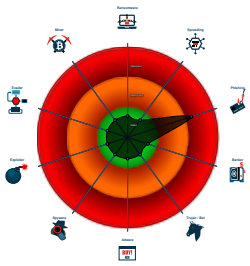
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- HTML document with suspicious na…
- JA3 SSL client fingerprint seen in co…
- 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: 4968 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6088 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=2000 --field-trial-handle=1812,i,13778629307497002630,14272478613148989793,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5224 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\NEW VOICEMAIL _MP3_11232022 20736 a.m..html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
NEW VOICEMAIL _MP3_11232022 20736 a.m..html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
08875.0.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

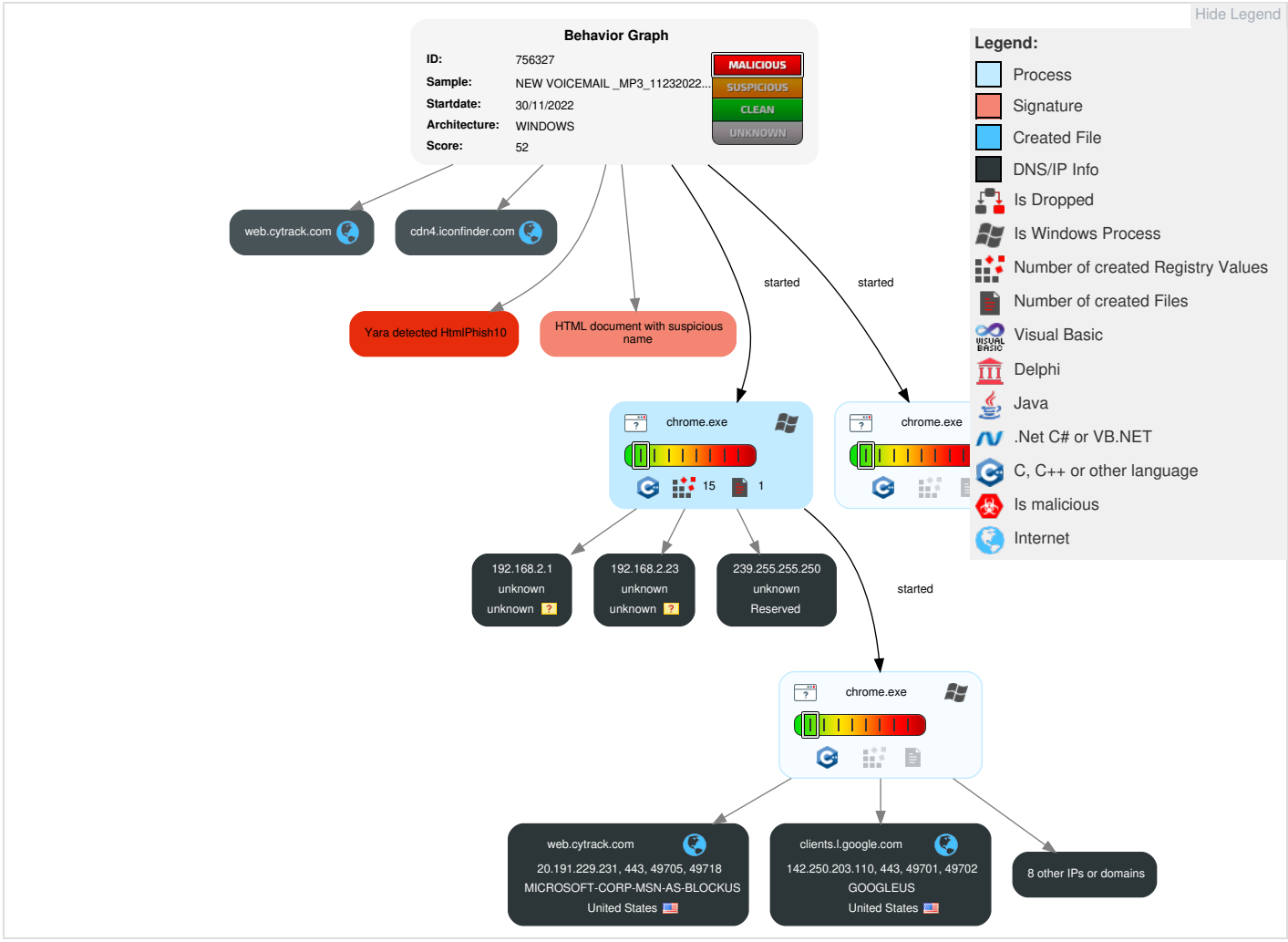
System Summary

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	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

