ID: 708244
Sample Name: 321 Amita Technical 16.09.2022.exe
Cookbook: default.jbs
Time: 07:59:04
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

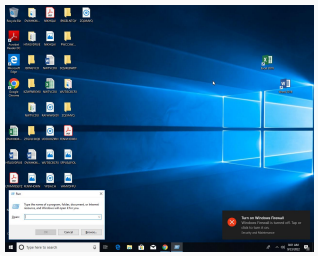
Windows Analysis Report

321 Amita Technical 16.09.2022.exe

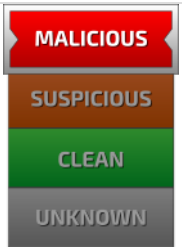
Overview

General Information

Sample Name:	321 Amita Technical 16.09.2022.exe
Analysis ID:	708244
MD5:	a2a924c124bbc5..
SHA1:	7ce1c45be6abf2...
SHA256:	9d45370a27c724..
Tags:	exe
Infos:	



Detection



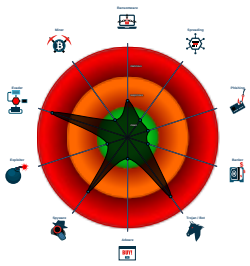
AgentTesla, DarkTortilla

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

Signatures

- Yara detected DarkTortilla Crypter
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected AgentTesla
- Tries to harvest and steal Putty / W...
- Machine Learning detection for sam...
- .NET source code contains method ...
- .NET source code contains very larg...
- Hides that the sample has been dow...
- Moves itself to temp directory
- Queries sensitive network adapter in...
- Tries to harvest and steal browser in...

Classification



Process Tree

- **System is w10x64**
- 321 Amita Technical 16.09.2022.exe (PID: 5436 cmdline: "C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe" MD5: A2A924C124BBC597A76495B4FB08F906)
  - phine.exe (PID: 5604 cmdline: "C:\Users\user\AppData\Local\Temp\phine.exe" MD5: A2A924C124BBC597A76495B4FB08F906)
    - InstallUtil.exe (PID: 5980 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "logs@multimetals.cfd",
  "Password": "multimetals.cfd",
  "Host": "asset@multimetals.cfd"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30184:$a13: get_DnsResolver • 0x2e986:$a20: get_LastAccessed • 0x30b16:$a27: set_InternalServerPort • 0x30e32:$a30: set_GuidMasterKey • 0x2ea8d:$a33: get_Clipboard • 0x2ea9b:$a34: get_Keyboard • 0x2fdb7:$a35: get_ShiftKeyDown • 0x2fdc8:$a36: get_AltKeyDown • 0x2eaa8:$a37: get_Password • 0x2f55e:$a38: get_PasswordHash • 0x30584:$a39: get_DefaultCredentials
00000000.00000002.343398236.00000000028F2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DarkTortilla	Yara detected DarkTortilla Crypter	Joe Security	
00000000.00000002.346179647.0000000002BC0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DarkTortilla	Yara detected DarkTortilla Crypter	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.phine.exe.3d366ba.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.phine.exe.3d366ba.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.phine.exe.3d366ba.2.unpack	JoeSecurity_DarkTortilla	Yara detected DarkTortilla Crypter	Joe Security	
1.2.phine.exe.3d366ba.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30e75:$s10: logins • 0x308dc:$s11: credential • 0x2ce85:$g1: get_Clipboard • 0x2ce93:$g2: get_Keyboard • 0x2cea0:$g3: get_Password • 0x2e19f:$g4: get_CtrlKeyDown • 0x2e1af:$g5: get_ShiftKeyDown • 0x2e1c0:$g6: get_AltKeyDown
1.2.phine.exe.3d366ba.2.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e57c:$a13: get_DnsResolver • 0x2cd7e:$a20: get_LastAccessed • 0x2ef0e:$a27: set_InternalServerPort • 0x2f22a:$a30: set_GuidMasterKey • 0x2ce85:$a33: get_Clipboard • 0x2ce93:$a34: get_Keyboard • 0x2e1af:$a35: get_ShiftKeyDown • 0x2e1c0:$a36: get_AltKeyDown • 0x2cea0:$a37: get_Password • 0x2d956:$a38: get_PasswordHash • 0x2e97c:$a39: get_DefaultCredentials
Click to see the 95 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

Yara detected DarkTortilla Crypter

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

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

Moves itself to temp directory

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

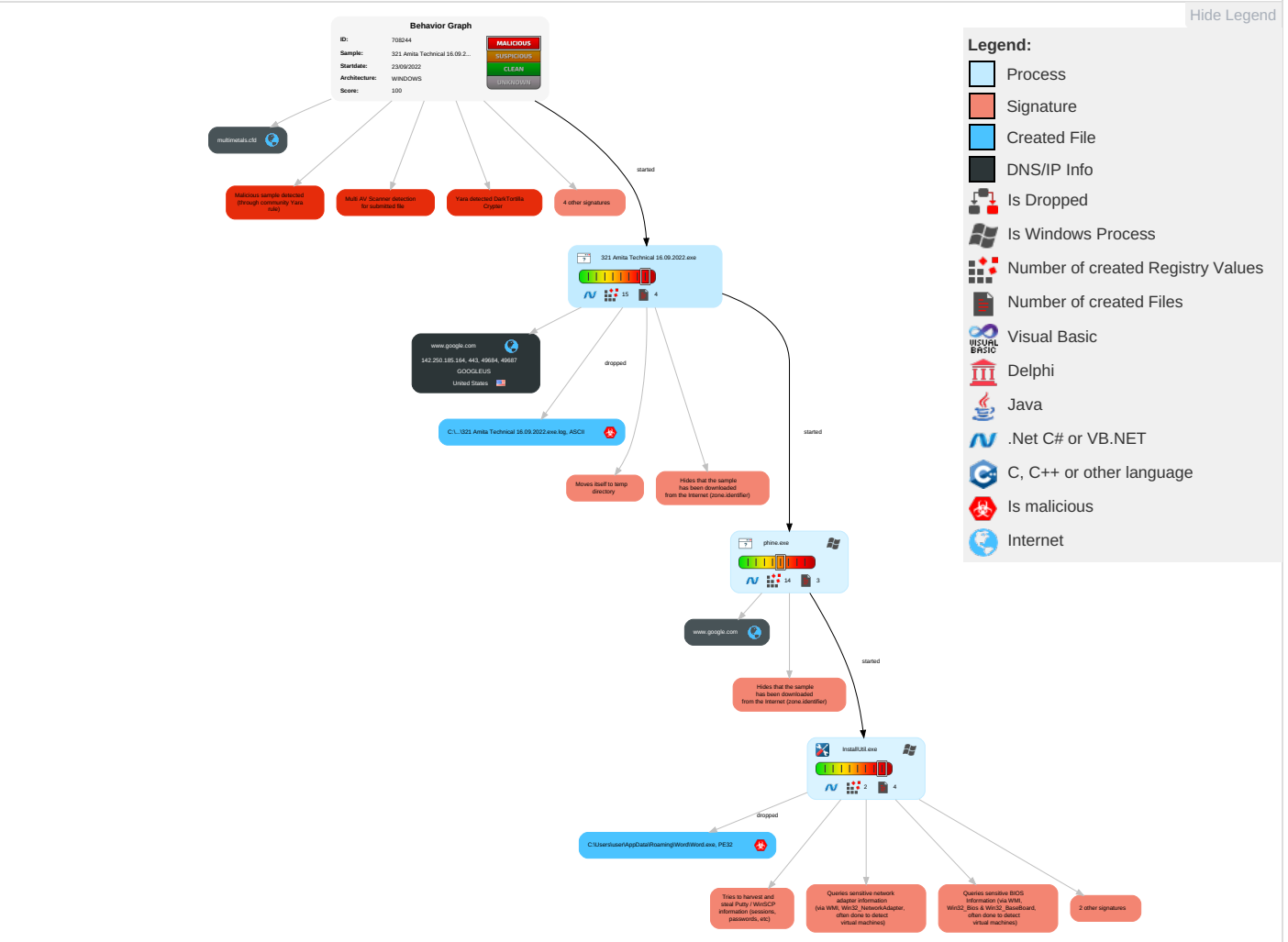
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 1 Masquerading	1 OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	1 1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

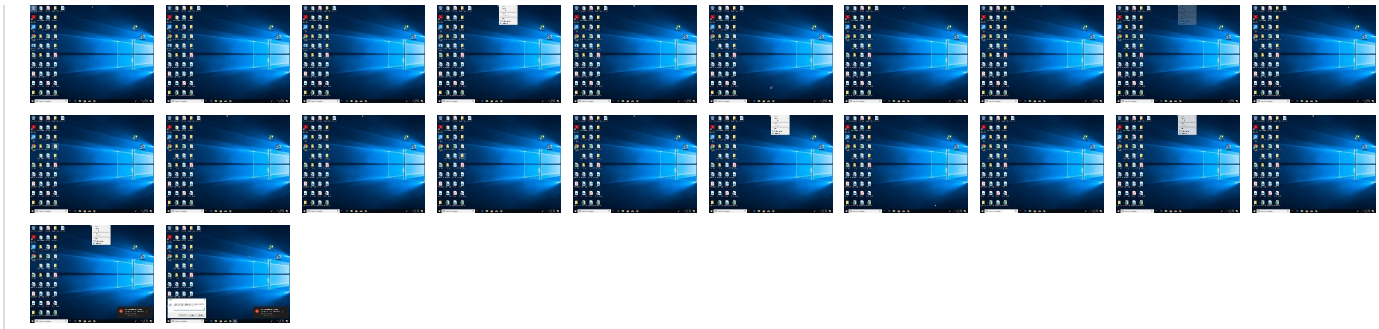
Behavior Graph



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
321 Amita Technical 16.09.2022.exe	65%	ReversingLabs	Win32.Trojan.AgentTesla	
321 Amita Technical 16.09.2022.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/M	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/1	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s_tr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.carterandcone.comV	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://cps.siths.se/sithsrootcav1.html0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.comg	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.carterandcone.comx	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://aTvxhlG42bxITzBzC.net	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnI	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/voit	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.m	0%	Avira URL Cloud	safe	
http://www.monotype.i	0%	Avira URL Cloud	safe	
http://multimetals.cfd	0%	Avira URL Cloud	safe	
http://jtKsKM.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
multimetals.cfd	192.185.37.183	true	false		unknown
www.google.com	142.250.185.164	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 00000004.00000002.562334194.00000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	InstallUtil.exe, 00000004.00000002.574556398.00000000000677C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-me.lv/repository0	InstallUtil.exe, 00000004.00000002.575530952.00000000006E7C000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.chambersign.org/chambersroot.crl0	InstallUtil.exe, 00000004.00000002.575954046.00000000006F18000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-int0	InstallUtil.exe, 00000004.00000002.576002903.00000000006F28000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.i.lencr.org/0W	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/M	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.chambersign.org1	InstallUtil.exe, 00000004.00000002.575954046.00000000006F18000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	InstallUtil.exe, 00000004.00000002.575982395.00000000006F25000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobe.c/g	phine.exe, 00000001.00000003.523826333.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.438631043.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361274706.00000000067A8000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360470623.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.523637270.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360882256.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360669570.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361500876.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com.	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308177419.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308304317.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 00000004.00000002.575677767.00000000006EC5000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.343046032.00000000028A1000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000002.527680627.00000000 02B91000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	InstallUtil.exe, 00000004.00000002.574332430.00000000006743000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 00000004.00000002.575677767.00000000006EC5000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/1	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.c.lencr.org/0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n-u	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308912197.000000000649D000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308752836.0000000006494000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://jtKsKM.com	InstallUtil.exe, 00000004.00000002.562334194.00000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.i	321 Amita Technical 16.09.2022.exe, 00000000.00000003.313615932.00000000064B0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	InstallUtil.exe, 00000004.00000002.562334194.00000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/s_tr	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308912197.000000000649D000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

