ID: 715165
Cookbook: browseurl.jbs
Time: 17:39:20
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

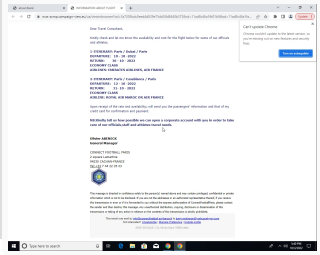
Windows Analysis Report

https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b3...

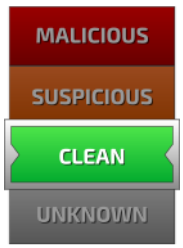
Overview

General Information

Sample URL:	https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e7...8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1
Analysis ID:	715165
Infos:	



Detection

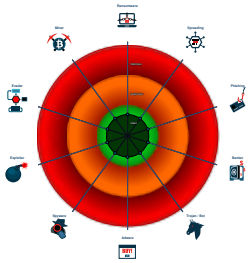


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5752 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5792 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=1944 --field-trial-handle=1624,i,17822862930805665288,9356387013567766339,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5268 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 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

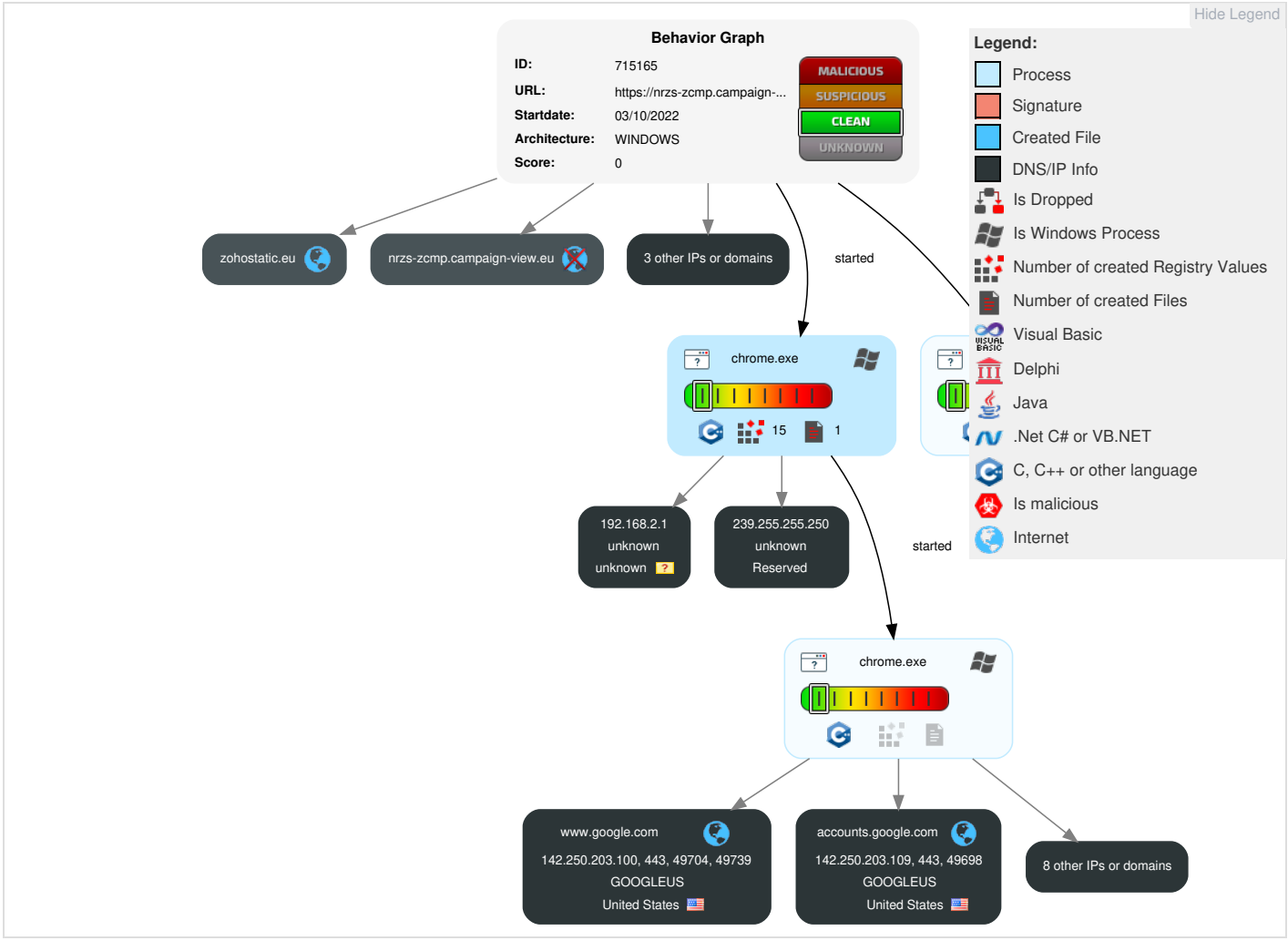
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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

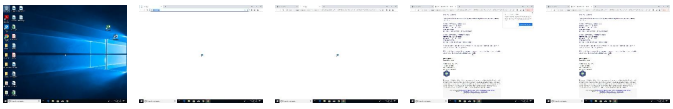
Behavior Graph

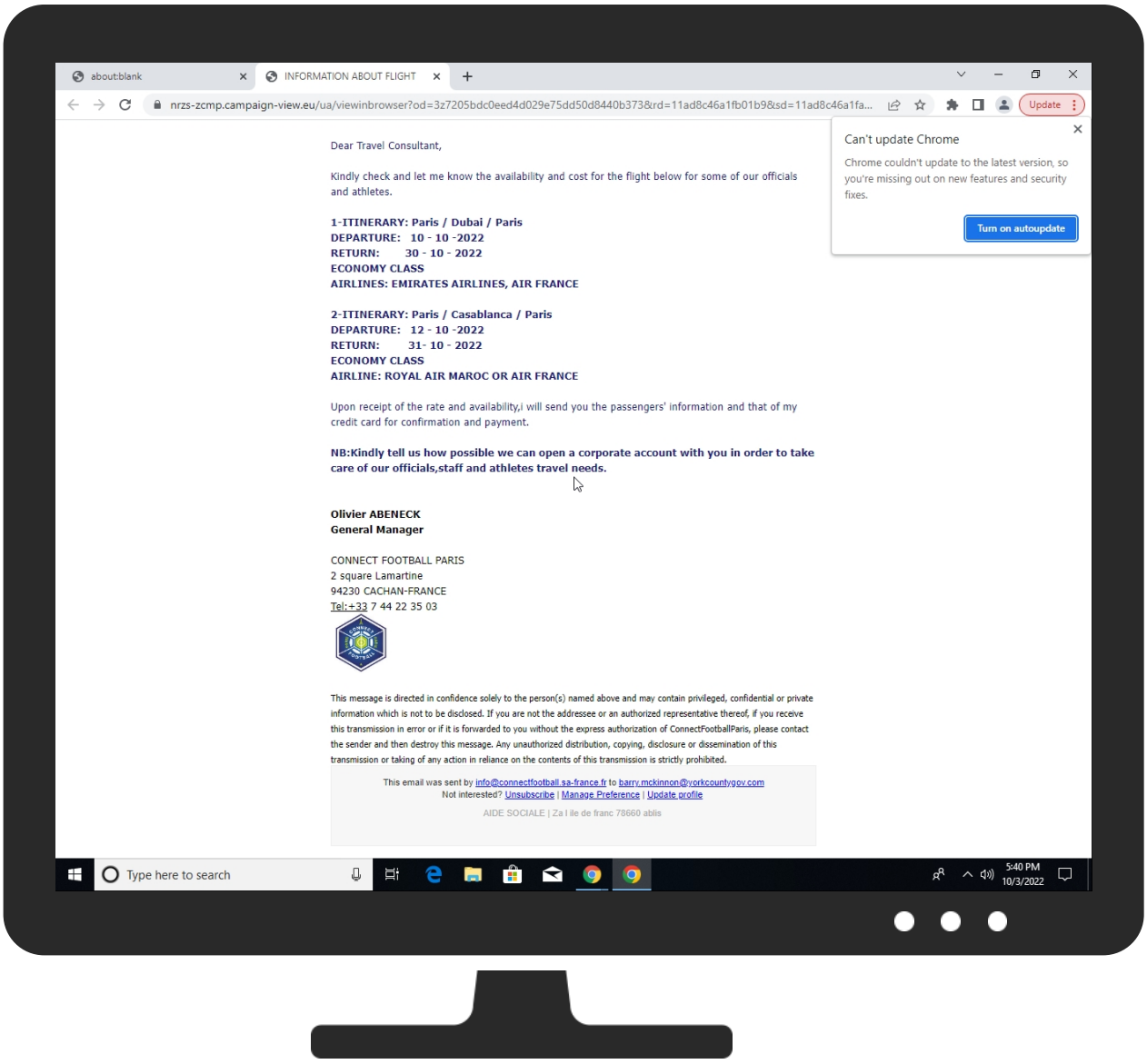


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://img.zohostatic.eu/campaigns/static2/images/spacer.gif	0%	Avira URL Cloud	safe	
http://https://img.zohostatic.eu/campaigns/static2/images/viewinbrowserarw.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://img.zohostatic.eu/campaigns/static2/images/videoclose.png	0%	Avira URL Cloud	safe	
http://https://campaign-image.eu/zohocampaigns/pmm_zc_v9_120907000001935004.png	0%	Avira URL Cloud	safe	
http://https://nrzs-zcmp.campaign-view.eu/favicon.ico	0%	Avira URL Cloud	safe	
http://https://nrzs-zcmp.campaign-view.eu/js/jquery-migrate-1.2.1.min.js	0%	Avira URL Cloud	safe	
http://https://nrzs-zcmp.campaign-view.eu/js/jquery-1.11.0.min.js	0%	Avira URL Cloud	safe	
http://https://nrzs-zcmp.campaign-view.eu/images/viewinbrowserarw.png	0%	Avira URL Cloud	safe	
http://https://img.zohostatic.eu/campaigns/static2/images/zc_tmblrpost.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