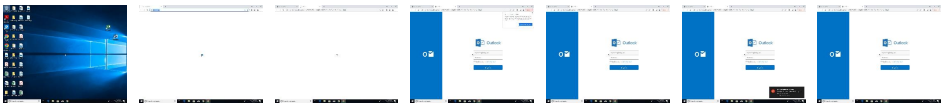
Behavior Graph

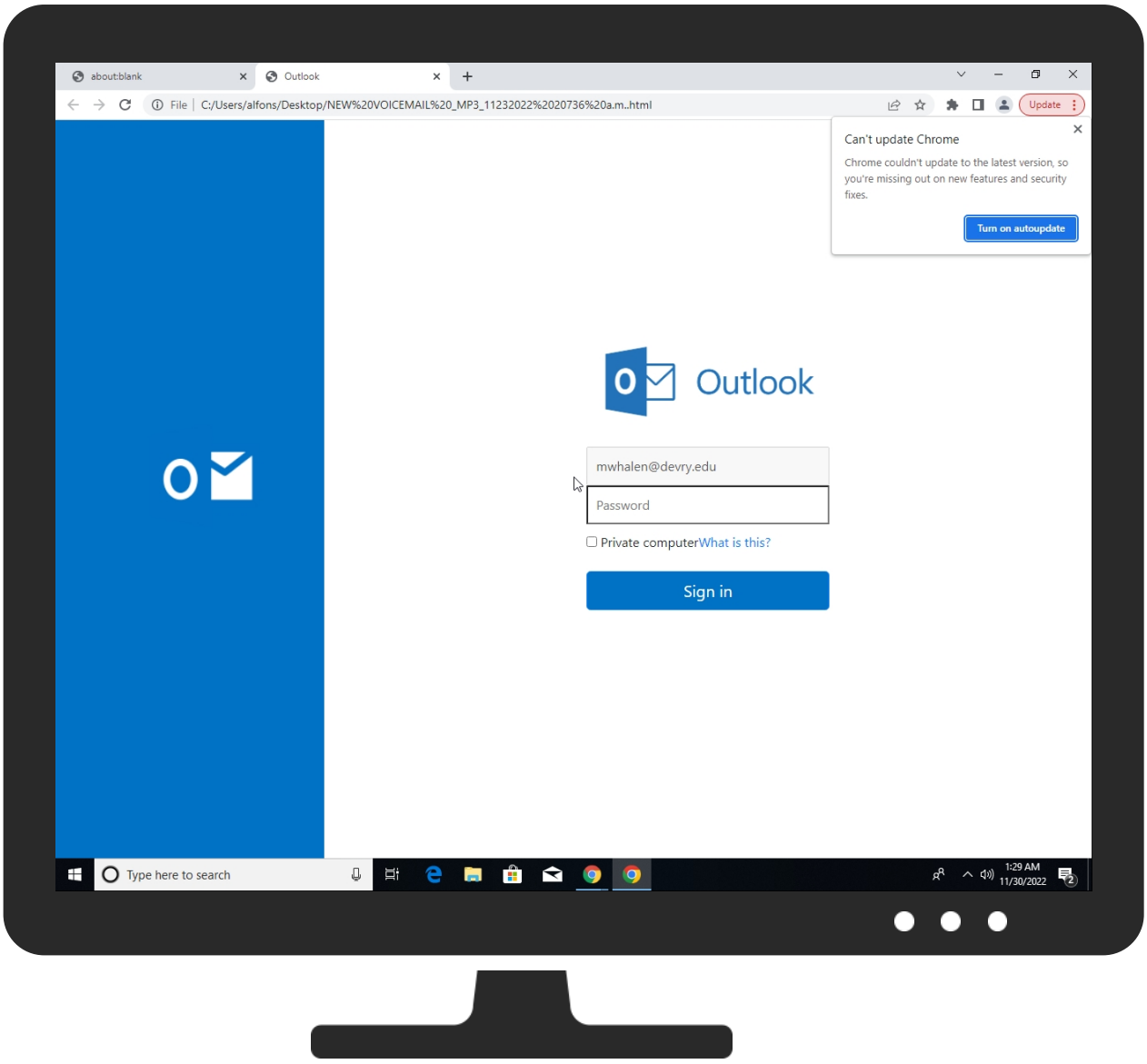


Screenshots

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

Source	Detection	Scanner	Label	Link
api.ipify.org.herokudns.com	0%	Virustotal		Browse
web.cytrack.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	0%	Avira URL Cloud	safe	
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	0%	Virustotal		Browse

Domains and IPs

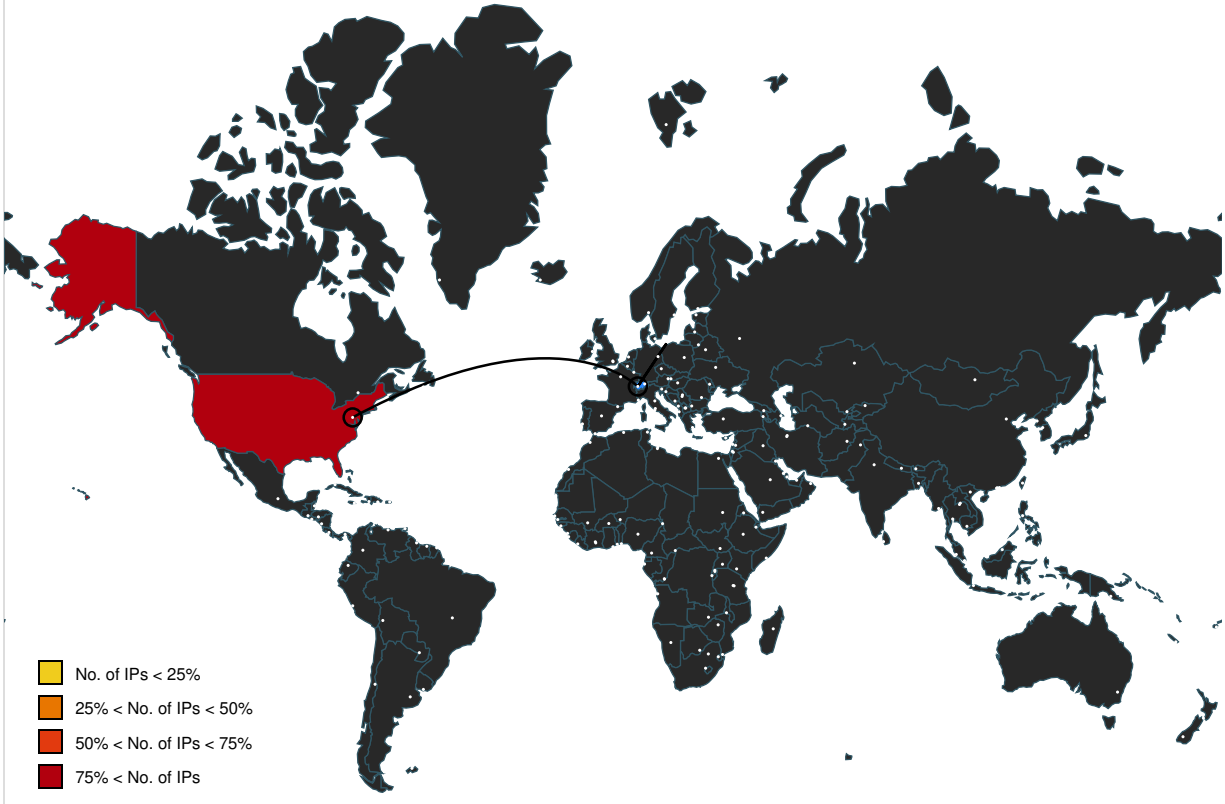
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
accounts.google.com	172.217.168.77	true	false		high
api.ipify.org.herokudns.com	3.232.242.170	true	false	• 0%, Virustotal, Browse	unknown
web.cytrack.com	20.191.229.231	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
cdn4.iconfinder.com	172.67.151.13	true	false		high
clients2.google.com	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/NEW%20VOICEMAIL%20_MP3_11232022%2020736%20a.m..html	false		low
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://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/css/bootstrap.min.css	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://api.ipify.org/?format=json	false		high
http://https://cdn4.iconfinder.com/data/icons/logos-and-brands/512/243_Outlook_logo-128.png	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.67.151.13	cdn4.iconfinder.com	United States		13335	CLOUDFLARENETUS	false
3.232.242.170	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false
20.191.229.231	web.cytrack.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	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
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.77	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.23
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756327
Start date and time:	2022-11-30 01:28:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW VOICEMAIL _MP3_11232022 20736 a.m..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:	13
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:	mal52.phis.winHTML@28/0@9/11
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 172.217.168.10, 34.104.35.123
- Excluded domains from analysis (whitelisted): client.wns.windows.com, edgedl.me.gvt1.com, ajax.googleapis.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