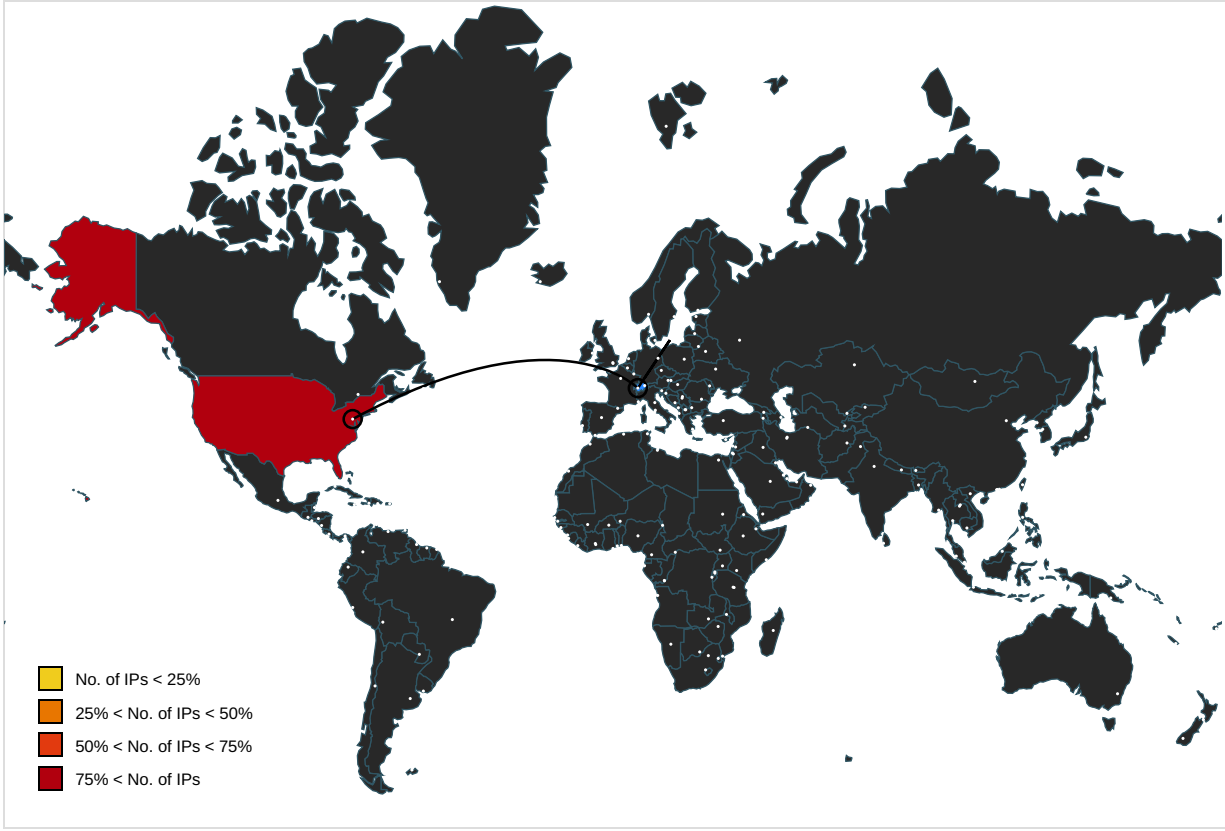
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comV	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/#	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308036488.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308177419.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308304317.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	321 Amita Technical 16.09.2022.exe, 00000000.00000002.343046032.00000000028A1000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000002.527680627.0000000002B91000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	InstallUtil.exe, 00000004.00000002.562334194.00000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://cps.root-x1.letsencrypt.org0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Z	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://multimetals.cfd	InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cps.letsencrypt.org0	InstallUtil.exe, 00000004.00000002.573913828.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570395017.0000000003490000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.cobj	phine.exe, 00000001.00000003.523826333.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.438631043.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361274706.00000000067A8000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360470623.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.523637270.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360882256.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360669570.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361061653.00000000067A9000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361500876.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	InstallUtil.exe, 00000004.00000002.575954046.00000006F18000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	InstallUtil.exe, 00000004.00000002.562334194.00000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	InstallUtil.exe, 00000004.00000002.562334194.00000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comlt	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308304317.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.hu/docs/	InstallUtil.exe, 00000004.00000002.575551872.00000006E80000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/D	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.siths.se/sithsrootcav1.html0	InstallUtil.exe, 00000004.00000002.575982395.00000006F25000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com.m	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	321 Amita Technical 16.09.2022.exe, 00000000.00000003.339673878.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.316580533.00000000064A1000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.316450459.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000002.354444180.00000000064A1000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.316177968.000000000649A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pki.digidentity.eu/validatie0	InstallUtil.exe, 00000004.00000002.574523943.00000006774000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.come.com	321 Amita Technical 16.09.2022.exe, 00000000.00000003.316580533.00000000064A1000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.316450459.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.316177968.000000000649A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comg	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comm	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308454333.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comk	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308304317.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/pc-root2.pdf0	InstallUtil.exe, 00000004.00000002.574332430.00000006743000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308036488.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308177419.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.disig.sk/ca0f	InstallUtil.exe, 00000004.00000002.575677767.00000006EC5000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comx	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308177419.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308304317.000000000649E000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308387580.000000000649F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/(	321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/voit	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308912197.000000000649D000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308752836.0000000006494000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308912197.000000000649D000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308752836.0000000006494000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.000000000649900.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/es-e	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308912197.000000000649D000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/adnl	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308973438.000000000649A000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309338640.0000000006499000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/i	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308752836.0000000006494000.00000004.00000800.00020000.00000000.sdmp, 321 Amita Technical 16.09.2022.exe, 00000000.00000003.309160709.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	321 Amita Technical 16.09.2022.exe, 00000000.00000002.354896208.00000000076A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.netlock.net/docs	InstallUtil.exe, 00000004.00000002.575500401.00000006E67000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnl	321 Amita Technical 16.09.2022.exe, 00000000.00000003.308036488.000000000649E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://aTvxhlG42bxITzBzC.net	InstallUtil.exe, 00000004.00000002.562334194.00000003131000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.570367604.000000000348A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1	phine.exe, 00000001.00000003.523826333.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.438631043.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361274706.00000000067A8000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360470623.00000000067A2000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.523637270.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360882256.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.360669570.00000000067A5000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361061653.00000000067A9000.00000004.00000800.00020000.00000000.sdmp, phine.exe, 00000001.00000003.361500876.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	InstallUtil.exe, 00000004.00000002.575677767.00000006EC5000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000004.00000002.575530952.0000000006E7C000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708244
Start date and time:	2022-09-23 07:59:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	321 Amita Technical 16.09.2022.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/3@3/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target 321 Amita Technical 16.09.2022.exe, PID 5436 because it is empty
- Execution Graph export aborted for target phine.exe, PID 5604 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: 321 Amita Technical 16.09.2022.exe

Simulations

Behavior and APIs

Time	Type	Description
08:00:19	API Interceptor	1x Sleep call for process: 321 Amita Technical 16.09.2022.exe modified
08:00:34	API Interceptor	203x Sleep call for process: phine.exe modified
08:01:49	API Interceptor	81x Sleep call for process: InstallUtil.exe modified
08:01:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Word C:\Users\user\AppData\Roaming\Word\Word.exe
08:02:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Word C:\Users\user\AppData\Roaming\Word\Word.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\321 Amita Technical 16.09.2022.exe.log

Process:	C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7GE4Kx1qE4KE4VE4j:Mgv2HKXwYHKhQnoPtHoxHhAHKzvGHKx3
MD5:	E0F1B7E3E2980062667DDAD219EBE1DE
SHA1:	3FF322345F415F0065DD1C762FDB04DC45F5C235
SHA-256:	DF9914B0AD05A6D8A5C1C7D6365867B579FFB6C1B40F8C0B087822AF458BBC5A
SHA-512:	4C1589C64F4D487100D9F7B2F357BE0891B3E103D15A32A87098036FA993659DFADB2FF6A153B48CAEB0B6112FD5145558F71FCD1FE066BCF780A6D69C3F865
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\phine.exe.log

Process:	C:\Users\user\AppData\Local\Temp\phine.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7GE4Kx1qE4KE4VE4j:Mgv2HKXwYHKhQnoPtHoxHhAHKzvGHKx3
MD5:	E0F1B7E3E2980062667DDAD219EBE1DE
SHA1:	3FF322345F415F0065DD1C762FDB04DC45F5C235
SHA-256:	DF9914B0AD05A6D8A5C1C7D6365867B579FFB6C1B40F8C0B087822AF458BBC5A
SHA-512:	4C1589C64F4D487100D9F7B2F357BE0891B3E103D15A32A87098036FA993659DFADB2FF6A153B48CAEB0B6112FD5145558F71FCD1FE066BCF780A6D69C3F865
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Roaming\Word\Word.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFA
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.reloc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(-...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.858986203279892
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	321 Amita Technical 16.09.2022.exe
File size:	636416
MD5:	a2a924c124bbc597a76495b4fb08f906
SHA1:	7ce1c45be6abf27c1b6f6c33ad16a27c4925e51b
SHA256:	9d45370a27c72436041f3ffb82b0c245eea5191c788b574e9656a23054340a61
SHA512:	4d2dfb53de6c5070f52facb1f0285d24aabca79385fdcc818cd383d86abcedabbc36d4824cd0c5ef7aab4d62ac5d2be192e06efb5e59c82a856cb72b838a24f6
SSDEEP:	12288:zie1sOdae4gm/EYA71l1W6cY7l9v4QjFMsZNSs86xNY:RskbTmMc1W6cl7JjFMsZN26E
TLSH:	55D48CE917D4FD11C63E723134A47930D2F6C0C9EAD14B9B999CA0D63F923E639E20A5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z.|F.....P..... .....@.. .....`