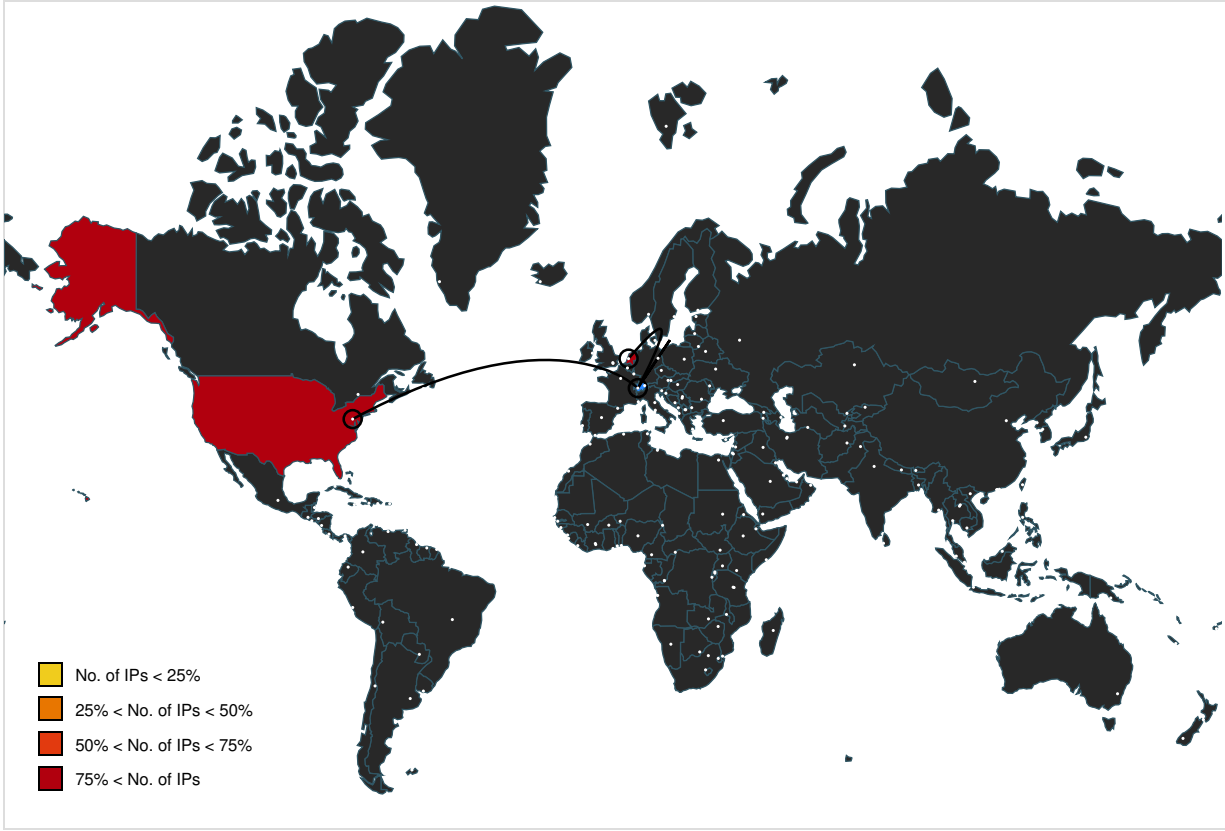
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
zohostatic.eu	185.230.212.112	true	false		unknown
www.google.com	142.250.203.100	true	false		high
campaign-image.eu	185.230.212.228	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
customer-campaign.zoho.eu	185.230.212.128	true	false		high
clients2.google.com	unknown	unknown	false		high
img.zohostatic.eu	unknown	unknown	false		unknown
nrzs-zcmp.campaign-view.eu	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1	false		unknown
http://https://nrzs-zcmp.campaign-view.eu/js/jquery-1.11.0.min.js	false	• Avira URL Cloud: safe	unknown
http://https://img.zohostatic.eu/campaigns/static2/images/videoclose.png	false	• Avira URL Cloud: safe	unknown
http://https://campaign-image.eu/zohocampaigns/pmm_zc_v9_120907000001935004.png	false	• Avira URL Cloud: safe	unknown
http://https://nrzs-zcmp.campaign-view.eu/images/viewinbrowserarw.png	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://img.zohostatic.eu/campaigns/static2/images/spacer.gif	false	• Avira URL Cloud: safe	unknown
http://https://img.zohostatic.eu/campaigns/static2/images/zc_tmblrpost.jpg	false	• Avira URL Cloud: safe	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://nrzs-zcmp.campaign-view.eu/js/jquery-migrate-1.2.1.min.js	false	• Avira URL Cloud: safe	unknown
http://https://img.zohostatic.eu/campaigns/static2/images/viewinbrowserarw.png	false	• Avira URL Cloud: safe	unknown
http://https://nrzs-zcmp.campaign-view.eu/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
185.230.212.112	zohostatic.eu	Netherlands		41913	COMPUTERLINEComputerlineSchlierbachSwitzerlandCH	false
185.230.212.228	campaign-image.eu	Netherlands		41913	COMPUTERLINEComputerlineSchlierbachSwitzerlandCH	false
185.230.212.128	customer-campaign.zoho.eu	Netherlands		41913	COMPUTERLINEComputerlineSchlierbachSwitzerlandCH	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.109	accounts.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:	715165
Start date and time:	2022-10-03 17:39:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1
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:	5
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:	CLEAN
Classification:	clean0.win@25/0@9/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 172.217.168.74, 142.250.203.106, 216.58.215.234, 172.217.168.10, 172.217.168.42
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, content-autofill.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.
- VT rate limit hit for: https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1

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

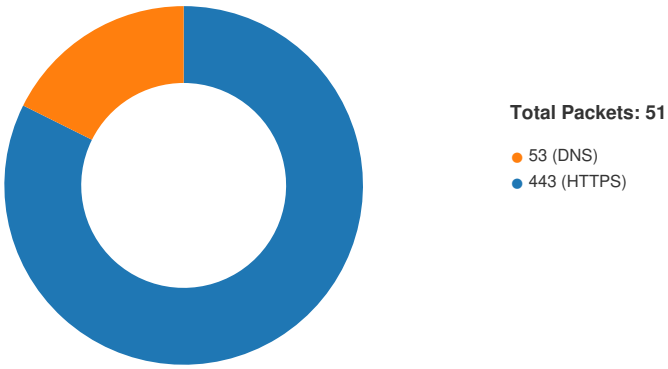
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:40:23.331084967 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:23.331135988 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.331228018 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:23.331720114 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:23.331744909 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:23.331800938 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:23.332357883 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:23.332376957 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.332776070 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:23.332791090 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:23.462976933 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.463125944 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:23.510674000 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:23.510696888 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:23.511096001 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:23.511120081 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.511975050 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.512072086 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:23.513732910 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:23.513860941 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:23.513860941 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:23.513914108 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.458549023 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.458657026 CEST	443	49699	185.230.212.128	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:40:24.458806992 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.464370012 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.464416981 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.543817043 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.543879986 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.544116020 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.544181108 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.544192076 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.545310020 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.546757936 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:24.546773911 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.546921015 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.548352957 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:24.548372030 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.554337025 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.554400921 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.556618929 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.556793928 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.567861080 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.567893028 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.568496943 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.568521976 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.569046974 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.579293013 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.579431057 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.579447985 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.579495907 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.582284927 CEST	49696	443	192.168.2.5	142.250.203.110
Oct 3, 2022 17:40:24.582324028 CEST	443	49696	142.250.203.110	192.168.2.5
Oct 3, 2022 17:40:24.614311934 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.614372015 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:24.614388943 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.615195990 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.615266085 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:24.616884947 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 17:40:24.616908073 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 17:40:24.727257967 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:24.727333069 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:24.927014112 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.205631971 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205679893 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205689907 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205709934 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205718994 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205737114 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.205756903 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205782890 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.205794096 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.205812931 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.205842018 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.236780882 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236804008 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236876011 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236901999 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236915112 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236929893 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.236939907 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.236982107 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.237267971 CEST	443	49699	185.230.212.128	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:40:25.237281084 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.237298965 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.237323046 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.237322092 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.237348080 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.237360954 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.237361908 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.237361908 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.237385035 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.237404108 CEST	49699	443	192.168.2.5	185.230.212.128
Oct 3, 2022 17:40:25.268059969 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268101931 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268199921 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268239021 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268248081 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268270016 CEST	443	49699	185.230.212.128	192.168.2.5
Oct 3, 2022 17:40:25.268290043 CEST	49699	443	192.168.2.5	185.230.212.128