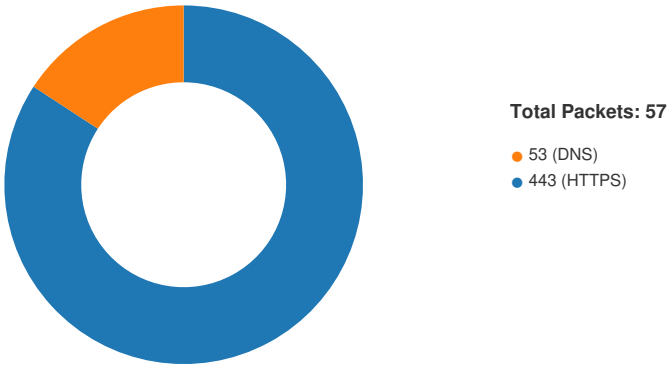
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (36336), with CRLF line terminators
Entropy (8bit):	5.256181179792569
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	NEW VOICEMAIL _MP3_11232022 20736 a.m..html
File size:	40153
MD5:	f0ad6b867b30dadd73860396ff9878f5
SHA1:	5ac910e6b2b26343c6544c1f84379c44bd68283d
SHA256:	1c7686885d0544ead84e43183d1527ba1e9169761e32344c82f07c386f6db7ab
SHA512:	aec656575e32fadd85a17a93382dba42d52f3d49e54668084b535ebf70d9460e46fd06be58515fd54d1da71e1cfc85778b97a25d1cac867f99ed5ea6cafa95e2
SSDEEP:	768:zEABVC3xkND6RLuQluKYEpj/Kb5F7C4iwD3MJV1bOWyp:zdBVoxEKLr3pj/KqTiWyp
TLSH:	0E0360B427429C334972F82FB69D2A578626DF63CDEE40E131C4E658D3E9FA1A2154CC
File Content Preview:	<script>..var email ="mwhalen@devry.edu";..</script>.....<!doctype html>.... <head>.. <meta charset="utf-8">.. .... <title>Outlook</title>.... .. <style>..... html,..body {.. height: 100%;..}....body {.. display: -ms-flexbox;.. display:

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:29:24.344043970 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.344115019 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.344199896 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.345079899 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.345133066 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.345215082 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.345856905 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.345891953 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.349308014 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.349348068 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.349421978 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.349740028 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.349792957 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.349970102 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.349988937 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.412429094 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.416285992 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.416330099 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.416944981 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.417062044 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.418279886 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.418788910 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.431106091 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.439260006 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.445985079 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.446033001 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.446479082 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.446518898 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.448028088 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.448324919 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.448537111 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.448612928 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.450512886 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.450613976 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.684357882 CET	49705	443	192.168.2.5	20.191.229.231
Nov 30, 2022 01:29:24.684412956 CET	443	49705	20.191.229.231	192.168.2.5
Nov 30, 2022 01:29:24.684511900 CET	49705	443	192.168.2.5	20.191.229.231