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49bc2e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x467CAA5A [Sat Jun 23 05:06:34 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9bbe0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x125b	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x99c34	0x99e00	False	0.6715481569861901	data	6.864655751113723	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x125b	0x1400	False	0.367578125	data	4.9068544050106	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

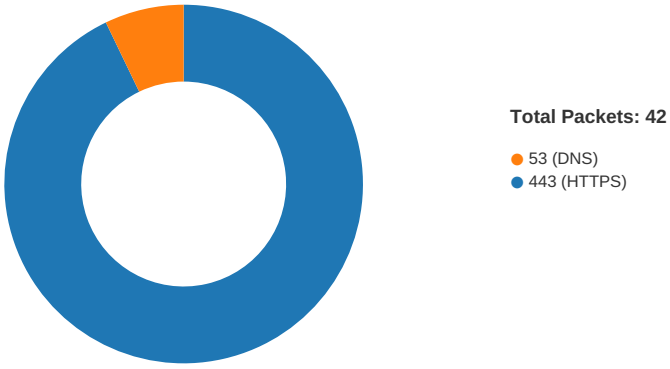
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9c0a0	0x3d8	data		
RT_MANIFEST	0x9c478	0xde3	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:00:00.779475927 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:00.779526949 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:00.779675007 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:00.845621109 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:00.845668077 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:00.907469988 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:00.907659054 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:00.917588949 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:00.917609930 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:00.917903900 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:00.986915112 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.269850016 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.311383009 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336564064 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336637974 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336693048 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336705923 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.336724997 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336765051 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336770058 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.336781025 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.336831093 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.338606119 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.338829041 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.338874102 CEST	443	49684	142.250.185.164	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:00:01.338887930 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.338907957 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.338948011 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.340102911 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.342545033 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.342607021 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.342643023 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.342662096 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.342734098 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.353533983 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.353959084 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.354005098 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.354041100 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.354063988 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.354104042 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.355290890 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.356671095 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.356724024 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.356731892 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.356753111 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.356795073 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.357906103 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.359222889 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.359276056 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.359282970 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.359302998 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.359339952 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.360532999 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.361828089 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.361891985 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.361927986 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.361951113 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.362005949 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.363126993 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.364238024 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.364300013 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.364310980 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.364329100 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.364373922 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.365379095 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.366497040 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.366553068 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.366559982 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.367693901 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.367754936 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.367763042 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.367952108 CEST	443	49684	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:01.368041039 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:01.371216059 CEST	49684	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.092722893 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.092808962 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.092900991 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.115080118 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.115142107 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.166870117 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.167102098 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.174918890 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.174958944 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.175548077 CEST	443	49687	142.250.185.164	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:00:22.254374981 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.591911077 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.635516882 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.662750959 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.662864923 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.662952900 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.662972927 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.663013935 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.663089991 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.663109064 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.663623095 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.663708925 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.663769007 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.663789988 CEST	443	49687	142.250.185.164	192.168.2.5
Sep 23, 2022 08:00:22.663849115 CEST	49687	443	192.168.2.5	142.250.185.164
Sep 23, 2022 08:00:22.664552927 CEST	443	49687	142.250.185.164	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:00:00.727139950 CEST	54882	53	192.168.2.5	8.8.8.8
Sep 23, 2022 08:00:00.755059958 CEST	53	54882	8.8.8.8	192.168.2.5
Sep 23, 2022 08:00:22.045969963 CEST	60136	53	192.168.2.5	8.8.8.8
Sep 23, 2022 08:00:22.065529108 CEST	53	60136	8.8.8.8	192.168.2.5
Sep 23, 2022 08:02:02.328102112 CEST	54949	53	192.168.2.5	8.8.8.8
Sep 23, 2022 08:02:02.509649992 CEST	53	54949	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 23, 2022 08:00:00.727139950 CEST	192.168.2.5	8.8.8.8	0x89a6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:00:22.045969963 CEST	192.168.2.5	8.8.8.8	0xa73	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:02:02.328102112 CEST	192.168.2.5	8.8.8.8	0x1e01	Standard query (0)	multimetals.cfd	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 08:00:00.755059958 CEST	8.8.8.8	192.168.2.5	0x89a6	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:00:22.065529108 CEST	8.8.8.8	192.168.2.5	0xa73	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:02:02.509649992 CEST	8.8.8.8	192.168.2.5	0x1e01	No error (0)	multimetals.cfd		192.185.37.183	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49684	142.250.185.164	443	C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-09-23 06:00:01 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:00:01 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: AEC=AakniGNElqM1uQ_3R3wAi5RyA-AySJikAjH_K2pPYn9JU2tJU-0eszbTcxY; expires=Wed, 22-Mar-2023 06:00:01 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=7.SE=VycMiaPM3l4ivFudIaOFYpzEmsVq3lwMeeVEI9hTo8lANSpJIn6E0q8v5lzVgBFqkG8l8o49yMRFLGzz1ptf2EmvLiPMIjwc1R0w8SCO20ND02iGStCG1TGOG8E3SUT-PzEtKqLEChvkeBvtb8MQxxsvr1FimKSaK0kUh0fppPQ; expires=Mon, 23-Oct-2023 22:18:19 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+458; expires=Sun, 22-Sep-2024 06:00:01 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-09-23 06:00:01 UTC	1	IN	Data Raw: 35 36 61 37 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 Data Ascii: 56a7<!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 con
2022-09-23 06:00:01 UTC	1	IN	Data Raw: 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 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 36 56 31 50 4a 6b 71 70 4d 75 68 6d 39 41 71 69 54 56 50 75 75 67 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 3d 7b 6b 45 49 3a 27 59 55 73 74 59 5f 65 47 45 66 71 4b 39 75 38 50 5f 39 32 72 2d 41 49 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 36 30 35 39 2c 32 30 36 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 36 2c 35 2c 35 Data Ascii: tent="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="6V1PJkqpMuhm9AqiTVPuug">(function(){window.google={kEI:'YUstY_eGEfqK9u8P_92r-AI',kEXPI:'0,1302536,56873,6059,206,4804,2316,383,246,5,5
2022-09-23 06:00:01 UTC	2	IN	Data Raw: 2c 31 39 36 34 2c 31 30 30 37 2c 32 30 38 37 2c 32 33 32 31 2c 31 31 32 35 37 2c 33 34 30 36 2c 35 35 34 33 2c 35 37 34 32 2c 31 34 35 34 35 37 32 27 2c 6b 42 4c 3a 27 78 39 56 45 27 7d 3b 67 6f 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 65 6e 2d 47 42 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 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 Data Ascii: ,1964,1007,2087,2321,11257,3406,5543,5742,1454572',kBL:'x9VE'};google.sn='webhp';google.kHL='en-GB';})();(function(){var f=this||self;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||h}function
2022-09-23 06:00:01 UTC	3	IN	Data Raw: 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 5b 61 5d 2c 62 2c 63 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 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 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 Data Ascii: {google.lq.push([[a],b,c])};google.loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.lx=function(){};}).call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttri
2022-09-23 06:00:01 UTC	5	IN	Data Raw: 65 66 74 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 33 30 70 78 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 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 Data Ascii: eft:0;position:absolute;top:30px;width:100%}.gbtcb{position:absolute;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;to
2022-09-23 06:00:01 UTC	6	IN	Data Raw: 63 63 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 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 Data Ascii: cc{display:block;list-style:none;margin:0;padding:0}.gbmc{background:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inl