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:40:23.289100885 CEST	60841	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:23.290642023 CEST	61893	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:23.316634893 CEST	53	61893	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:23.316822052 CEST	53	60841	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:24.066952944 CEST	51441	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:24.110471964 CEST	53	51441	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:25.197225094 CEST	61452	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:25.223310947 CEST	53	61452	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:25.290143013 CEST	65323	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:25.295053005 CEST	51484	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:25.311253071 CEST	53	65323	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:25.315578938 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:28.142142057 CEST	60975	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:28.143261909 CEST	59220	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:28.161709070 CEST	53	60975	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:28.176218987 CEST	53	59220	8.8.8.8	192.168.2.5
Oct 3, 2022 17:40:28.336839914 CEST	55068	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:40:28.357873917 CEST	53	55068	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
Oct 3, 2022 17:40:23.289100885 CEST	192.168.2.5	8.8.8.8	0xfd0d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:23.290642023 CEST	192.168.2.5	8.8.8.8	0xef24	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:24.066952944 CEST	192.168.2.5	8.8.8.8	0xf752	Standard query (0)	nrzs-zcmp.campaign-view.eu	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.197225094 CEST	192.168.2.5	8.8.8.8	0x2186	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.290143013 CEST	192.168.2.5	8.8.8.8	0x9b48	Standard query (0)	campaign-image.eu	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.295053005 CEST	192.168.2.5	8.8.8.8	0x3b14	Standard query (0)	img.zohostatic.eu	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.142142057 CEST	192.168.2.5	8.8.8.8	0x7301	Standard query (0)	img.zohostatic.eu	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.143261909 CEST	192.168.2.5	8.8.8.8	0x8bbd	Standard query (0)	nrzs-zcmp.campaign-view.eu	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.336839914 CEST	192.168.2.5	8.8.8.8	0xa73	Standard query (0)	campaign-image.eu	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
Oct 3, 2022 17:40:23.316634893 CEST	8.8.8.8	192.168.2.5	0xef24	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 17:40:23.316634893 CEST	8.8.8.8	192.168.2.5	0xef24	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:23.316822052 CEST	8.8.8.8	192.168.2.5	0xfd0d	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:24.110471964 CEST	8.8.8.8	192.168.2.5	0xf752	No error (0)	nrzs-zcmp.campaign-view.eu	customer-campaign.zoho.eu		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 17:40:24.110471964 CEST	8.8.8.8	192.168.2.5	0xf752	No error (0)	customer-campaign.zoho.eu		185.230.212.128	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.223310947 CEST	8.8.8.8	192.168.2.5	0x2186	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.311253071 CEST	8.8.8.8	192.168.2.5	0x9b48	No error (0)	campaign-image.eu		185.230.212.228	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.315578938 CEST	8.8.8.8	192.168.2.5	0x3b14	No error (0)	img.zohostatic.eu	zohostatic.eu		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 17:40:25.315578938 CEST	8.8.8.8	192.168.2.5	0x3b14	No error (0)	zohostatic.eu		185.230.212.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:25.315578938 CEST	8.8.8.8	192.168.2.5	0x3b14	No error (0)	zohostatic.eu		89.36.170.31	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.161709070 CEST	8.8.8.8	192.168.2.5	0x7301	No error (0)	img.zohostatic.eu	zohostatic.eu		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 17:40:28.161709070 CEST	8.8.8.8	192.168.2.5	0x7301	No error (0)	zohostatic.eu		89.36.170.31	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.161709070 CEST	8.8.8.8	192.168.2.5	0x7301	No error (0)	zohostatic.eu		185.230.212.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.176218987 CEST	8.8.8.8	192.168.2.5	0x8bbd	No error (0)	nrzs-zcmp.campaign-view.eu	customer-campaign.zoho.eu		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 17:40:28.176218987 CEST	8.8.8.8	192.168.2.5	0x8bbd	No error (0)	customer-campaign.zoho.eu		185.230.212.128	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:40:28.357873917 CEST	8.8.8.8	192.168.2.5	0xa73	No error (0)	campaign-image.eu		185.230.212.228	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- nrzs-zcmp.campaign-view.eu
- https:
  - campaign-image.eu
  - img.zohostatic.eu

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49696	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:24 UTC	0	OUT	GET /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 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:24 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-9BxsJ8kFDpy5lb0x-J1n8Q' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 15:40:24 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 31224 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 15:40:24 UTC	2	IN	Data Raw: 32 63 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 33 31 32 32 34 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="31224"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 15:40:24 UTC	3	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 15:40:24 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49698	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:24 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:24 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:24 UTC	3	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 15:40:24 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-OWhtn-qjyQfv_dBMh5gFyw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 15:40:24 UTC	5	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-10-03 15:40:24 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49707	185.230.212.112	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	263	OUT	GET /campaigns/static2/images/videoclose.png HTTP/1.1 Host: img.zohostatic.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:25 UTC	267	IN	HTTP/1.1 200 OK Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: image/png Content-Length: 2967 Last-Modified: Mon, 03 Oct 2022 13:27:43 GMT Connection: close ETag: "633ae34f-b97" Expires: Tue, 03 Oct 2023 15:40:25 GMT Cache-Control: max-age=31536000 X-Robots-Tag: noindex, nofollow, nosnippet, noarchive Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Strict-Transport-Security: max-age=63072000 Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	267	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1d 00 00 00 1d 08 06 00 00 00 56 93 67 0f 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 Data Ascii: PNGIHDRVgtEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M 0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49710	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:26 UTC	272	OUT	GET /favicon.ico HTTP/1.1 Host: nrzs-zcmp.campaign-view.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: 1e5a17c8ab=38d19ed51de33532d3b7e87a22c4d973; ZCAMPAIGN_CSRF_TOKEN=6dbc78ab-4589-4358-baa1-ed77de15c5db; _zcsr_tmp=6dbc78ab-4589-4358-baa1-ed77de15c5db; JSESSIONID=2D2561E620E609AC020ED2EC3D99E714
2022-10-03 15:40:26 UTC	273	IN	HTTP/1.1 404 Server: ZGS Date: Mon, 03 Oct 2022 15:40:26 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 446 Connection: close X-Content-Type-Options: nosniff X-XSS-Protection: 1 X-Frame-Options: SAMEORIGIN
2022-10-03 15:40:26 UTC	273	IN	Data Raw: 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 20 61 6c 65 72 74 6d 73 67 20 22 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 20 32 30 70 78 20 30 70 78 3b 22 3e 3c 74 61 62 6c 65 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 22 30 22 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 30 22 20 62 6f 72 64 65 72 3d 22 30 22 20 77 69 64 74 68 3d 22 39 35 25 22 3e 3c 74 62 6f 64 79 3e 0a 3c 74 72 3e 3c 74 64 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 20 77 69 64 74 68 3d 22 37 30 22 20 76 61 6c 69 67 6e 3d 22 6d 69 64 64 6c 65 22 20 68 65 69 67 68 74 3d 22 35 30 22 3e 20 3c 69 6d 67 20 63 6c 61 73 73 3d 22 61 6c 65 72 74 69 63 6f 6e 62 69 67 20 6d 72 31 30 22 20 61 6c 69 67 6e 3d 22 61 62 73 6d 69 64 64 6c 65 22 20 73 72 63 3d 22 2f 2f 69 6d 67 2e 7a 6f 68 6f 73 74 61 74 69 63 2e Data Ascii: <table cellspacing="0" cellpadding="0" border="0" width="95%"><tbody><tr><td align="center" width="70" valign="middle" height="50"> <img class="alerticonbig mr10" align ="absmiddle" src="//img.zohostatic.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49717	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:28 UTC	273	OUT	GET /ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: nrzs-zcmp.campaign-view.eu