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:29:24.863107920 CET	49707	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.863166094 CET	443	49707	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.863459110 CET	49707	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.865577936 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.865614891 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.865705967 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.866050005 CET	49705	443	192.168.2.5	20.191.229.231
Nov 30, 2022 01:29:24.866106987 CET	443	49705	20.191.229.231	192.168.2.5
Nov 30, 2022 01:29:24.867244959 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.867333889 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.867434978 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.867573977 CET	49710	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.867624998 CET	443	49710	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.867697001 CET	49710	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.868287086 CET	49707	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.868319035 CET	443	49707	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.868729115 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.868746042 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.869139910 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.869185925 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.869417906 CET	49710	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.869452000 CET	443	49710	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.951461077 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.951488972 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.951581955 CET	49702	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.951598883 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.951643944 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.951751947 CET	443	49702	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.951945066 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.951960087 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.952059031 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.952073097 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.952259064 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.952816010 CET	49703	443	192.168.2.5	172.217.168.77
Nov 30, 2022 01:29:24.952830076 CET	443	49703	172.217.168.77	192.168.2.5
Nov 30, 2022 01:29:24.958852053 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.959218979 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.959249020 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.961194992 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.961296082 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.964086056 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.964108944 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.964255095 CET	49708	443	192.168.2.5	172.67.151.13
Nov 30, 2022 01:29:24.964262009 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.964397907 CET	443	49708	172.67.151.13	192.168.2.5
Nov 30, 2022 01:29:24.964817047 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.965147018 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.965195894 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.966454983 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.966574907 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.968799114 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.968832970 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.968983889 CET	49709	443	192.168.2.5	104.18.10.207
Nov 30, 2022 01:29:24.968993902 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.969011068 CET	443	49709	104.18.10.207	192.168.2.5
Nov 30, 2022 01:29:24.988557100 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.988687992 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.988713980 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.988828897 CET	443	49701	142.250.203.110	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:29:24.988897085 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.990379095 CET	49701	443	192.168.2.5	142.250.203.110
Nov 30, 2022 01:29:24.990391970 CET	443	49701	142.250.203.110	192.168.2.5
Nov 30, 2022 01:29:24.992566109 CET	443	49710	172.67.151.13	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:29:24.079976082 CET	49177	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:24.080174923 CET	49724	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:24.097395897 CET	53	49177	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:24.108066082 CET	53	49724	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:24.574326038 CET	51484	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:24.578699112 CET	63446	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:24.593811989 CET	55039	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:24.594775915 CET	53	51484	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:24.598325014 CET	53	63446	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:24.615720987 CET	53	55039	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:25.375689983 CET	55068	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:25.394407988 CET	53	55068	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:25.793207884 CET	56682	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:25.812587023 CET	53	56682	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:27.977798939 CET	62659	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:27.978885889 CET	58581	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:29:28.000149012 CET	53	62659	8.8.8.8	192.168.2.5
Nov 30, 2022 01:29:28.001149893 CET	53	58581	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 30, 2022 01:29:24.079976082 CET	192.168.2.5	8.8.8.8	0x8a57	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.080174923 CET	192.168.2.5	8.8.8.8	0x7d71	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.574326038 CET	192.168.2.5	8.8.8.8	0xb824	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.578699112 CET	192.168.2.5	8.8.8.8	0x7e9a	Standard query (0)	cdn4.iconfinder.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.593811989 CET	192.168.2.5	8.8.8.8	0x994a	Standard query (0)	web.cytrack.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.375689983 CET	192.168.2.5	8.8.8.8	0xc5be	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.793207884 CET	192.168.2.5	8.8.8.8	0xf183	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:27.977798939 CET	192.168.2.5	8.8.8.8	0xd1f9	Standard query (0)	cdn4.iconfinder.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:27.978885889 CET	192.168.2.5	8.8.8.8	0xf1f1	Standard query (0)	web.cytrack.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 01:29:24.097395897 CET	8.8.8.8	192.168.2.5	0x8a57	No error (0)	accounts.google.com		172.217.168.77	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.108066082 CET	8.8.8.8	192.168.2.5	0x7d71	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:29:24.108066082 CET	8.8.8.8	192.168.2.5	0x7d71	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.594775915 CET	8.8.8.8	192.168.2.5	0xb824	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false