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	7	IN	Data Raw: 68 76 72 2c 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 23 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 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 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 Data Ascii: hvr,.gbgt:focus{background-color:#4c4c4c;background-image:none;_background-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4
2022-09-23 06:00:01 UTC	8	IN	Data Raw: 78 7d 2e 67 62 6e 20 2e 67 62 6d 74 2c 2e 67 62 6e 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 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 Data Ascii: x}.gbn .gbmt,.gbn .gbmt:visited,.gbnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !import
2022-09-23 06:00:01 UTC	10	IN	Data Raw: 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 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 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 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 Data Ascii: px rgba(0,0,0,.12);box-shadow:0 2px 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{
2022-09-23 06:00:01 UTC	11	IN	Data Raw: 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 32 30 70 78 20 30 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 62 6d 70 61 6c 61 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 7d 23 67 62 6d 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 Data Ascii: eight:27px;padding:10px 20px 0;white-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{d
2022-09-23 06:00:01 UTC	12	IN	Data Raw: 66 66 66 2c 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 2d 6e 6f 2d 66 6f 63 75 73 3a 66 6f 63 75 73 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 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 Data Ascii: fff,0 1px 1px rgba(0,0,0,.1)}.gbqfb-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1
2022-09-23 06:00:01 UTC	14	IN	Data Raw: 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 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 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 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 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 2d 6f 2d 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 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 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a Data Ascii: op,#4d90fe,#357ae8);background-image:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:
2022-09-23 06:00:01 UTC	15	IN	Data Raw: 6e 74 28 74 6f 70 2c 23 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 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 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 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 Data Ascii: nt(top,#f8f8f8,#f1f1f1);background-image:linear-gradient(top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,
2022-09-23 06:00:01 UTC	16	IN	Data Raw: 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 3b 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 2c 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 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 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 Data Ascii: z-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	17	IN	Data Raw: 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 33 29 3b 74 6f 70 3a 30 7d 2e 67 62 73 62 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 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 2e 35 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 38 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 Data Ascii: color:rgba(0,0,0,.3);top:0}.gbsb .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from
2022-09-23 06:00:01 UTC	19	IN	Data Raw: 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 7d 2e 66 6c 20 61 7b 63 6f 6c 6f 72 3a 23 31 35 35 38 64 36 7d 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 34 62 31 31 61 38 7d 2e 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 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 Data Ascii: decoration:underline}.fl a{color:#1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.l
2022-09-23 06:00:01 UTC	20	IN	Data Raw: 3d 22 26 73 63 72 69 70 74 3d 22 2b 62 28 67 29 2c 66 26 26 67 3d 3d 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 26 26 28 66 3d 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 6f 75 74 65 72 48 54 4d 4c 2e 73 70 6c 69 74 28 22 5c 6e 22 29 5b 66 5d 2c 63 2b 3d 22 26 63 61 64 3d 22 2b 62 28 66 3f 66 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 33 30 30 29 3a 22 4e 6f 20 73 63 72 69 70 74 20 66 6f 75 6e 64 2e 22 29 29 29 3b 63 2b 3d 22 26 6a 73 65 6c 3d 22 2b 65 3b 66 6f 72 28 76 61 72 20 75 20 69 6e 20 64 29 63 2b 3d 22 26 22 2c 63 2b 3d 62 28 75 29 2c 63 2b 3d 22 3d 22 2c 63 2b 3d 62 28 64 5b 75 5d 29 3b 63 3d 63 2b 22 26 65 6d 73 67 3d 22 2b 62 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b Data Ascii: ="&script="+b(g),f&&g===window.location.href&&(f=document.documentElement.outerHTML.split("\n")[f],c+="&cad="+b(f?f.substring(0,300):"No script found.")));c+="&jsel="+e;for(var u in d)c+="&",c+=b(u),c+="=",c+=b(d[u]);c=c+"&emsg="+b(a.name+": "+a.message);
2022-09-23 06:00:01 UTC	21	IN	Data Raw: 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 6c 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 6c 3a 76 6f 69 64 20 30 3d 3d 6c 3f 6b 3a 6c 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 Data Ascii: nt)a.attachEvent(d,c);else{var f=a[d];a[d]=function(){var k=f.apply(this,arguments),l=c.apply(this,arguments);return void 0==k?l:void 0==l?k:l&&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.
2022-09-23 06:00:01 UTC	22	IN	Data Raw: 66 30 0d 0a 72 61 28 32 2c 61 29 2c 62 5b 31 5d 2e 75 72 6c 26 26 71 61 28 62 5b 31 5d 2e 75 72 6c 2c 61 29 2c 62 5b 31 5d 2e 6c 69 62 73 26 26 44 26 26 44 28 62 5b 31 5d 2e 6c 69 62 73 29 29 7d 2c 74 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 22 67 63 22 2c 61 29 7d 2c 75 61 3d 6e 75 6c 6c 2c 76 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 75 61 3d 61 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 75 61 29 7b 61 3d 7b 74 3a 61 2c 62 3a 62 7d 3b 69 66 28 63 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 63 29 61 5b 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 77 29 3b 70 28 22 6d 64 69 22 2c 6b 61 29 3b 70 28 22 62 6e 63 22 2c 78 0d 0a Data Ascii: f0ra(2,a),b[1].url&&qa(b[1].url,a),b[1].libs&&D&&D(b[1].libs))},ta=function(a){B("gc",a)},ua=null,va=function(a){ua=a},ra=function(a,b,c){if(ua){a={t:a,b:b};if(c)for(var d in c)a[d]=c[d];try{ua(a)}catch(f){}}};p("mdc",w);p("mdi",ka);p("bnc",x
2022-09-23 06:00:01 UTC	23	IN	Data Raw: 36 35 65 38 0d 0a 29 3b 70 28 22 71 47 43 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 43 29 3b 70 28 22 71 64 22 2c 41 29 3b 70 28 22 6c 62 22 2c 73 61 29 3b 70 28 22 6d 63 66 22 2c 6f 61 29 3b 70 28 22 62 63 66 22 2c 6e 61 29 3b 70 28 22 61 71 22 2c 42 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 70 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 72 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 49 4b 35 4f 6d 55 55 52 64 32 45 2e 4f 2f 64 3d 31 2f 72 73 3d 41 48 70 4f 6f 39 33 32 4a 69 6e 6b 53 4a 48 4b 39 32 57 67 56 6a 49 56 2d 4a 77 77 79 75 33 52 77 2f 6d 3d 5f 5f 66 65 61 74 75 72 65 73 5f 5f 22 29 29 Data Ascii: 65e8);p("qGC",ta);p("qm",C);p("qd",A);p("lb",sa);p("mcf",oa);p("bcf",na);p("aq",B);p("mdd","");p("has",pa);p("trh",va);p("tev",ra);if(h.a("m;/_/scs/abc-static/_/js/k=gapi.gapi.en.IK5OmUURd2E.O/d=1/rs=AHpOoo932JinkSJHK92WgVjIV-Jwwyu3Rw/m=__features__"))
2022-09-23 06:00:01 UTC	24	IN	Data Raw: 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 59 55 73 74 59 38 71 51 45 76 6d 52 39 75 38 50 30 38 69 76 38 41 55 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 34 37 33 36 33 35 31 38 32 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 32 30 38 30 31 2e 30 5f 70 30 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 65 6e 22 Data Ascii: (),"&jexpid=",d("28834"),"&srcpg=",d("prop=1"),"&jsr=",Math.round(1/Fa),"&ogev=",d("YUstY8qQEvmR9u8P08iv8AU"),"&ogf=",g.bv.f,"&ogrp=",d(""),"&ogv=",d("473635182.0"),"&oggv="+d("es_plusone_gc_20220801.0_p0"),"&ogd=",d("com"),"&ogc=",d("GBR"),"&ogl=",d("en"
2022-09-23 06:00:01 UTC	25	IN	Data Raw: 79 54 6d 71 49 75 77 51 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 67 33 65 72 6a 35 31 55 38 45 59 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 71 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 49 29 3b 70 28 22 63 72 22 2c 4a 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 49 3b 68 2e 6c 3d 4a 3b 68 2e 6d 3d 48 3b 68 2e 6e 3d 4d 61 3b 68 2e 70 3d 4f 61 3b 68 2e 71 3d 4e 61 3b 76 61 72 20 50 61 3d 5b 22 67 62 5f 37 31 22 2c 22 67 62 5f 31 35 35 22 5d 2c 51 61 3b 66 75 6e 63 74 69 6f 6e 20 52 61 28 61 29 7b 51 61 3d 61 7d 66 75 6e 63 74 69 6f 6e 20 53 61 28 61 29 7b 76 61 72 20 62 3d 51 61 26 26 21 61 2e 68 72 65 66 2e 6d 61 74 63 Data Ascii: yTmqIuwQ"];Ka&&a.push("?host=www.gstatic.com&bust=og.og2.en_US.g3erj51U8EY.DU");a=a.join("");qa(a);p("ca",I);p("cr",J);p("cc",H);h.k=I;h.l=J;h.m=H;h.n=Ma;h.p=Oa;h.q=Na;var Pa=["gb_71","gb_155"],Qa;function Ra(a){Qa=a}function Sa(a){var b=Qa&&!a.href.matc