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:29 UTC	347	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:29 GMT Content-Type: text/html;charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: 1e5a17c8ab=bb02a19096eb104b6fdfa90f2b944002; Path=/ X-Content-Type-Options: nosniff X-XSS-Protection: 1 Set-Cookie: ZCAMPAIGN_CSRF_TOKEN=6f18f8e1-f5c2-4cdb-9b03-21911b729bd9;path=/;SameSite=None;Secure;priority=high Set-Cookie: _zcsr_tmp=6f18f8e1-f5c2-4cdb-9b03-21911b729bd9;path=/;SameSite=Strict;Secure;priority=high Pragma: no-cache Cache-Control: private,no-cache,no-store,max-age=0,must-revalidate Expires: Thu, 01 Jan 1970 00:00:00 GMT X-Frame-Options: SAMEORIGIN Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Cache-Control, Pragma, Origin, Authorization, Content-Type, X-Requested-With Access-Control-Allow-Methods: GET,POST,OPTIONS Set-Cookie: JSESSIONID=F956D638DEC17713D9D55765488BA465; Path=/; Secure; HttpOnly vary: accept-encoding Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:29 UTC	348	IN	Data Raw: 31 63 62 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 49 4e 46 4f 52 4d 41 54 49 4f 4e 20 41 42 4f 55 54 20 46 4c 49 47 48 54 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 21 2d 2d 20 54 77 69 74 74 65 72 20 4d 65 74 61 20 54 61 67 73 20 2d 2d 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 63 61 72 64 22 20 63 6f 6e 74 65 6e 74 3d 22 73 75 6d 6d 61 72 79 22 3e 3c 6d 65 74 61 20 6e 61 Data Ascii: 1cb3<!DOCTYPE html ><html xmlns="http://www.w3.org/1999/xhtml"><head><title>INFORMATION ABOUT FLIGHT</title><meta content="text/html;charset=UTF-8" http-equiv="Content-Type">... Twitter Meta Tags --><meta name="twitter:card" content="summary"><meta na
2022-10-03 15:40:29 UTC	363	IN	Data Raw: 0a 09 09 09 09 63 68 61 72 43 6e 74 2e 68 74 6d 6c 28 30 29 3b 0a 09 09 09 09 73 75 63 42 6f 78 2e 68 74 6d 6c 28 22 59 6f 75 72 20 63 6f 6d 6d 65 6e 74 20 61 64 64 65 64 20 73 75 63 63 65 73 73 66 75 6c 6c 79 2e 22 29 2e 66 61 64 65 4f 75 74 28 35 30 30 30 29 3b 0a 09 09 09 09 62 74 6e 2e 68 74 6d 6c 28 22 50 6f 73 74 22 29 3b 0a 0a 09 09 09 7d 0a 09 09 7d 29 3b 0a 09 7d 0a 09 65 6c 73 65 0a 09 7b 0a 09 09 65 72 72 42 6f 78 2e 68 74 6d 6c 28 22 45 6e 0d 0a 34 30 30 30 0d 0a 74 65 72 65 64 20 4d 6f 72 65 20 74 68 61 6e 20 32 35 30 20 43 68 61 72 61 63 74 65 72 73 2e 22 29 3b 0a 09 7d 0a 0a 7d 0a 09 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 0a 09 09 09 66 75 6e 63 74 69 6f 6e 20 28 29 0a 09 09 09 7b 0a 09 09 09 69 66 20 28 74 6f 70 20 3d 3d 3d Data Ascii: charCnt.html(0);sucBox.html("Your comment added successfully.").fadeOut(5000);btn.html("Post");}});}else{errBox.html("En4000tered More than 250 Characters.");}}$(document).ready(function (){if (top ===
2022-10-03 15:40:29 UTC	379	IN	Data Raw: 0a 09 09 09 09 09 69 66 20 28 64 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 69 64 29 29 20 7b 72 65 74 75 72 6e 3b 7d 0a 09 09 09 09 09 6a 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 73 29 3b 20 6a 73 2e 69 64 20 3d 20 69 64 3b 0a 09 09 09 09 09 6a 73 2e 73 72 63 20 3d 20 22 22 3b 0a 09 09 09 09 09 66 6a 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 6a 73 2c 20 66 6a 73 29 3b 0a 09 09 09 09 7d 28 64 6f 63 75 6d 65 6e 74 2c 0d 0a 32 30 30 30 0d 0a 20 27 73 63 72 69 70 74 27 2c 20 27 66 61 63 65 62 6f 6f 6b 2d 6a 73 73 64 6b 27 29 29 3b 0a 09 09 09 09 0a 09 09 09 09 0a 09 09 09 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 74 79 6c 65 3e 0a 2e 7a 63 76 62 62 61 6e 64 62 67 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 Data Ascii: if (d.getElementById(id)) {return;}js = d.createElement(s); js.id = id;js.src = "";fjs.parentNode.insertBefore(js, fjs);}(document,2000 'script', 'facebook-jssdk'));</script><style>.zcvbbandbg{ background-c
2022-10-03 15:40:29 UTC	395	IN	Data Raw: 09 09 09 09 09 09 09 09 09 09 3c 61 20 76 61 6c 75 65 20 3d 22 70 6c 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 20 63 6f 6c 6f 72 3a 23 33 33 33 3b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 20 20 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 22 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 3b 22 20 6f 6e 63 6c 69 63 6b 3d 22 74 72 61 6e 73 6c 61 74 65 54 6f 4c 61 6e 67 28 27 70 6c 27 29 22 3e 50 6f 6c 69 73 68 3c 2f 61 3e 0a 09 09 09 09 09 09 09 09 09 09 3c 61 20 76 61 6c 75 65 20 3d 22 70 74 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 20 63 6f 6c 6f 72 3a 23 33 33 33 3b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 20 20 77 68 69 74 Data Ascii: Polish<a value ="pt" style="font-size:12px; color:#333; text-decoration:none; whit
2022-10-03 15:40:29 UTC	411	IN	Data Raw: 79 53 68 6f 77 48 69 64 65 28 29 3b 09 0a 09 09 09 09 09 09 09 09 09 09 7d 0a 09 09 09 09 09 09 09 09 09 09 2f 2f 24 28 22 23 47 50 6c 75 73 44 69 76 22 29 2e 68 69 64 65 28 29 3b 09 09 0a 09 09 09 09 09 09 09 09 09 2f 2f 24 28 22 23 6d 65 64 69 61 4f 76 65 72 4c 61 79 22 29 2e 68 69 64 65 28 29 3b 09 09 0a 09 09 09 09 09 09 09 09 7d 0a 09 09 09 09 09 09 09 09 09 7d 29 3b 0a 09 09 09 09 09 09 09 09 7d 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 21 2d 2d 20 47 6f 6f 6f 67 6c 65 2b 20 45 4e 44 44 20 0d 0a 33 65 66 30 0d 0a 2d 2d 3e 0a 3c 21 2d 2d 20 54 75 6d 62 6c 72 20 53 68 61 72 65 20 53 74 61 72 74 20 20 2d 2d 3e 0a 0a 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 7a 63 76 62 70 6c 75 67 Data Ascii: yShowHide();}//$("#GPlusDiv").hide();//$("#mediaOverLay").hide();}});}</script> ... Google+ ENDD 3ef0-->... Tumblr Share Start --><div class="zcvbplug

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49716	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:28 UTC	274	OUT	GET /images/viewinbrowserarw.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: nrzs-zcmp.campaign-view.eu

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:28 UTC	274	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:28 GMT Content-Type: image/png Content-Length: 1610 Connection: close Set-Cookie: 1e5a17c8ab=6aee27535d1d2cea5f181d63cb361d80; Path=/ Accept-Ranges: bytes ETag: W/"1610-1664603890000" Last-Modified: Sat, 01 Oct 2022 05:58:10 GMT Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:28 UTC	274	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 47 00 00 00 17 08 06 00 00 00 59 3e 52 e8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 Data Ascii: PNGIHDRGY>RtEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W 5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49720	185.230.212.228	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:28 UTC	276	OUT	GET /zohocampaigns/pmm_zc_v9_120907000001935004.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: campaign-image.eu
2022-10-03 15:40:28 UTC	276	IN	HTTP/1.1 200 OK Server: ZGS Date: Mon, 03 Oct 2022 15:40:28 GMT Content-Type: image/png Content-Length: 72470 Connection: close Set-Cookie: 45342b9b1e=0a49ff5c1535be0fc90fdb69cb1fd4a5; Path=/ Cache-Control: no-cache Last-Modified: Sun, 2 Oct 2022 23:22:29 GMT Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:28 UTC	276	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 e1 00 00 00 e1 08 02 00 00 00 b1 d1 45 2d 00 00 00 03 73 42 49 54 08 08 08 db e1 4f e0 00 00 20 00 49 44 41 54 78 9c ec bd 77 98 26 55 b5 35 be f6 39 a7 f2 9b 3b 4c 4f 0e 4c 60 c8 02 02 06 82 88 82 01 f1 7a af 0a 06 50 c1 2b c9 44 52 f2 c8 90 25 89 12 e4 0a 82 62 c2 2b 88 81 a8 08 8a 12 25 83 33 0c 93 43 e7 ee 37 55 3e e1 f7 c7 db 13 c0 f4 78 bf 1f 7c df dc 67 d6 d3 4f 4d 77 75 4f bd 55 75 56 ed b3 f7 d9 6b ef 22 63 0c b6 e1 ef 63 e2 f6 10 00 0d e4 40 0e 64 80 01 68 60 64 c8 73 2a 85 a0 ca 99 03 83 76 0b 85 02 14 14 67 ba f3 7f d3 3c 65 8c 59 dc 52 46 71 e2 40 e7 20 9b b6 00 18 c1 02 d8 1b 7b 4d 5b 19 68 1b 47 ff 31 b6 b8 3b 1a d0 80 02 e4 c6 3d 0c 10 cd 56 a8 24 55 ab 65 18 80 90 66 b1 63 b3 5c 29 Data Ascii: PNGIHDRE-sBITO IDATxw&U59;LOL`zP+DR%b+%3C7U>x|gOMwuOUuVk"cc@dh`ds*vg<eYRFq@ {M [hG1;=V$Uefc\)
2022-10-03 15:40:28 UTC	292	IN	Data Raw: 2b a8 5e 12 d8 1d c2 a1 37 fc c9 46 64 d8 c0 c1 61 68 34 ac 23 04 8d db ba 59 3a c5 77 9e c1 77 ad db 3f ef 44 7e 2e e5 54 cb 9f 1e f5 cb 9d 6b 75 06 08 2e bc ec ee 7d 0e 59 f0 f8 cb 85 bb 1f 59 75 c0 2f ae e8 2e 40 b9 06 e5 4a f8 ab 53 f6 0d bd 6f 62 86 ed fa fc ad 25 cb 43 0e 0c 60 d4 84 91 93 b6 9c 74 ec f1 a7 be ff d1 5a db 03 2e 40 96 55 15 c1 ac 99 5b fb 91 83 08 4c 98 3c 15 2b 60 45 b0 a6 d0 db 35 d8 db 3e 6e c6 ef 16 de 8a 28 30 00 8f 13 84 a0 6b 4d 01 61 05 a8 bd cd f6 13 b2 69 13 20 a8 f9 e1 2e 7b ee b3 fd 9c 8b 1e 5b 54 5f f9 35 14 06 fa 80 5b 91 d7 ad 2a 7d d7 5d 7b d2 d1 87 ce 75 fd 7e 19 86 10 25 0c a0 52 86 9f ce 1c f3 ec 13 8f 14 fb 36 52 e0 eb d7 ac 9a b8 c5 b8 42 71 60 93 2a 1c 7a 87 37 95 85 31 60 02 98 0c 19 99 c6 0d c5 42 e0 21 30 cc Data Ascii: +^7Fdah4#Y:ww?D~.Tku.}YYu/.@JSob%C`tZ.@U[L<+`E5>n(0kMai .{[T_5[*]}{u~%R6RBq`*z71`B!0
2022-10-03 15:40:28 UTC	308	IN	Data Raw: 4b d7 22 bc 95 4c 25 89 88 f5 1e 6d a8 fe c5 6b 32 2f ce ce b7 2a 08 6c 2c 09 6a 7b 29 20 01 d8 c7 b8 59 9f 0b 7a 33 ce 9a 45 2b 7f fd 73 ef cc 39 90 41 00 12 3c 13 00 38 03 7e e9 f9 e7 de 76 e7 83 86 e9 50 c5 0c 0c a0 44 67 47 ef d1 d1 23 8b 56 36 c7 e7 b6 71 75 b4 d8 59 49 6a 1d 8c 2e c7 54 57 83 69 9e 86 d0 f0 6d 19 18 86 41 35 58 4c c5 e9 cf b3 ed f8 e7 82 b3 8b a3 44 38 65 da 9d 0a 01 24 4d 8d 19 46 ad 5c 6e 6a 59 11 e7 8b 87 67 27 1e ed 5f e9 34 fa b0 97 2d de 78 93 2f 02 dc 18 67 07 0e d6 9f 3f b0 45 c0 52 ad 04 65 14 2b 25 52 5f 0b be 65 d3 96 30 82 82 2d ca a6 05 10 45 51 13 74 c6 b5 3a 12 0c 6b d6 d9 0f 3c 3f cd 53 4b 52 c2 8c 98 b2 c0 04 4f 80 61 9b 65 95 36 a5 a0 9c 58 44 cb 56 3d 15 18 3c 0a 22 26 29 57 00 8e 69 71 c4 fc 84 83 89 96 94 cb 17 Data Ascii: K"L%mk2/*I,j{) Yz3E+s9A<8~vPDgG#V6quYIj.TWimA5XLD8e$MF\njYg'_4-x/g?ERe+%R_e0-EQt:k<?SKRO ae6XDV=<"&)Wiq
2022-10-03 15:40:28 UTC	324	IN	Data Raw: 57 13 a7 6f 24 b0 bd 72 b4 0c 98 9a 06 d6 2d 65 64 bc 51 e5 1c 80 4c ee 69 73 ea e3 63 2b 57 c6 68 c6 e5 5e df 84 de ef 07 16 f5 4c 49 18 54 38 91 c0 8a 26 05 93 42 22 29 51 2b 29 5f 73 cb 12 42 d8 a6 15 85 7c 68 e5 30 06 9e 4d 65 97 2c 59 7a e9 9c af 6e bb 4a bb f4 a2 33 76 dc 79 aa 00 68 b8 fe 4e 7b 6e b4 eb 5e 9b 7d fc d1 b2 13 4e 3c ab 52 ab 66 d2 ed ba 61 54 ca 25 a2 e8 b6 95 74 9b 0d 85 62 a6 00 a1 92 0b 08 7d 30 4d 00 80 44 42 07 60 3f 56 e2 ff 63 d6 47 ff b5 60 86 a4 10 3c 2c 0c af cc 25 d3 dd 6d 5d 85 91 f1 e2 58 01 89 a0 56 5f 59 6f 2e 3b ef a2 a3 5e 78 f5 ba 43 8f dc 58 33 00 63 28 96 9d cf 3f 5b ba db 1e 47 9d 72 da 79 df 2e 19 ea ea 9d 8a 69 1c 90 ae a8 d6 f2 81 55 52 60 00 22 05 91 02 03 20 90 58 b6 7c 8d b8 6b 27 d4 50 f2 42 a9 e2 d7 9c de Data Ascii: Wo$r-edQLisc+Wh^LIT8&B")Q+)_sB|h0Me,YznJ3vyhN{n^}N<RfaT%tb}0MDB`?VcG`<,%m]XV_Yo.;^xCX3c(? [Gry.iUR`" X|k'PB