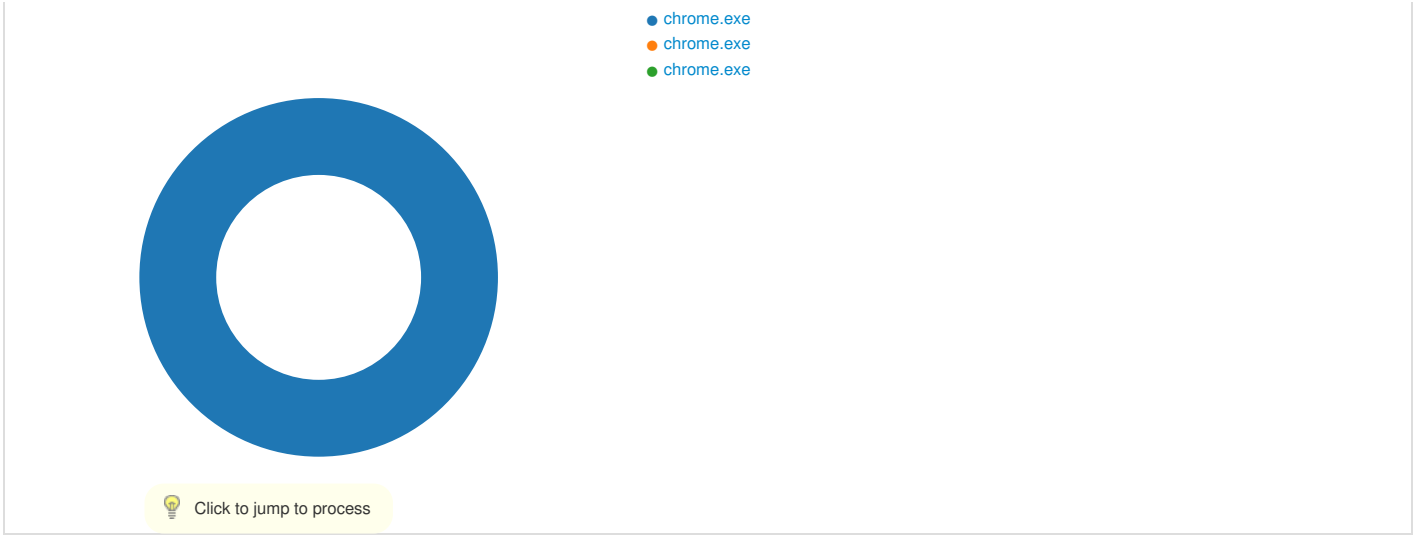
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 01:29:24.594775915 CET	8.8.8.8	192.168.2.5	0xb824	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.598325014 CET	8.8.8.8	192.168.2.5	0x7e9a	No error (0)	cdn4.iconfinder.com		172.67.151.13	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.598325014 CET	8.8.8.8	192.168.2.5	0x7e9a	No error (0)	cdn4.iconfinder.com		104.21.48.117	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:24.615720987 CET	8.8.8.8	192.168.2.5	0x994a	No error (0)	web.cytrack.com		20.191.229.231	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.394407988 CET	8.8.8.8	192.168.2.5	0xc5be	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:29:25.394407988 CET	8.8.8.8	192.168.2.5	0xc5be	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.394407988 CET	8.8.8.8	192.168.2.5	0xc5be	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.394407988 CET	8.8.8.8	192.168.2.5	0xc5be	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.394407988 CET	8.8.8.8	192.168.2.5	0xc5be	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:25.812587023 CET	8.8.8.8	192.168.2.5	0xf183	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:28.000149012 CET	8.8.8.8	192.168.2.5	0xd1f9	No error (0)	cdn4.iconfinder.com		104.21.48.117	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:28.000149012 CET	8.8.8.8	192.168.2.5	0xd1f9	No error (0)	cdn4.iconfinder.com		172.67.151.13	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:29:28.001149893 CET	8.8.8.8	192.168.2.5	0xf1f1	No error (0)	web.cytrack.com		20.191.229.231	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- cdn4.iconfinder.com
- stackpath.bootstrapcdn.com
- web.cytrack.com
- api.ipify.org

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4968, Parent PID: 2772

General

Target ID:	2
Start time:	01:29:19
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:	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: 6088, Parent PID: 4968

General

Target ID:	4
Start time:	01:29:20
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=2000 --field-trial-handle=1812,i,13778629307497002630,14272478613148989793,131072 --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: **5224**, Parent PID: **2772**

General

Target ID:	5
Start time:	01:29:21
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_11232022 20736 a.m..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