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	26	IN	Data Raw: 29 3b 6d 26 26 6d 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 4a 28 6d 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 22 67 62 74 6f 22 29 7d 7d 7d 24 61 28 66 29 26 26 61 62 28 66 29 3b 4e 3d 64 3b 49 28 6b 2c 22 67 62 74 6f 22 29 7d 7d 7d 7d 43 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 62 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 64 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 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 65 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 72 64 64 28 61 29 7d 29 7d 2c 5a 61 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 Data Ascii:);m&&m.parentNode&&J(m.parentNode,"gbto")}}}$a(f)&&ab(f);N=d;I(k,"gbto")}}}}C(function(){g.tg(a,b,!0)});bb(a)}catch(q){r(q,"sb","tg")}},db=function(a){C(function(){g.close(a)})},eb=function(a){C(function(){g.rdd(a)})},Za=function(a){var b,c=document.defau
2022-09-23 06:00:01 UTC	28	IN	Data Raw: 68 28 42 62 29 7b 72 28 42 62 2c 22 73 62 22 2c 22 61 6c 22 29 7d 7d 2c 66 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 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 62 28 61 2c 22 67 62 65 22 2c 62 29 7d 2c 6a 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 43 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 6b 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 43 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 Data Ascii: h(Bb){r(Bb,"sb","al")}},fb=function(a,b){for(var c=b.length,d=0;d<c;d++)if(H(a,b[d]))return!0;return!1},hb=function(a,b,c){gb(a,b,c)},ib=function(a,b){gb(a,"gbe",b)},jb=function(){C(function(){g.pcm&&g.pcm()})},kb=function(){C(function(){g.pca&&g.pca()})
2022-09-23 06:00:01 UTC	29	IN	Data Raw: 29 72 65 74 75 72 6e 20 62 7d 2c 4f 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 71 62 26 26 77 69 6e 64 6f 77 2e 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 71 62 29 7d 2c 75 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 76 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 31 7d 2c 77 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 21 Data Ascii:)return b},O=function(){qb&&window.clearTimeout(qb)},ub=function(a){var b="inner"+a;a="offset"+a;return window[b]?window[b]:document.documentElement&&document.documentElement[a]?document.documentElement[a]:0},vb=function(){return!1},wb=function(){return!!
2022-09-23 06:00:01 UTC	30	IN	Data Raw: 22 22 3b 76 61 72 20 45 62 3d 5b 31 2c 32 2c 33 2c 34 2c 35 2c 36 2c 39 2c 31 30 2c 31 31 2c 31 33 2c 31 34 2c 32 38 2c 32 39 2c 33 30 2c 33 34 2c 33 35 2c 33 37 2c 33 38 2c 33 39 2c 34 30 2c 34 31 2c 34 32 2c 34 33 2c 34 38 2c 34 39 2c 35 30 30 5d 3b 76 61 72 20 46 62 3d 68 2e 62 28 22 30 2e 30 30 31 22 2c 31 45 2d 34 29 2c 47 62 3d 68 2e 62 28 22 31 22 2c 31 29 2c 48 62 3d 21 31 2c 49 62 3d 21 31 3b 69 66 28 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 4a 62 3d 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 3b 4a 62 3c 46 62 26 26 28 48 62 3d 21 30 29 3b 4a 62 3c 47 62 26 26 28 49 62 3d 21 30 29 7d 76 61 72 20 51 3d 6e 75 6c 6c 3b 0a 66 75 6e 63 74 69 6f 6e 20 4b 62 28 61 2c 62 29 7b 76 61 72 20 63 3d 46 62 2c 64 3d 48 62 3b 76 61 72 20 66 3d 61 3b 69 66 28 21 51 Data Ascii: "";var Eb=[1,2,3,4,5,6,9,10,11,13,14,28,29,30,34,35,37,38,39,40,41,42,43,48,49,500];var Fb=h.b("0.001",1E-4),Gb=h.b("1",1),Hb=!1,Ib=!1;if(h.a("1")){var Jb=Math.random();Jb<Fb&&(Hb=!0);Jb<Gb&&(Ib=!0)}var Q=null;function Kb(a,b){var c=Fb,d=Hb;var f=a;if(!Q
2022-09-23 06:00:01 UTC	31	IN	Data Raw: 63 74 69 6f 6e 28 29 7b 67 2e 70 72 6d 28 29 7d 29 7d 2c 50 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 6e 28 61 29 7d 29 7d 2c 51 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 73 28 61 29 7d 29 7d 2c 52 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 70 28 61 29 7d 29 7d 2c 53 62 3d 7b 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 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 Data Ascii: ction(){g.prm()})},Pb=function(a){C(function(){g.spn(a)})},Qb=function(a){C(function(){g.sps(a)})},Rb=function(a){C(function(){g.spp(a)})},Sb={"27":"https://lh3.googleusercontent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/ogw/defaul
2022-09-23 06:00:01 UTC	33	IN	Data Raw: 62 2c 63 29 7b 69 66 28 59 28 5b 31 5d 2c 22 61 6f 70 22 29 26 26 63 29 7b 69 66 28 57 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 57 29 57 5b 64 5d 3d 57 5b 64 5d 26 26 2d 31 21 3d 59 62 28 63 2c 64 29 3b 65 6c 73 65 20 66 6f 72 28 57 3d 7b 7d 2c 64 3d 30 3b 64 3c 63 2e 6c 65 6e 67 74 68 3b 64 2b 2b 29 57 5b 63 5b 64 5d 5d 3d 21 30 3b 67 2e 75 70 2e 73 70 6c 28 61 2c 62 2c 22 61 6f 70 22 2c 63 29 7d 7d 2c 63 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 69 66 28 58 3d 32 2c 21 58 62 29 7b 58 62 3d 21 30 3b 66 6f 72 28 76 61 72 20 61 20 69 6e 20 52 29 66 6f 72 28 76 61 72 20 62 3d 52 5b 61 5d 2c 63 3d 30 3b 63 3c 62 2e 6c 65 6e 67 74 68 3b 63 2b 2b 29 74 72 79 7b 62 5b 63 5d 28 5a 62 28 61 29 29 7d 63 61 74 63 68 28 64 29 7b 72 28 64 2c 22 75 70 22 2c Data Ascii: b,c){if(Y([1],"aop")&&c){if(W)for(var d in W)W[d]=W[d]&&-1!=Yb(c,d);else for(W={},d=0;d<c.length;d++)W[c[d]]=!0;g.up.spl(a,b,"aop",c)}},cc=function(){try{if(X=2,!Xb){Xb=!0;for(var a in R)for(var b=R[a],c=0;c<b.length;c++)try{b[c](Zb(a))}catch(d){r(d,"up",
2022-09-23 06:00:01 UTC	34	IN	Data Raw: 69 66 28 64 63 28 61 29 29 72 65 74 75 72 6e 2d 31 3b 76 61 72 20 63 3d 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 2f 4f 47 50 43 3d 28 5b 5e 3b 5d 2a 29 2f 29 3b 69 66 28 63 26 26 63 5b 31 5d 29 7b 76 61 72 20 64 3d 63 5b 31 5d 2e 6d 61 74 63 68 28 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 62 22 2b 0a 62 2b 22 2d 28 5b 30 2d 39 5d 2b 29 3a 22 29 29 3b 69 66 28 64 26 26 64 5b 31 5d 29 72 65 74 75 72 6e 20 70 61 72 73 65 49 6e 74 28 64 5b 31 5d 2c 31 30 29 7d 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 67 63 63 22 29 7d 72 65 74 75 72 6e 2d 31 7d 3b 70 28 22 75 70 22 2c 7b 72 3a 24 62 2c 6e 61 70 3a 61 63 2c 61 6f 70 Data Ascii: if(dc(a))return-1;var c=a.cookie.match(/OGPC=([^;]*)/);if(c&&c[1]){var d=c[1].match(new RegExp("\\b"+b+"-([0-9]+):"));if(d&&d[1])return parseInt(d[1],10)}}catch(f){f.code!=DOMException.QUOTA_EXCEEDED_ERR&&r(f,"up","gcc")}return-1};p("up",{r:$b,nap:ac,aop
2022-09-23 06:00:01 UTC	35	IN	Data Raw: 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 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 70 6d 22 2c 7b 70 3a 22 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 Data Ascii: }})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var a=window.gbar;a.mcf("pm",{p:""});}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	37	IN	Data Raw: 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 61 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 62 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 76 61 72 20 63 3d 62 2e 69 3b 76 61 72 20 64 3d 63 2e 61 2c 65 3d 63 2e 63 2c 66 3d 7b 63 74 79 3a 22 47 42 52 22 2c 63 76 3a 22 34 37 33 36 33 35 31 38 32 22 2c 64 62 67 3a 64 28 22 22 29 2c 65 63 76 3a 22 30 22 2c 65 69 3a 65 28 22 59 55 73 74 59 38 71 51 45 76 6d 52 39 75 38 50 30 38 69 76 38 41 55 22 29 2c 65 6c 65 3a 64 28 22 31 22 29 2c 65 73 72 3a 65 Data Ascii: (function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var a=this||self;var b=window.gbar;var c=b.i;var d=c.a,e=c.c,f={cty:"GBR",cv:"473635182",dbg:d(""),ecv:"0",ei:e("YUstY8qQEvmR9u8P08iv8AU"),ele:d("1"),esr:e
2022-09-23 06:00:01 UTC	38	IN	Data Raw: 65 3d 27 36 56 31 50 4a 6b 71 70 4d 75 68 6d 39 41 71 69 54 56 50 75 75 67 27 3e 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 65 6c 69 26 26 67 62 61 72 2e 65 6c 69 28 29 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 69 64 3d 67 62 77 3e 3c 64 69 76 20 69 64 3d 67 62 7a 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 69 64 3d 67 62 7a 63 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 63 6c 61 73 73 3d 22 67 62 7a 74 20 67 62 7a 30 6c 20 67 62 70 31 22 20 69 64 3d 67 62 5f 31 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 77 65 62 68 70 3f 74 61 62 3d 77 77 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f Data Ascii: e='6V1PJkqpMuhm9AqiTVPuug'>window.gbar&&gbar.eli&&gbar.eli()</script> <ol id=gbzc class=gbtc><li class=gbt></
2022-09-23 06:00:01 UTC	39	IN	Data Raw: 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 67 74 20 69 64 3d 67 62 7a 74 6d 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 20 61 72 69 61 2d 68 61 73 70 6f 70 75 70 3d 74 72 75 65 20 61 72 69 61 2d 6f 77 6e 73 3d 67 62 64 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 20 69 64 3d 67 62 7a 74 6d 73 20 63 6c 61 73 73 3d 22 67 62 74 73 20 67 62 74 73 61 3e 3c 73 70 61 6e 20 69 64 3d 67 62 7a 74 6d 73 31 3e 4d 6f 72 65 3c 2f 73 70 61 6e 3e 3c 73 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 Data Ascii: li><li class=gbt>More
2022-09-23 06:00:01 UTC	40	IN	Data Raw: 72 65 66 3d 22 68 74 74 70 3a 2f 2f 76 69 64 65 6f 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 76 22 3e 56 69 64 65 6f 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 32 35 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 64 6f 63 75 6d 65 6e 74 2f 3f 75 73 70 3d 64 6f 63 73 5f 61 6c 63 22 3e 44 6f 63 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 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 Data Ascii: ref="http://video.google.co.uk/?hl=en&tab=wv">Videos <li class=gbmtc>Docs <li class=gbmtc> <li class=gbmtc><a href="https://www.
2022-09-23 06:00:01 UTC	42	IN	Data Raw: 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 35 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 67 35 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 63 3e 3c 6f 6c 20 69 64 3d 67 62 6f 6d 20 63 6c 61 73 73 3d 67 62 6d 63 63 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 63 20 67 62 6d 74 63 22 3e 3c 61 20 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 2f 70 72 65 66 65 72 65 6e 63 65 73 3f 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 Data Ascii: EventListener('click', function clickHandler() { gbar.tg(event,this); });</script> <ol id=gbom class=gbmcc><li class="gbkc gbmtc">Search settings <li cl
2022-09-23 06:00:01 UTC	43	IN	Data Raw: 3d 22 6f 66 66 22 20 76 61 6c 75 65 3d 22 22 20 74 69 74 6c 65 3d 22 47 6f 6f 67 6c 65 20 53 65 61 72 63 68 22 20 6d 61 78 6c 65 6e 67 74 68 3d 22 32 30 34 38 22 20 6e 61 6d 65 3d 22 71 22 20 73 69 7a 65 3d 22 35 37 22 3e 3c 2f 64 69 76 3e 3c 62 72 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 22 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 76 61 6c 75 65 3d 22 47 6f 6f 67 6c 65 20 53 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 62 74 6e 47 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 2f 73 70 61 6e 3e 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 Data Ascii: ="off" value="" title="Google Search" maxlength="2048" name="q" size="57"> <br style="line-height:0"><input class="lsb" value="Google Search" name="btnG" type="submit"><span class="ls
2022-09-23 06:00:01 UTC	44	IN	Data Raw: 6f 6f 67 6c 65 2e 67 62 76 75 2c 67 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 76 22 29 3b 67 26 26 28 67 2e 76 61 6c 75 65 3d 61 29 3b 66 26 26 77 69 6e 64 6f 77 2e 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 66 7d 2c 30 29 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 66 6f 72 6d 3e 3c 64 69 76 20 69 64 3d 22 67 61 63 5f 73 63 6f 6e 74 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 33 25 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 2e 35 65 6d 22 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 64 69 76 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 Data Ascii: oogle.gbvu,g=document.getElementById("gbv");g&&(g.value=a);f&&window.setTimeout(function(){location.href=f},0)};}).call(this);</script></form> <div style="fon
2022-09-23 06:00:01 UTC	46	IN	Data Raw: 6c 76 56 77 2e 4c 2e 58 2e 4f 27 2c 63 73 3a 27 41 43 54 39 30 6f 46 62 53 6e 69 32 64 69 79 71 57 48 6b 5a 45 30 4e 42 50 77 76 77 4d 39 43 55 56 77 27 2c 65 78 63 6d 3a 5b 5d 7d 3b 7d 29 28 29 3b 3c 2f 73 63 72 69 70 74 3e 20 20 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 36 56 31 50 4a 6b 71 70 4d 75 68 6d 39 41 71 69 54 56 50 75 75 67 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 75 3d 27 2f 78 6a 73 2f 5f 2f 6a 73 2f 6b 5c 78 33 64 78 6a 73 2e 68 70 2e 65 6e 2e 50 61 32 46 7a 52 51 66 79 57 55 2e 4f 2f 61 6d 5c 78 33 64 41 41 43 65 41 41 41 6b 41 45 41 42 2f 64 5c 78 33 64 31 2f 65 64 5c 78 33 64 31 2f 72 73 5c 78 33 64 41 43 54 39 30 6f 47 47 4f 48 41 47 39 39 71 72 61 41 39 68 59 4d 73 78 64 79 71 33 54 58 33 62 76 51 2f 6d 5c 78 33 64 73 Data Ascii: lvVw.L.X.O',cs:'ACT90oFbSni2diyqWHkZE0NBPwvwM9CUVw',excm:[]};})();</script> <script nonce="6V1PJkqpMuhm9AqiTVPuug">(function(){var u='/xjs/_/js/k\x3dxjs.hp.en.Pa2FzRQfyWU.O/am\x3dAACeAAAkAEAB/d\x3d1/ed\x3d1/rs\x3dACT90oGGOHAG99qraA9hYMsxdyq3TX3bvQ/m\x3ds