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:28 UTC	340	IN	Data Raw: 98 24 c2 0c 5f a1 c1 0c 18 cd 68 12 b7 dc 33 22 c6 85 c5 85 86 d1 52 71 4b 90 41 9a 75 a4 6e f5 54 07 3b 35 47 69 d7 73 1c cd 52 d7 c9 9b 9d 26 d3 ae 06 67 d0 9a e5 8c 62 4d 9a 69 a1 e9 f9 76 74 3a cd c7 10 33 0c 60 5a e6 9c f3 c9 da 58 5f 5f 4f b9 e4 47 71 e8 38 bc dd 6e cb 2c 2b 95 4a 2a 97 da e4 9f 38 e6 b0 bf fb bb bd 87 66 73 0e 68 c4 79 1e ab 0c 36 b7 38 e7 8c 93 c5 34 60 43 5b eb d7 e9 0f bc ef 88 27 1e 5f b7 64 bb 3d a3 44 6b 45 85 a2 f7 f4 b3 bf 7d cd 5e 8b cf 5b 7a e2 eb de 38 0c 20 92 53 be 60 9b 27 46 e7 f6 2f fa 23 8e 32 00 2f 34 bc dd 0a 7f 61 10 c3 8b c0 cb c3 d1 2e f4 7f f2 78 cb 79 07 40 ad 76 1a 14 83 34 53 8c 31 21 a8 d9 08 6d db 75 6c fe d3 7b 1e fd f8 c7 8e f7 dd de 34 66 e5 d2 10 19 b7 d3 4e c7 26 d6 1c 71 f4 db ce 3a f7 38 21 28 8e Data Ascii: $_h3"RqKAunT;5GisR&gbMivt:3`ZX__OGq8n,+J*8fshy684`C['_d=DkE}^[z8 S`F/#2/4a.xy@v4S1!mul{4fN&q:8!(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49699	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:24 UTC	1	OUT	GET /ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 HTTP/1.1 Host: nrzs-zcmp.campaign-view.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:25 UTC	5	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: text/html;charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: 1e5a17c8ab=38d19ed51de33532d3b7e87a22c4d973; Path=/ X-Content-Type-Options: nosniff X-XSS-Protection: 1 Set-Cookie: ZCAMPAIGN_CSRF_TOKEN=6dbc78ab-4589-4358-baa1-ed77de15c5db;path=/;SameSite=None;Secure;priority=high Set-Cookie: _zcsr_tmp=6dbc78ab-4589-4358-baa1-ed77de15c5db;path=/;SameSite=Strict;Secure;priority=high Pragma: no-cache Cache-Control: private,no-cache,no-store,max-age=0,must-revalidate Expires: Thu, 01 Jan 1970 00:00:00 GMT X-Frame-Options: SAMEORIGIN Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Cache-Control, Pragma, Origin, Authorization, Content-Type, X-Requested-With Access-Control-Allow-Methods: GET,POST,OPTIONS Set-Cookie: JSESSIONID=2D2561E620E609AC020ED2EC3D99E714; Path=/; Secure; HttpOnly vary: accept-encoding Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:25 UTC	6	IN	Data Raw: 31 63 62 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 49 4e 46 4f 52 4d 41 54 49 4f 4e 20 41 42 4f 55 54 20 46 4c 49 47 48 54 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 21 2d 2d 20 54 77 69 74 74 65 72 20 4d 65 74 61 20 54 61 67 73 20 2d 2d 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 63 61 72 64 22 20 63 6f 6e 74 65 6e 74 3d 22 73 75 6d 6d 61 72 79 22 3e 3c 6d 65 74 61 20 6e 61 Data Ascii: 1cb3<!DOCTYPE html ><html xmlns="http://www.w3.org/1999/xhtml"><head><title>INFORMATION ABOUT FLIGHT</title><meta content="text/html;charset=UTF-8" http-equiv="Content-Type">... Twitter Meta Tags --><meta name="twitter:card" content="summary"><meta na
2022-10-03 15:40:25 UTC	21	IN	Data Raw: 0a 09 09 09 09 63 68 61 72 43 6e 74 2e 68 74 6d 6c 28 30 29 3b 0a 09 09 09 09 73 75 63 42 6f 78 2e 68 74 6d 6c 28 22 59 6f 75 72 20 63 6f 6d 6d 65 6e 74 20 61 64 64 65 64 20 73 75 63 63 65 73 73 66 75 6c 6c 79 2e 22 29 2e 66 61 64 65 4f 75 74 28 35 30 30 30 29 3b 0a 09 09 09 09 62 74 6e 2e 68 74 6d 6c 28 22 50 6f 73 74 22 29 3b 0a 0a 09 09 7d 0a 09 09 7d 29 3b 0a 09 7d 0a 09 65 6c 73 65 0a 09 7b 0a 09 09 65 72 72 42 6f 78 2e 68 74 6d 6c 28 22 45 6e 74 65 72 65 64 20 4d 6f 72 65 20 74 68 61 6e 20 32 35 30 20 43 68 61 72 61 63 74 65 72 73 2e 22 29 3b 0a 09 7d 0a 0a 7d 0a 09 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 0a 09 09 09 66 75 6e 63 74 69 6f 6e 20 28 29 0a 09 09 09 7b 0a 09 09 09 69 66 20 28 74 6f 70 20 3d 3d 3d 20 73 65 6c 66 29 20 0a Data Ascii: charCnt.html(0);sucBox.html("Your comment added successfully.").fadeOut(5000);btn.html("Post");}});}else{errBox.html("Entered More than 250 Characters.");}}$(document).ready(function (){if (top === self)