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:01 UTC	47	IN	Data Raw: 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 28 29 7d 2c 30 29 3b 7d 29 28 29 3b 66 75 6e 63 74 69 6f 6e 20 5f 44 75 6d 70 45 78 63 65 70 74 69 6f 6e 28 65 29 7b 74 68 72 6f 77 20 65 3b 7d 0a 66 75 6e 63 74 69 6f 6e 20 5f 46 5f 69 6e 73 74 61 6c 6c 43 73 73 28 63 29 7b 7d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 6f 6f 67 6c 65 2e 6a 6c 3d 7b 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 64 77 75 3a 74 72 75 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 69 6e 6a 73 3a 27 6e 6f 6e 65 27 2c 69 6e 6a 74 3a 30 2c 69 6e 6a 74 68 3a 30 2c 69 6e 6a 76 32 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 6e 65 74 3a 74 72 75 65 2c 73 74 Data Ascii: imeout(function(){n()},0);})();function _DumpException(e){throw e;}function _F_installCss(c){}(function(){google.jl={blt:'none',chnk:0,dw:false,dwu:true,emtn:0,end:0,ine:false,injs:'none',injt:0,injth:0,injv2:false,lls:'default',pdt:0,rep:0,snet:true,st
2022-09-23 06:00:01 UTC	48	IN	Data Raw: 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: </body></html>
2022-09-23 06:00:01 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	192.168.2.5	49687	142.250.185.164	443	C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	48	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-09-23 06:00:22 UTC	48	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:00:22 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: AEC=AakniGNjgQDiCVqaXVqYIPfbiDl8iqHqgJUInEQXTntObFrzG2OB8cHvAPI; expires=Wed, 22-Mar-2023 06:00:22 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=7.SE=JzA7-vvtRDA50DmxjRDVf8WDHSaC143fZFcJIFcTYaJb2ZAaAd92c-05_3s xTe7C6ET4puuaR4cEmF4IXtbeZKB5b6OdVtEMVrfssaDPvW81I4qWgRLYeiUF1ozFHwUjIMydoa1sjhpS_bB6g7gsA GYNuR6PglxXmw4ES805qQE; expires=Mon, 23-Oct-2023 22:18:40 GMT; path=/; domain=.google.com; Secure; H ttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+103; expires=Sun, 22-Sep-2024 06:00:22 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-09-23 06:00:22 UTC	49	IN	Data Raw: 35 36 63 38 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 Data Ascii: 56c8<!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 con
2022-09-23 06:00:22 UTC	49	IN	Data Raw: 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 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 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 61 38 50 37 4a 46 2d 4a 41 77 68 5f 4b 50 74 69 37 36 38 43 79 41 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 3d 7b 6b 45 49 3a 27 64 6b 73 74 59 5f 66 71 4a 50 43 43 39 75 38 50 75 4e 57 32 6f 41 51 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 36 30 35 38 2c 32 30 37 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 36 2c 35 2c 35 Data Ascii: tent="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google </title><script nonce="a8P7JF-JAwh_KPti768CyA">(function(){window.google={kEI:'dkstY_fqJPCC9u8PuNW2o AQ',kEXPI:'0,1302536,56873,6058,207,4804,2316,383,246,5,5
2022-09-23 06:00:22 UTC	51	IN	Data Raw: 2c 31 33 35 37 39 2c 33 34 30 35 2c 35 35 34 33 2c 31 34 36 30 33 31 34 27 2c 6b 42 4c 3a 27 78 39 56 45 27 7d 3b 67 6f 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 65 6e 2d 47 42 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 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 Data Ascii: ,13579,3405,5543,1460314',kBL:'x9VE'};google.sn='webhp';google.kHL='en-GB';})();(function(){var f=this||self ;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||h}function m(a){for(var b=null;a&&(

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	52	IN	Data Raw: 29 7d 3b 67 6f 6f 67 6c 65 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 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 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 Data Ascii:)};google.loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.lx=function(){};}).call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfalse");
2022-09-23 06:00:22 UTC	53	IN	Data Raw: 6f 70 3a 33 30 70 78 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 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 Data Ascii: op:30px;width:100%}.gbtcb{position:absolute;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility:hidde
2022-09-23 06:00:22 UTC	54	IN	Data Raw: 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 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 Data Ascii: le:none;margin:0;padding:0}.gbmc{background:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shadow:0 2p
2022-09-23 06:00:22 UTC	56	IN	Data Raw: 64 2d 63 6f 6c 6f 72 3a 23 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 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 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 Data Ascii: d-color:#4c4c4c;background-image:none;_background-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4s,#gbi
2022-09-23 06:00:22 UTC	57	IN	Data Raw: 69 73 69 74 65 64 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 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 Data Ascii: isited,.gbnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{d
2022-09-23 06:00:22 UTC	58	IN	Data Raw: 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 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 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 Data Ascii: adow:0 2px 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmp
2022-09-23 06:00:22 UTC	60	IN	Data Raw: 30 70 78 20 30 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 62 6d 70 61 6c 61 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 7d 23 67 62 6d 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 Data Ascii: 0px 0;white-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;paddi
2022-09-23 06:00:22 UTC	61	IN	Data Raw: 2e 31 29 7d 2e 67 62 71 66 62 2d 6e 6f 2d 66 6f 63 75 73 3a 66 6f 63 75 73 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 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 Data Ascii: .1)}.gbqfb-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-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 rg

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	62	IN	Data Raw: 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 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 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 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 2d 6f 2d 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 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 Data Ascii: round-image:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:active{background-color:i
2022-09-23 06:00:22 UTC	63	IN	Data Raw: 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 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 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 Data Ascii: ackground-image:linear-gradient(top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#fff),to
2022-09-23 06:00:22 UTC	65	IN	Data Raw: 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 3b 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 61 3a 61 63 74 69 76 65 2c 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 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 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 Data Ascii: ba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(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-he
2022-09-23 06:00:22 UTC	66	IN	Data Raw: 30 7d 2e 67 62 73 62 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 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 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 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 Data Ascii: 0}.gbsb .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(
2022-09-23 06:00:22 UTC	67	IN	Data Raw: 61 7b 63 6f 6c 6f 72 3a 23 31 35 35 38 64 36 7d 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 34 62 31 31 61 38 7d 2e 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 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 Data Ascii: a{color:#1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block}#WqQANb
2022-09-23 06:00:22 UTC	69	IN	Data Raw: 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 26 26 28 66 3d 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 6f 75 74 65 72 48 54 4d 4c 2e 73 70 6c 69 74 28 22 5c 6e 22 29 5b 66 5d 2c 63 2b 3d 22 26 63 61 64 3d 22 2b 62 28 66 3f 66 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 33 30 30 29 3a 22 4e 6f 20 73 63 72 69 70 74 20 66 6f 75 6e 64 2e 22 29 29 3b 63 2b 3d 22 26 6a 73 65 6c 3d 22 2b 65 3b 66 6f 72 28 76 61 72 20 75 20 69 6e 20 64 29 63 2b 3d 22 26 22 2c 63 2b 3d 62 28 75 29 2c 63 2b 3d 22 3d 22 2c 63 2b 3d 62 28 64 5b 75 5d 29 3b 63 3d 63 2b 22 26 65 6d 73 67 3d 22 2b 62 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b 63 3d 63 2b 22 26 6a 73 73 74 3d 22 2b 62 28 61 2e 73 74 61 63 6b 7c 7c 22 Data Ascii: indow.location.href&&(f=document.documentElement.outerHTML.split("\n")[f],c+="&cad="+b(f?f.substring(0,300):"No script found.")));c+="&jsel="+e;for(var u in d)c+="&",c+=b(u),c+="=",c+=b(d[u]);c=c+"&emsg="+b(a.name+": "+a.message);c=c+"&jsst="+b(a.stack||
2022-09-23 06:00:22 UTC	70	IN	Data Raw: 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 6c 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 6c 3a 76 6f 69 64 20 30 3d 3d 6c 3f 6b 3a 6c 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 Data Ascii: e{var f=a[d];a[d]=function(){var k=f.apply(this,arguments),l=c.apply(this,arguments);return void 0==k?l:void 0==l?k:l&&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;va
2022-09-23 06:00:22 UTC	71	IN	Data Raw: 65 61 0d 0a 29 29 7d 2c 74 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 22 67 63 22 2c 61 29 7d 2c 75 61 3d 6e 75 6c 6c 2c 76 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 61 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 75 61 29 7b 61 3d 7b 74 3a 61 2c 62 3a 62 7d 3b 69 66 28 63 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 63 29 61 5b 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 3b 70 28 22 6d 64 69 22 2c 77 29 3b 70 28 22 6d 64 69 22 2c 6b 61 29 3b 70 28 22 62 6e 63 22 2c 78 29 3b 70 28 22 71 47 43 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 43 29 3b 70 28 22 71 64 22 2c 41 29 3b 70 28 22 6c 62 22 2c 73 61 29 3b 70 28 22 6d 63 66 22 0d 0a Data Ascii: ea))},ta=function(a){B("gc",a)},ua=null,va=function(a){ua=a},ra=function(a,b,c){if(ua){a={t:a,b:b};if(c)for(var d in c)a[d]=c[d];try{ua(a)}catch(f){}}};p("mdc",w);p("mdi",ka);p("bnc",x);p("qGC",ta);p("qm",C);p("qd",A);p("lb",sa);p("mcf"