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	37	IN	Data Raw: 0a 09 09 09 09 09 69 66 20 28 64 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 69 64 29 29 20 7b 72 65 74 75 72 6e 3b 7d 0a 09 09 09 09 09 6a 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 73 29 3b 20 6a 73 2e 69 64 20 3d 20 69 64 3b 0a 09 09 09 09 09 6a 73 2e 73 72 63 20 3d 20 22 22 3b 0a 09 09 09 09 09 66 6a 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 6a 73 2c 20 66 6a 73 29 3b 0a 09 09 09 09 7d 28 64 6f 63 75 6d 65 6e 74 2c 0d 0a 31 30 30 30 0d 0a 20 27 73 63 72 69 70 74 27 2c 20 27 66 61 63 65 62 6f 6f 6b 2d 6a 73 73 64 6b 27 29 29 3b 0a 09 09 09 09 0a 09 09 09 09 0a 09 09 09 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 74 79 6c 65 3e 0a 2e 7a 63 76 62 62 61 6e 64 62 67 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 Data Ascii: if (d.getElementById(id)) {return;}js = d.createElement(s); js.id = id;js.src = "";fjs.parentNode.insertBefore(js, fjs);}(document,1000 'script', 'facebook-jssdk'));</script><style>.zcvbbandbg{ background-c
2022-10-03 15:40:25 UTC	53	IN	Data Raw: 09 09 09 09 09 09 09 09 09 09 3c 61 20 76 61 6c 75 65 20 3d 22 70 6c 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 20 63 6f 6c 6f 72 3a 23 33 33 33 3b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 20 20 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 22 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 3b 22 20 6f 6e 63 6c 69 63 6b 3d 22 74 72 61 6e 73 6c 61 74 65 54 6f 4c 61 6e 67 28 27 70 6c 27 29 22 3e 50 6f 6c 69 73 68 3c 2f 61 3e 0a 09 09 09 09 09 09 09 09 09 09 3c 61 20 76 61 6c 75 65 20 3d 22 70 74 22 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 20 63 6f 6c 6f 72 3a 23 33 33 33 3b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 20 20 77 68 69 74 Data Ascii: Polish<a value ="pt" style="font-size:12px; color:#333; text-decoration:none; whit
2022-10-03 15:40:25 UTC	69	IN	Data Raw: 09 09 6f 76 65 72 4c 61 79 53 68 6f 77 48 69 64 65 28 29 3b 09 0a 09 09 09 09 09 09 09 09 09 7d 0a 09 09 09 09 09 09 09 09 09 2f 2f 24 28 22 23 47 50 6c 75 73 44 69 76 22 29 2e 68 69 64 65 28 29 3b 09 09 0a 09 09 09 09 09 09 09 09 09 2f 2f 24 28 22 23 6d 65 64 69 61 4f 76 65 72 4c 61 79 22 29 2e 68 69 64 65 28 29 3b 09 09 0a 09 09 09 09 09 09 09 09 09 7d 0a 09 09 09 09 09 09 09 09 09 7d 29 3b 0a 09 09 09 09 09 09 09 09 7d 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 21 2d 2d 20 47 6f 6f 6f 67 6c 65 2b 20 45 4e 44 20 0d 0a 33 65 66 30 0d 0a 2d 2d 3e 0a 3c 21 2d 2d 20 54 75 6d 62 6c 72 20 53 68 61 72 65 20 53 74 61 72 74 20 20 2d 2d 3e 0a 0a 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 Data Ascii: overLayShowHide();}//$("#GPlusDiv").hide();//$("#mediaOverLay").hide();}});}</script> ... Goooogle+ ENDD 3ef0-->... Tumblr Share Start --><div class="

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49701	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	85	OUT	GET /js/jquery-1.11.0.min.js HTTP/1.1 Host: nrzs-zcmp.campaign-view.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: 1e5a17c8ab=38d19ed51de33532d3b7e87a22c4d973; ZCAMPAIGN_CSRF_TOKEN=6dbc78ab-4589-4358-baa1-ed77de15c5db; _zcsr_tmp=6dbc78ab-4589-4358-baa1-ed77de15c5db; JSESSIONID=2D2561E620E609AC020ED2EC3D99E714
2022-10-03 15:40:25 UTC	86	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: application/javascript Content-Length: 96381 Connection: close Accept-Ranges: bytes ETag: W/"96381-1664603880000" Last-Modified: Sat, 01 Oct 2022 05:58:00 GMT Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:25 UTC	87	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 31 2e 31 31 2e 30 20 7c 20 28 63 29 20 32 30 30 35 2c 20 32 30 31 34 20 6a 51 75 65 72 79 20 46 6f 75 6e 64 61 74 69 6f 6e 2c 20 49 6e 63 2e 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 61 2e 64 6f 63 75 6d 65 6e 74 3f 62 28 61 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 21 61 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 20 72 65 71 75 69 72 65 73 20 61 20 77 69 6e Data Ascii: /*! jQuery v1.11.0	(c) 2005, 2014 jQuery Foundation, Inc.	jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a win

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	119	IN	Data Raw: 6e 67 74 68 3b 77 68 69 6c 65 28 68 2d 2d 29 28 66 3d 67 5b 68 5d 29 26 26 28 61 5b 68 5d 3d 21 28 62 5b 68 5d 3d 66 29 29 7d 29 3a 66 75 6e 63 74 69 6f 6e 28 61 2c 65 2c 66 29 7b 72 65 74 75 72 6e 20 62 5b 30 5d 3d 61 2c 64 28 62 2c 6e 75 6c 6c 2c 66 2c 63 29 2c 21 63 2e 70 6f 70 28 29 7d 7d 29 2c 68 61 73 3a 66 62 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 62 29 7b 72 65 74 75 72 6e 20 64 62 28 61 2c 62 29 2e 6c 65 6e 67 74 68 3e 30 7d 7d 29 2c 63 6f 6e 74 61 69 6e 73 3a 66 62 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 62 29 7b 72 65 74 75 72 6e 28 62 2e 74 65 78 74 43 6f 6e 74 65 6e 74 7c 7c 62 2e 69 6e 6e 65 72 54 65 78 74 7c 7c 65 28 62 29 29 2e 69 6e 64 65 78 4f Data Ascii: ngth;while(h--)(f=g[h])&&(a[h]=!(b[h]=f))}):function(a,e,f){return b[0]=a,d(b,null,f,c),!c.pop()}}),has:fb(function(a){return function(b){return db(a,b).length>0}}),contains:fb(function(a){return function(b){return(b.textContent||b.innerText||e(b)).indexO
2022-10-03 15:40:25 UTC	171	IN	Data Raw: 2e 6e 6f 64 65 54 79 70 65 2c 67 3d 66 3f 6e 2e 63 61 63 68 65 3a 61 2c 68 3d 66 3f 61 5b 6e 2e 65 78 70 61 6e 64 6f 5d 3a 6e 2e 65 78 70 61 6e 64 6f 3b 69 66 28 67 5b 68 5d 29 7b 69 66 28 62 26 26 28 64 3d 63 3f 67 5b 68 5d 3a 67 5b 68 5d 2e 64 61 74 61 29 29 7b 6e 2e 69 73 41 72 72 61 79 28 62 29 3f 62 3d 62 2e 63 6f 6e 63 61 74 28 6e 2e 6d 61 70 28 62 2c 6e 2e 63 61 6d 65 6c 43 61 73 65 29 29 3a 62 20 69 6e 20 64 3f 62 3d 5b 62 5d 3a 28 62 3d 6e 2e 63 61 6d 65 6c 43 61 73 65 28 62 29 2c 62 3d 62 20 69 6e 20 64 3f 5b 62 5d 3a 62 2e 73 70 6c 69 74 28 22 20 22 29 29 2c 65 3d 62 2e 6c 65 6e 67 74 68 3b 77 68 69 6c 65 28 65 2d 2d 29 64 65 6c 65 74 65 20 64 5b 62 5b 65 5d 5d 3b 69 66 28 63 3f 21 51 28 64 29 3a 21 6e 2e 69 73 45 6d 70 74 79 4f 62 6a 65 63 74 Data Ascii: .nodeType,g=f?n.cache:a,h=f?a[n.expando]:n.expando;if(g[h]){if(b&&(d=c?g[h]:g[h].data)){n.isArray(b)?b=b.concat(n.map(b,n.camelCase)):b in d?b=[b]:(b=n.camelCase(b),b=b in d?[b]:b.split(" ")),e=b.length;while(e--)delete d[b[e]];if(c?!Q(d):!n.isEmptyObject
2022-10-03 15:40:25 UTC	187	IN	Data Raw: 5b 65 5d 29 3b 65 2b 2b 29 21 62 7c 7c 6e 2e 6e 6f 64 65 4e 61 6d 65 28 64 2c 62 29 3f 66 2e 70 75 73 68 28 64 29 3a 6e 2e 6d 65 72 67 65 28 66 2c 76 62 28 64 2c 62 29 29 3b 72 65 74 75 72 6e 20 76 6f 69 64 20 30 3d 3d 3d 62 7c 7c 62 26 26 6e 2e 6e 6f 64 65 4e 61 6d 65 28 61 2c 62 29 3f 6e 2e 6d 65 72 67 65 28 5b 61 5d 2c 66 29 3a 66 7d 66 75 6e 63 74 69 6f 6e 20 77 62 28 61 29 7b 58 2e 74 65 73 74 28 61 2e 74 79 70 65 29 26 26 28 61 2e 64 65 66 61 75 6c 74 43 68 65 63 6b 65 64 3d 61 2e 63 68 65 63 6b 65 64 29 7d 66 75 6e 63 74 69 6f 6e 20 78 62 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 6e 2e 6e 6f 64 65 4e 61 6d 65 28 61 2c 22 74 61 62 6c 65 22 29 26 26 6e 2e 6e 6f 64 65 4e 61 6d 65 28 31 31 21 3d 3d 62 2e 6e 6f 64 65 54 79 70 65 3f 62 3a 62 2e 66 69 72 73 Data Ascii: [e]);e++)!b||n.nodeName(d,b)?f.push(d):n.merge(f,vb(d,b));return void 0===b||b&&n.nodeName(a,b)?n.merge([a],f):f}function wb(a){X.test(a.type)&&(a.defaultChecked=a.checked)}function xb(a,b){return n.nodeName(a,"table")&&n.nodeName(11!==b.nodeType?b:b.firs
2022-10-03 15:40:25 UTC	203	IN	Data Raw: 2b 74 68 69 73 2e 73 74 61 72 74 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 73 74 65 70 26 26 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 73 74 65 70 2e 63 61 6c 6c 28 74 68 69 73 2e 65 6c 65 6d 2c 74 68 69 73 2e 6e 6f 77 2c 74 68 69 73 29 2c 63 26 26 63 2e 73 65 74 3f 63 2e 73 65 74 28 74 68 69 73 29 3a 24 62 2e 70 72 6f 70 48 6f 6f 6b 73 2e 5f 64 65 66 61 75 6c 74 2e 73 65 74 28 74 68 69 73 2c 74 68 69 73 7d 7d 2c 24 62 2e 70 72 6f 74 6f 74 79 70 65 2e 69 6e 69 74 2e 70 72 6f 74 6f 74 79 70 65 3d 24 62 2e 70 72 6f 74 6f 74 79 70 65 2c 24 62 2e 70 72 6f 70 48 6f 6f 6b 73 3d 7b 5f 64 65 66 61 75 6c 74 3a 7b 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3b 72 65 74 75 72 6e 20 6e 75 6c 6c 3d 3d 61 2e 65 6c 65 6d 5b 61 2e 70 72 6f 70 5d 7c 7c Data Ascii: +this.start,this.options.step&&this.options.step.call(this.elem,this.now,this),c&&c.set?c.set(this):$b.propHooks._default.set(this),this}},$b.prototype.init.prototype=$b.prototype,$b.propHooks={_default:{get:function(a){var b;return null==a.elem[a.prop]||
2022-10-03 15:40:25 UTC	219	IN	Data Raw: 72 41 74 28 30 29 3f 28 64 3d 64 2e 73 6c 69 63 65 28 31 29 7c 7c 22 2a 22 2c 28 61 5b 64 5d 3d 61 5b 64 5d 7c 7c 5b 5d 29 2e 75 6e 73 68 69 66 74 28 63 29 29 3a 28 61 5b 64 5d 3d 61 5b 64 5d 7c 7c 5b 5d 29 2e 70 75 73 68 28 63 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 4e 63 28 61 2c 62 2c 63 2c 64 29 7b 76 61 72 20 65 3d 7b 7d 2c 66 3d 61 3d 3d 3d 4a 63 3b 66 75 6e 63 74 69 6f 6e 20 67 28 68 29 7b 76 61 72 20 69 3b 72 65 74 75 72 6e 20 65 5b 68 5d 3d 21 30 2c 6e 2e 65 61 63 68 28 61 5b 68 5d 7c 7c 5b 5d 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 68 29 7b 76 61 72 20 6a 3d 68 28 62 2c 63 2c 64 29 3b 72 65 74 75 72 6e 22 73 74 72 69 6e 67 22 21 3d 74 79 70 65 6f 66 20 6a 7c 7c 66 7c 7c 65 5b 6a 5d 3f 66 3f 21 28 69 3d 6a 29 3a 76 6f 69 64 20 30 3a 28 62 2e 64 61 74 61 Data Ascii: rAt(0)?(d=d.slice(1)||"*",(a[d]=a[d]||[]).unshift(c)):(a[d]=a[d]||[]).push(c)}}function Nc(a,b,c,d){var e={},f=a===Jc;function g(h){var i;return e[h]=!0,n.each(a[h]||[],function(a,h){var j=h(b,c,d);return"string"!=typeof j||f||e[j]?f?!(i=j):void 0:(b.data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49705	185.230.212.228	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	86	OUT	GET /zohocampaigns/pmm_zc_v9_120907000001935004.png HTTP/1.1 Host: campaign-image.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	102	IN	HTTP/1.1 200 OK Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: image/png Content-Length: 72470 Connection: close Set-Cookie: 45342b9b1e=0a49ff5c1535be0fc90fdb69cb1fd4a5; Path=/ Cache-Control: no-cache Last-Modified: Sun, 2 Oct 2022 23:22:29 GMT Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:25 UTC	103	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 e1 00 00 00 e1 08 02 00 00 00 b1 d1 45 2d 00 00 00 03 73 42 49 54 08 08 08 db e1 4f e0 00 00 20 00 49 44 41 54 78 9c ec bd 77 98 26 55 b5 35 be f6 39 a7 f2 9b 3b 4c 4f 0e 4c 60 c8 02 02 06 82 88 82 01 f1 7a af 0a 06 50 c1 2b c9 44 52 f2 c8 90 25 89 12 e4 0a 82 62 c2 2b 88 81 a8 08 8a 12 25 83 33 0c 93 43 e7 ee 37 55 3e e1 f7 c7 db 13 c0 f4 78 bf 1f 7c df dc 67 d6 d3 4f 4d 77 75 4f bd 55 75 56 ed b3 f7 d9 6b ef 22 63 0c b6 e1 ef 63 e2 f6 10 00 0d e4 40 0e 64 80 01 68 60 64 c8 73 2a 85 a0 ca 99 03 83 76 0b 85 02 14 14 67 ba f3 7f d3 3c 65 8c 59 dc 52 46 71 e2 40 e7 20 9b b6 00 18 c1 02 d8 1b 7b 4d 5b 19 68 1b 47 ff 31 b6 b8 3b 1a d0 80 02 e4 c6 3d 0c 10 cd 56 a8 24 55 ab 65 18 80 90 66 b1 63 b3 5c 29 Data Ascii: PNGIHDRE-sBITO IDATxw&U59;LOL`zP+DR%b+%3C7U>x|gOMwuOUuVk"cc@dh`ds*vg<eYRFq@ {M [hG1;=V$Uefc\)
2022-10-03 15:40:25 UTC	137	IN	Data Raw: 2b a8 5e 12 d8 1d c2 a1 37 fc c9 46 64 d8 c0 c1 61 68 34 ac 23 04 8d db ba 59 3a c5 77 9e c1 77 ad db 3f ef 44 7e 2e e5 54 cb 9f 1e f5 cb 9d 6b 75 06 08 2e bc ec ee 7d 0e 59 f0 f8 cb 85 bb 1f 59 75 c0 2f ae e8 2e 40 b9 06 e5 4a f8 ab 53 f6 0d bd 6f 62 86 ed fa fc ad 25 cb 43 0e 0c 60 d4 84 91 93 b6 9c 74 ec f1 a7 be ff d1 5a db 03 2e 40 96 55 15 c1 ac 99 5b fb 91 83 08 4c 98 3c 15 2b 60 45 b0 a6 d0 db 35 d8 db 3e 6e c6 ef 16 de 8a 28 30 00 8f 13 84 a0 6b 4d 01 61 05 a8 bd cd f6 13 b2 69 13 20 a8 f9 e1 2e 7b ee b3 fd 9c 8b 1e 5b 54 5f f9 35 14 06 fa 80 5b 91 d7 ad 2a 7d d7 5d 7b d2 d1 87 ce 75 fd 7e 19 86 10 25 0c a0 52 86 9f ce 1c f3 ec 13 8f 14 fb 36 52 e0 eb d7 ac 9a b8 c5 b8 42 71 60 93 2a 1c 7a 87 37 95 85 31 60 02 98 0c 19 99 c6 0d c5 42 e0 21 30 cc Data Ascii: +^7Fdah4#Y:ww?D~.Tku.}YYu/.@JSob%C`tZ.@U[L<+`E5>n(0kMai .{[T_5[*]]{u~%R6RBq`*z71`B!0
2022-10-03 15:40:25 UTC	153	IN	Data Raw: 4b d7 22 bc 95 4c 25 89 88 f5 1e 6d a8 fe c5 6b 32 2f ce ce b7 2a 08 6c 2c 09 6a 7b 29 20 01 d8 c7 b8 59 9f 0b 7a 33 ce 9a 45 2b 7f fd 73 ef cc 39 90 41 00 12 3c 13 00 38 03 7e e9 f9 e7 de 76 e7 83 86 e9 50 c5 0c 0c a0 44 67 47 ef d1 d1 23 8b 56 36 c7 e7 b6 71 75 b4 d8 59 49 6a 1d 8c 2e c7 54 57 83 69 9e 86 d0 f0 6d 19 18 86 41 35 58 4c c5 e9 cf b3 ed f8 e7 82 b3 8b a3 44 38 65 da 9d 0a 01 24 4d 8d 19 46 ad 5c 6e 6a 59 11 e7 8b 87 67 27 1e ed 5f e9 34 fa b0 97 2d de 78 93 2f 02 dc 18 67 07 0e d6 9f 3f b0 45 c0 52 ad 04 65 14 2b 25 52 5f 0b be 65 d3 96 30 82 82 2d ca a6 05 10 45 51 13 74 c6 b5 3a 12 0c 6b d6 d9 0f 3c 3f cd 53 4b 52 c2 8c 98 b2 c0 04 4f 80 61 9b 65 95 36 a5 a0 9c 58 44 cb 56 3d 15 18 3c 0a 22 26 29 57 00 8e 69 71 c4 fc 84 83 89 96 94 cb 17 Data Ascii: K"L%mk2/*l,j{) Yz3E+s9A<8~vPDgG#V6quYIj.TWimA5XLD8e$MF\njYg'_4-x/g?ERe+%R_e0-EQt:k<?SKRO ae6XDV=<"&)Wiq
2022-10-03 15:40:25 UTC	240	IN	Data Raw: 57 13 a7 6f 24 b0 bd 72 b4 0c 98 9a 06 d6 2d 65 64 bc 51 e5 1c 80 4c ee 69 73 ea e3 63 2b 57 c6 68 c6 e5 5e df 84 de ef 07 16 f5 4c 49 18 54 38 91 c0 8a 26 05 93 42 22 29 51 2b 29 5f 73 cb 12 42 d8 a6 15 85 7c 68 e5 30 06 9e 4d 65 97 2c 59 7a e9 9c af 6e bb 4a bb f4 a2 33 76 dc 79 aa 00 68 b8 fe 4e 7b 6e b4 eb 5e 9b 7d fc d1 b2 13 4e 3c ab 52 ab 66 d2 ed ba 61 54 ca 25 a2 e8 b6 95 74 9b 0d 85 62 a6 00 a1 92 0b 08 7d 30 4d 00 80 44 42 07 60 3f 56 e2 ff 63 d6 47 ff b5 60 86 a4 10 3c 2c 0c af cc 25 d3 dd 6d 5d 85 91 f1 e2 58 01 89 a0 56 5f 59 6f 2e 3b ef a2 a3 5e 78 f5 ba 43 8f dc 58 33 00 63 28 96 9d cf 3f 5b ba db 1e 47 9d 72 da 79 df 2e 19 ea ea 9d 8a 69 1c 90 ae a8 d6 f2 81 55 52 60 00 22 05 91 02 03 20 90 58 b6 7c 8d b8 6b 27 d4 50 f2 42 a9 e2 d7 9c de Data Ascii: Wo$r-edQLisc+Wh^LIT8&B")Q+)_sB|h0Me,YznJ3vyhN{n^}N<RfaT%tb}0MDB`?VcG`<,%m]XV_Yo.;^xCX3c(? [Gry.iUR`" X|k'PB
2022-10-03 15:40:25 UTC	256	IN	Data Raw: 98 24 c2 0c 5f a1 c1 0c 18 cd 68 12 b7 dc 33 22 c6 85 c5 85 86 d1 52 71 4b 90 41 9a 75 a4 6e f5 54 07 3b 35 47 69 d7 73 1c cd 52 d7 c9 9b 9d 26 d3 ae 06 67 d0 9a e5 8c 62 4d 9a 69 a1 e9 f9 76 74 3a cd c7 10 33 0c 60 5a e6 9c f3 c9 da 58 5f 5f 4f b9 e4 47 71 e8 38 bc dd 6e cb 2c 2b 95 4a 2a 97 da e4 9f 38 e6 b0 bf fb bb bd 87 66 73 0e 68 c4 79 1e ab 0c 36 b7 38 e7 8c 93 c5 34 60 43 5b eb d7 e9 0f bc ef 88 27 1e 5f b7 64 bb 3d a3 44 6b 45 85 a2 f7 f4 b3 bf 7d cd 5e 8b cf 5b 7a e2 eb de 38 0c 20 92 53 be 60 9b 27 46 e7 f6 2f fa 23 8e 32 00 2f 34 bc dd 0a 7f 61 10 c3 8b c0 cb c3 d1 2e f4 7f f2 78 cb 79 07 40 ad 76 1a 14 83 34 53 8c 31 21 a8 d9 08 6d db 75 6c fe d3 7b 1e fd f8 c7 8e f7 dd de 34 66 e5 d2 10 19 b7 d3 4e c7 26 d6 1c 71 f4 db ce 3a f7 38 21 28 8e Data Ascii: $_h3"RqKAunT;5GisR&gbMivt:3`ZX__OGq8n,+J*8fshy684`C['_d=DkE}^[z8 S`F/#2/4a.xy@v4S1!mul{4fN&q:8! (