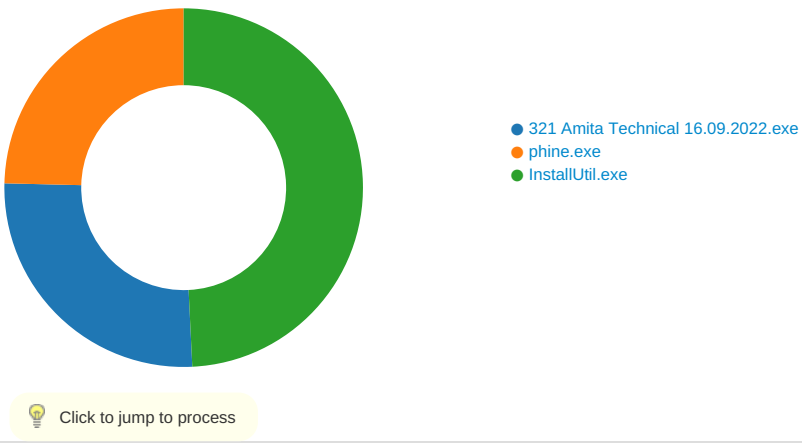
Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	71	IN	Data Raw: 36 35 62 34 0d 0a 2c 6f 61 29 3b 70 28 22 62 63 66 22 2c 6e 61 29 3b 70 28 22 61 71 22 2c 42 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 70 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 72 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 49 4b 35 4f 6d 55 55 52 64 32 45 2e 4f 2f 64 3d 31 2f 72 73 3d 41 48 70 4f 6f 6f 39 33 32 4a 69 6e 6b 53 4a 48 4b 39 32 57 67 56 6a 49 56 2d 4a 77 77 79 75 33 52 77 2f 6d 3d 5f 5f 66 65 61 74 75 72 65 73 5f 5f 22 29 29 7b 76 61 72 20 45 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 61 3d 68 2e 61 28 22 31 22 29 2c 79 Data Ascii: 65b4,oa);p("bcf",na);p("aq",B);p("mdd","");p("has",pa);p("trh",va);p("tev",ra);if(h.a("m;/_/scs/abc-static/_/js/k=gapi.gapi.en.IK5OmUURd2E.O/d=1/rs=AHpOoo932JinkSJHK92WgVjIV-Jwwyu3Rw/m=__features__")){var E=function(a,b){return wa?a||b:b},xa=h.a("1"),y
2022-09-23 06:00:22 UTC	72	IN	Data Raw: 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 64 6b 73 74 59 34 36 53 4a 71 62 67 37 5f 55 50 7a 35 32 62 67 41 77 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 34 37 33 36 33 35 31 38 32 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 32 30 38 30 31 2e 30 5f 70 30 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 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 69 6e 20 62 29 66 2e 70 75 73 68 Data Ascii: =",Math.round(1/Fa),"&ogev=",d("dkstY46SJqbg7_UPz52bgAw"),"&ogf=",g.bv.f,"&ogrp=",d(""),"&ogv=",d("473635182.0"),"&oggv="+d("es_plusone_gc_20220801.0_p0"),"&ogd=",d("com"),"&ogc=",d("GBR"),"&ogl=",d("en")];b._sn&&(b._sn="og."+b._sn);for(var k in b)f.push
2022-09-23 06:00:22 UTC	74	IN	Data Raw: 2e 6f 67 32 2e 65 6e 5f 55 53 2e 67 33 65 72 6a 35 31 55 38 45 59 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 71 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 49 29 3b 70 28 22 63 72 22 2c 4a 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 49 3b 68 2e 6c 3d 4a 3b 68 2e 6d 3d 48 3b 68 2e 6e 3d 4d 61 3b 68 2e 70 3d 4f 61 3b 68 2e 71 3d 4e 61 3b 76 61 72 20 50 61 3d 5b 22 67 62 5f 37 31 22 2c 22 67 62 5f 31 35 35 22 5d 2c 51 61 3b 66 75 6e 63 74 69 6f 6e 20 52 61 28 61 29 7b 51 61 3d 61 7d 66 75 6e 63 74 69 6f 6e 20 53 61 28 61 29 7b 76 61 72 20 62 3d 51 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 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 51 Data Ascii: .og2.en_US.g3erj51U8EY.DU");a=a.join("");qa(a)};p("ca",I);p("cr",J);p("cc",H);h.k=I;h.l=J;h.m=H;h.n=Ma;h.p=Oa;h.q=Na;var Pa=["gb_71","gb_155"],Qa;function Ra(a){Qa=a}function Sa(a){var b=Qa&&!a.href.match(/.*\/accounts\/ClearSID[?]/)&&encodeURIComponent(Q
2022-09-23 06:00:22 UTC	75	IN	Data Raw: 62 28 66 29 3b 4e 3d 64 3b 49 28 6b 2c 22 67 62 74 6f 22 29 7d 7d 7d 7d 43 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 62 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 64 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 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 65 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 72 64 64 28 61 29 7d 29 7d 2c 5a 61 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 Data Ascii: b(f);N=d;I(k,"gbto")}}}}C(function(){g.tg(a,b,!0)});bb(a)}catch(q){r(q,"sb","tg")}},db=function(a){C(function(){g.close(a)})},eb=function(a){C(function(){g.rdd(a)})},Za=function(a){var b,c=document.defaultView;c&&c.getComputedStyle?(a=c.getComputedStyle(a
2022-09-23 06:00:22 UTC	76	IN	Data Raw: 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 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 6a 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 43 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 6b 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 43 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 6c 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 2c 66 2c 6b 2c 6c 2c 6e 2c 6d 2c 71 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 61 Data Ascii: .length,d=0;d<c;d++)if(H(a,b[d]))return!0;return!1},hb=function(a,b,c){gb(a,b,c)},ib=function(a,b){gb(a,"gbe",b)},jb=function(){C(function(){g.pcm&&g.pcm()})},kb=function(){C(function(){g.pca&&g.pca()})},lb=function(a,b,c,d,f,k,l,n,m,q){C(function(){g.pa
2022-09-23 06:00:22 UTC	78	IN	Data Raw: 2c 75 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 76 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 31 7d 2c 77 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 21 4e 7d 3b 70 28 22 73 6f 22 2c 57 61 29 3b 70 28 22 73 6f 73 22 2c 56 61 29 3b 70 28 22 73 69 22 2c 58 61 29 3b 70 28 22 74 67 22 2c 63 62 29 3b 0a 70 28 22 Data Ascii: ,ub=function(a){var b="inner"+a;a="offset"+a;return window[b]?window[b]:document.documentElement&&document.documentElement[a]?document.documentElement[a]:0},vb=function(){return!1},wb=function(){return!!N};p("so",Wa);p("sos",Va);p("si",Xa);p("tg",cb);p("
2022-09-23 06:00:22 UTC	79	IN	Data Raw: 33 37 2c 33 38 2c 33 39 2c 34 30 2c 34 31 2c 34 32 2c 34 33 2c 34 38 2c 34 39 2c 35 30 30 5d 3b 76 61 72 20 46 62 3d 68 2e 62 28 22 30 2e 30 31 22 2c 31 45 2d 34 29 2c 47 62 3d 68 2e 62 28 22 31 22 2c 31 2c 48 62 3d 21 31 2c 49 62 3d 21 31 3b 69 66 28 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 4a 62 3d 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 3b 4a 62 3c 46 62 26 26 28 48 62 3d 21 30 29 3b 4a 62 3c 47 62 26 26 28 49 62 3d 21 30 29 7d 76 61 72 20 51 3d 6e 75 6c 6c 3b 0a 66 75 6e 63 74 69 6f 6e 20 4b 62 28 61 2c 62 29 7b 76 61 72 20 63 3d 46 62 2c 64 3d 48 62 3b 76 61 72 20 66 3d 61 3b 69 66 28 21 51 29 7b 51 3d 7b 7d 3b 66 6f 72 28 76 61 72 20 6b 3d 30 3b 6b 3c 45 62 2e 6c 65 6e 67 74 68 3b 6b 2b 2b 29 7b 76 61 72 20 6c 3d 45 62 5b 6b 5d 3b 51 5b 6c 5d Data Ascii: 37,38,39,40,41,42,43,48,49,500];var Fb=h.b("0.001",1E-4),Gb=h.b("1",1),Hb=!1,Ib=!1;if(h.a("1")){var Jb=Math.random();Jb<Fb&&(Hb=!0);Jb<Gb&&(Ib=!0)}var Q=null;function Kb(a,b){var c=Fb,d=Hb;var f=a;if(!Q){Q={};for(var k=0;k<Eb.length;k++){var l=Eb[k];Q[l]
2022-09-23 06:00:22 UTC	80	IN	Data Raw: 28 61 29 7d 29 7d 2c 51 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 73 28 61 29 7d 29 7d 2c 52 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 70 28 61 29 7d 29 7d 2c 53 62 3d 7b 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 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 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 Data Ascii: (a)}},Qb=function(a){C(function(){g.sps(a)})},Rb=function(a){C(function(){g.spp(a)})},Sb={"27":"https://lh3.googleusercontent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	81	IN	Data Raw: 64 5d 26 26 2d 31 21 3d 59 62 28 63 2c 64 29 3b 65 6c 73 65 20 66 6f 72 28 57 3d 7b 7d 2c 64 3d 30 3b 64 3c 63 2e 6c 65 6e 67 74 68 3b 64 2b 2b 29 57 5b 63 5b 64 5d 5d 3d 21 30 3b 67 2e 75 70 2e 73 70 6c 28 61 2c 62 2c 22 61 6f 70 22 2c 63 29 7d 7d 2c 63 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 69 66 28 58 3d 32 2c 21 58 62 29 7b 58 62 3d 21 30 3b 66 6f 72 28 76 61 72 20 61 20 69 6e 20 52 29 66 6f 72 28 76 61 72 20 62 3d 52 5b 61 5d 2c 63 3d 30 3b 63 3c 62 2e 6c 65 6e 67 74 68 3b 63 2b 2b 29 74 72 79 7b 62 5b 63 5d 28 5a 62 28 61 29 29 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 5a 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 Data Ascii: d]&&-1!=Yb(c,d);else for(W={},d=0;d<c.length;d++)W[c[d]]=!0;g.up.spl(a,b,"aop",c)}},cc=function(){try{if(X=2 ,!Xb){Xb=!0;for(var a in R)for(var b=R[a],c=0;c<b.length;c++)try{b[c](Zb(a))}catch(d){r(d,"up","tp")}}}catch(d){r(d,"up" ,"mtp")}},Zb=function(a){if
2022-09-23 06:00:22 UTC	83	IN	Data Raw: 2f 29 3b 69 66 28 63 26 26 63 5b 31 5d 29 7b 76 61 72 20 64 3d 63 5b 31 5d 2e 6d 61 74 63 68 28 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 62 22 2b 0a 62 2b 22 2d 28 5b 30 2d 39 5d 2b 29 3a 22 29 29 3b 69 66 28 64 26 26 64 5b 31 5d 29 72 65 74 75 72 6e 20 70 61 72 73 65 49 6e 74 28 64 5b 31 5d 2c 31 30 29 7d 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 67 63 63 22 29 7d 72 65 74 75 72 6e 2d 31 7d 3b 70 28 22 75 70 22 2c 7b 72 3a 24 62 2c 6e 61 70 3a 61 63 2c 61 6f 70 3a 62 63 2c 74 70 3a 63 63 2c 73 73 70 3a 5a 62 2c 73 70 64 3a 67 63 2c 67 70 64 3a 68 63 2c 61 65 68 3a 69 63 2c 61 61 6c 3a 6a 63 2c 67 63 63 3a 6b 63 7d Data Ascii: /);if(c&&c[1]){var d=c[1].match(new RegExp("\\b"+b+"-([0-9]+):"));if(d&&d[1])return parseInt(d[1],10)}}catch(f) {f.code!=DOMException.QUOTA_EXCEEDED_ERR&&r(f,"up","gcc")}return-1};p("up",{r:$b,nap:ac,aop:bc,tp:cc,ssp:Zb ,spd:gc,gpd:hc,aeh:ic,aal:jc,gcc:kc}
2022-09-23 06:00:22 UTC	84	IN	Data Raw: 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 70 6d 22 2c 7b 70 3a 22 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 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 Data Ascii: brary Authors. SPDX-License-Identifier: Apache-2.0*/var a=window.gbar;a.mcf("pm",{p:""});}catch(e) {window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Library A uthors. SPDX-License-Identifie
2022-09-23 06:00:22 UTC	85	IN	Data Raw: 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 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 62 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 76 61 72 20 63 3d 62 2e 69 3b 76 61 72 20 64 3d 63 2e 61 2c 65 3d 63 2e 63 2c 66 3d 7b 63 74 79 3a 22 47 42 52 22 2c 63 76 3a 22 34 37 33 36 33 35 31 38 32 22 2c 64 62 67 3a 64 28 22 22 29 2c 65 63 76 3a 22 30 22 2c 65 69 3a 65 28 22 64 6b 73 74 59 34 36 53 4a 71 62 67 37 5f 55 50 7a 35 32 62 67 41 77 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 Data Ascii: uthors. SPDX-License-Identifier: Apache-2.0*/var a=this||self;var b=window.gbar;var c=b.i;var d=c.a,e=c.c,f= {cty:"GBR",cv:"473635182",dbg:d(""),ecv:"0",ei:e("dkstY46SJqbg7_UPz52bgAw"),ele:d("1"),esr:e("0.1"),evts:["mou sedown","touchstart","touchmove","'
2022-09-23 06:00:22 UTC	86	IN	Data Raw: 61 72 2e 65 6c 69 28 29 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 69 64 3d 67 62 77 3e 3c 64 69 76 20 69 64 3d 67 62 7a 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 69 64 3d 67 62 7a 63 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 63 6c 61 73 73 3d 22 67 62 7a 74 20 67 62 7a 30 6c 20 67 62 70 31 22 20 69 64 3d 67 62 5f 31 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 77 65 62 68 70 3f 74 61 62 3d 77 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 69 64 3d 67 62 7a 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 Data Ascii: ar.eli()</script> <ol id=gbzc class=gbtc><li class=gbt>Search <li clas
2022-09-23 06:00:22 UTC	88	IN	Data Raw: 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 20 61 72 69 61 2d 68 61 73 70 6f 70 75 70 3d 74 72 75 65 20 61 72 69 61 2d 6f 77 6e 73 3d 67 62 64 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 74 73 20 63 6c 61 73 73 3d 22 67 62 74 73 20 67 62 74 73 61 22 3e 3c 73 70 61 6e 20 69 64 3d 67 62 7a 74 6d 73 20 63 6c 61 73 73 3d 22 67 62 74 73 20 67 62 74 73 61 22 3e 3c 73 70 61 6e 20 69 64 3d 67 62 7a 74 6d 73 31 3e 4d 6f 72 65 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 6d 61 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 61 38 50 37 4a 46 2d 4a 41 77 68 5f 4b 50 74 69 37 36 38 43 79 41 27 3e 64 6f 63 75 6d 65 6e 74 2e Data Ascii: //www.google.co.uk/intl/en/about/products?tab=wh" aria-haspopup=true aria-owns=gbd> More<script nonce='a8P7JF-JAwh_KPti768CyA'>document.
2022-09-23 06:00:22 UTC	89	IN	Data Raw: 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 32 35 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 64 6f 63 75 6d 65 6e 74 2f 3f 75 73 70 3d 64 6f 63 73 5f 61 6c 63 22 3e 44 6f 63 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 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 Data Ascii: <li class=gbmtc>Docs <li class=gbmtc> <li class=gbmtc><a href="https://www.googl e.co.uk/intl/en/about/products?tab=wh" class=gb
2022-09-23 06:00:22 UTC	90	IN	Data Raw: 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 35 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 67 35 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 63 3e 3c 6f 6c 20 69 64 3d 67 62 6f 6d 20 63 6c 61 73 73 3d 67 62 6d 63 63 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 63 20 67 62 6d 74 63 22 3e 3c 61 20 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 2f 70 72 65 66 65 72 65 6e 63 65 73 3f 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 Data Ascii: r.tg(event,this); });</script> <ol id=gbom c lass=gbmcc><li class="gbkc gbmtc">Search settings <li class=gbmtc> <li clas