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49708	185.230.212.112	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	118	OUT	GET /campaigns/static2/images/spacer.gif HTTP/1.1 Host: img.zohostatic.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	170	IN	HTTP/1.1 200 OK Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: image/gif Content-Length: 43 Last-Modified: Mon, 03 Oct 2022 13:27:43 GMT Connection: close ETag: "633ae34f-2b" Expires: Tue, 03 Oct 2023 15:40:25 GMT Cache-Control: max-age=31536000 X-Robots-Tag: noindex, nofollow, nosnippet, noarchive Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Strict-Transport-Security: max-age=63072000 Accept-Ranges: bytes
2022-10-03 15:40:25 UTC	170	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 ff ff ff 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49702	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	135	OUT	GET /js/jquery-migrate-1.2.1.min.js HTTP/1.1 Host: nrzs-zcmp.campaign-view.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: 1e5a17c8ab=38d19ed51de33532d3b7e87a22c4d973; ZCAMPAIGN_CSRF_TOKEN=6dbc78ab-4589-4358-baa1-ed77de15c5db; _zcsr_tmp=6dbc78ab-4589-4358-baa1-ed77de15c5db; JSESSIONID=2D2561E620E609AC020ED2EC3D99E714
2022-10-03 15:40:25 UTC	233	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: application/javascript Content-Length: 7199 Connection: close Accept-Ranges: bytes ETag: W/"7199-1664603880000" Last-Modified: Sat, 01 Oct 2022 05:58:00 GMT vary: accept-encoding Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:25 UTC	233	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 4d 69 67 72 61 74 65 20 76 31 2e 32 2e 31 20 7c 20 28 63 29 20 32 30 30 35 2c 20 32 30 31 33 20 6a 51 75 65 72 79 20 46 6f 75 6e 64 61 74 69 6f 6e 2c 20 49 6e 63 2e 20 61 6e 64 20 6f 74 68 65 72 20 63 6f 6e 74 72 69 62 75 74 6f 72 73 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0a 6a 51 75 65 72 79 2e 6d 69 67 72 61 74 65 4d 75 74 65 3d 3d 3d 76 6f 69 64 20 30 26 26 28 6a 51 75 65 72 79 2e 6d 69 67 72 61 74 65 4d 75 74 65 3d 21 30 29 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 66 75 6e 63 74 69 6f 6e 20 72 28 6e 29 7b 76 61 72 20 72 3d 74 2e 63 6f 6e 73 6f 6c 65 3b 69 5b 6e 5d 7c 7c 28 69 5b 6e 5d 3d 21 30 2c 65 2e 6d 69 67 72 61 74 65 57 61 72 6e 69 6e 67 73 2e 70 75 73 68 28 6e 29 2c 72 Data Ascii: /*! jQuery Migrate v1.2.1 | (c) 2005, 2013 jQuery Foundation, Inc. and other contributors | jquery.org/license */jQuery.migrateMute===void 0&&(jQuery.migrateMute=!0),function(e,t,n){function r(n){var r=t.console;i[n]||(i[n]=!0,e.migrateWarnings.push(n),r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49703	185.230.212.128	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	136	OUT	GET /images/viewinbrowserarw.png HTTP/1.1 Host: nrzs-zcmp.campaign-view.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: 1e5a17c8ab=38d19ed51de33532d3b7e87a22c4d973; ZCAMPAIGN_CSRF_TOKEN=6dbc78ab-4589-4358-baa1-ed77de15c5db; _zcsr_tmp=6dbc78ab-4589-4358-baa1-ed77de15c5db; JSESSIONID=2D2561E620E609AC020ED2EC3D99E714
2022-10-03 15:40:25 UTC	270	IN	HTTP/1.1 200 Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: image/png Content-Length: 1610 Connection: close Accept-Ranges: bytes ETag: W/"1610-1664603890000" Last-Modified: Sat, 01 Oct 2022 05:58:10 GMT Strict-Transport-Security: max-age=63072000
2022-10-03 15:40:25 UTC	270	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 47 00 00 00 17 08 06 00 00 00 59 3e 52 e8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 Data Ascii: PNGIHDRGY>RtEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49709	185.230.212.112	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	169	OUT	GET /campaigns/static2/images/viewinbrowserarw.png HTTP/1.1 Host: img.zohostatic.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:25 UTC	264	IN	HTTP/1.1 200 OK Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: image/png Content-Length: 1610 Last-Modified: Mon, 03 Oct 2022 13:27:43 GMT Connection: close ETag: "633ae34f-64a" Expires: Tue, 03 Oct 2023 15:40:25 GMT Cache-Control: max-age=31536000 X-Robots-Tag: noindex, nofollow, nosnippet, noarchive Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Strict-Transport-Security: max-age=63072000 Accept-Ranges: bytes

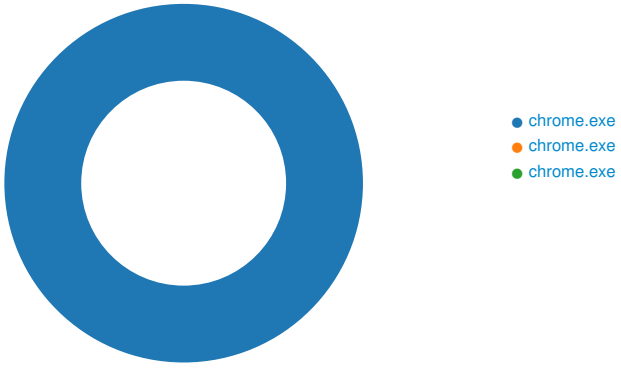
Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	264	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 47 00 00 00 17 08 06 00 00 00 59 3e 52 e8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 Data Ascii: PNGIHDRGY>RtEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W 5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49706	185.230.212.112	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:40:25 UTC	169	OUT	GET /campaigns/static2/images/zc_tmblrpost.jpg HTTP/1.1 Host: img.zohostatic.eu Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://nrzs-zcmp.campaign-view.eu/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 15:40:25 UTC	266	IN	HTTP/1.1 404 Not Found Server: ZGS Date: Mon, 03 Oct 2022 15:40:25 GMT Content-Type: text/html Content-Length: 520 Connection: close
2022-10-03 15:40:25 UTC	266	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page --><!-

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5752, Parent PID: 4896

General

Target ID:	0
Start time:	17:40:18
Start date:	03/10/2022
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:	low

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: 5792, Parent PID: 5752

General

Target ID:	1
Start time:	17:40:20
Start date:	03/10/2022
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=1944 --field-trial-handle=1624,i,17822862930805665288,9356387013567766339,131072 --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:	low

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: **5268**, Parent PID: **4896**

General

Target ID:	2
Start time:	17:40:21
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://nrzs-zcmp.campaign-view.eu/ua/viewinbrowser?od=3z7205bdc0eed4d029e75dd50d8440b373&rd=11ad8c46a1fb01b9&sd=11ad8c46a1fad4bf&n=11699e4c25537ae&mrd=11ad8c46a1fad4ad&m=1
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:	low

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