Timestamp	kBytes transferred	Direction	Data
2022-09-23 06:00:22 UTC	92	IN	Data Raw: 38 22 20 6e 61 6d 65 3d 22 71 22 20 73 69 7a 65 3d 22 35 37 22 3e 3c 2f 64 69 76 3e 3c 62 72 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 22 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 76 61 6c 75 65 3d 22 47 6f 6f 67 6c 65 20 53 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 62 74 6e 47 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 2f 73 70 61 6e 3e 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 5f 31 22 20 76 61 6c 75 65 3d 22 49 27 6d 20 46 65 65 6c 69 Data Ascii: 8" name="q" size="57"> <br style="line-height:0"><input c lass="lsb" value="Google Search" name="btnG" type="submit"><input class="lsb" id="tsuid_1" value="I'm Feeli
2022-09-23 06:00:22 UTC	93	IN	Data Raw: 6c 75 65 3d 61 29 3b 66 26 26 77 69 6e 64 6f 77 2e 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 66 7d 2c 30 29 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 66 6f 72 6d 3e 3c 64 69 76 20 69 64 3d 22 67 61 63 5f 73 63 6f 6e 74 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 33 25 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 2e 35 65 6d 22 3e 3c 62 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 Data Ascii: lue=a);f&&window.setTimeout(function(){location.href=f},0)};}).call(this);</script></form> <div style=" margin:19px auto;text-align
2022-09-23 06:00:22 UTC	94	IN	Data Raw: 65 78 63 6d 3a 5b 5d 7d 3b 7d 29 28 29 3b 3c 2f 73 63 72 69 70 74 3e 20 20 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 61 38 50 37 4a 46 2d 4a 41 77 68 5f 4b 50 74 69 37 36 38 43 79 41 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 75 3d 27 2f 78 6a 73 2f 5f 2f 6a 73 2f 6b 5c 78 33 64 78 6a 73 2e 68 70 2e 65 6e 2e 50 61 32 46 7a 52 51 66 79 57 55 2e 4f 2f 61 6d 5c 78 33 64 41 41 43 65 41 41 41 6b 41 45 41 42 2f 64 5c 78 33 64 31 2f 65 64 5c 78 33 64 31 2f 72 73 5c 78 33 64 41 43 54 39 30 6f 47 47 4f 48 41 47 39 39 71 72 61 41 39 68 59 4d 73 78 64 79 71 33 54 58 33 62 76 51 2f 6d 5c 78 33 64 73 62 5f 68 65 2c 64 27 3b 0a 76 61 72 20 64 3d 74 68 69 73 7c 7c 73 65 6c 66 2c 65 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 7d 3b 0a 76 Data Ascii: excm:[]};})();</script> <script nonce="a8P7JF-JAwh_KPti768CyA">(function(){var u='/xjs/_/js/k\x3dxjs.hp.en. Pa2FzRQfyWU.O/am\x3dAACeAAAkAEAB/d\x3d1/ed\x3d1/rs\x3dACT90oGGOHAG99qraA9hYMsxdyq3TX3bvQ/m \x3dsb_he,d';var d=this||self,e=function(a){return a};v
2022-09-23 06:00:22 UTC	95	IN	Data Raw: 6f 6e 28 65 29 7b 74 68 72 6f 77 20 65 3b 7d 0a 66 75 6e 63 74 69 6f 6e 20 5f 46 5f 69 6e 73 74 61 6c 6c 43 73 73 28 63 29 7b 7d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 6f 6f 67 6c 65 2e 6a 6c 3d 7b 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 64 77 75 3a 74 72 75 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 69 6e 6a 3a 27 6e 6f 6e 65 27 2c 69 6e 6a 74 3a 30 2c 69 6e 6a 74 68 3a 30 2c 69 6e 6a 76 32 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 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 Data Ascii: on(e){throw e;}function _F_installCss(c){}(function(){google.jl={blt:'none',chnk:0,dw:false,dwu:true,emtn:0, end:0,ine:false,injs:'none',injt:0,injth:0,injv2:false,lls:'default',pdt:0,rep:0,snet:true,strt:0,ubm:false,uwp:true};})();(function() {var pmc='{
2022-09-23 06:00:22 UTC	97	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: 321 Amita Technical 16.09.2022.exe PID: **5436**, Parent PID: **2256**

General

Target ID:	0
Start time:	07:59:57
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe"
Imagebase:	0xed0000
File size:	636416 bytes
MD5 hash:	A2A924C124BBC597A76495B4FB08F906
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000000.00000002.343398236.00000000028F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000000.00000002.346179647.0000000002BC0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.350191112.00000000039A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.350191112.00000000039A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000000.00000002.350191112.00000000039A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.350191112.00000000039A9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.351247039.0000000003AB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.351247039.0000000003AB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000000.00000002.351247039.0000000003AB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.351247039.0000000003AB0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\321 Amita Technical 16.09.2022.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCFC78D	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\321 Amita Technical 16.09.2022.exe	C:\Users\user\AppData\Local\Temp\phine.exe	success or wait	1	7BA1ACE	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\321 Amita Technical 16.09.2022.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",12,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6CCFC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C9C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B831B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: phine.exe PID: **5604**, Parent PID: **5436**

General

Target ID:	1
Start time:	08:00:17
Start date:	23/09/2022
Path:	C:\Users\user\AppData\Local\Temp\phine.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\phine.exe"

Imagebase:	0xed0000
File size:	636416 bytes
MD5 hash:	A2A924C124BBC597A76495B4FB08F906
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.543325516.0000000003C3E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.545362105.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.545362105.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000001.00000002.545362105.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.545362105.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.543889878.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.543889878.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000001.00000002.543889878.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.543889878.0000000003C98000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_DarkTortilla, Description: Yara detected DarkTortilla Crypter, Source: 00000001.00000002.528157488.0000000002BE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\phine.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\phine.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",12,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6CCFC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C9C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B831B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: **5980**, Parent PID: **5604**

General

Target ID:	4
Start time:	08:01:07
Start date:	23/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Imagebase:	0xe30000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.447939474.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.447939474.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.447939474.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.562334194.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.562334194.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C9ECF06	unknown
C:\Users\user\AppData\Roaming\Word	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B83BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Word\Word.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6B83DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Word\Word.exe	0	41064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 07 5a fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 fd 72 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 01 00 03 00 60 fd 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	MZ@!L!This program cannot be run in DOS mode.$PELZZ0Tr @ `	success or wait	1	6B83DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C9C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6C9CCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6C9CCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6C9C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6B831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6B831B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6B831B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Word	unicode	C:\Users\user\AppData\Roaming\Word\Word.exe	success or wait	1	6B83646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Word	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6B83DE2E	RegSetValueExW

Disassembly

No disassembly