ID: 673906
Sample Name:
D6GEVBNNH11111.exe
Cookbook: default.jbs
Time: 21:51:07
Date: 26/07/2022
Version: 35.0.0 Citrine

Table of Contents

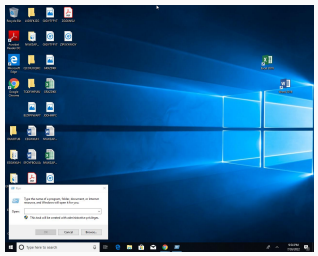
Windows Analysis Report

D6GEVBNNH11111.exe

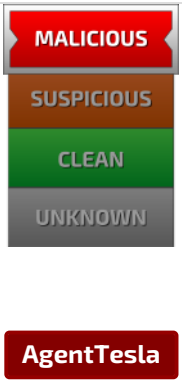
Overview

General Information

Sample Name:	D6GEVBNNH11111.exe
Analysis ID:	673906
MD5:	9cef8265c679ba…
SHA1:	ac7faaa7e84399..
SHA256:	18f7c9fcf552066…
Tags:	agenttesla exe
Infos:	



Detection



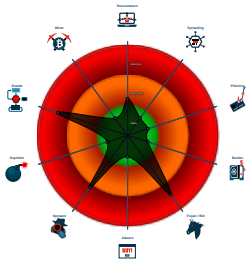
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Drops executable to a common third…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Moves itself to temp directory
- Queries sensitive network adapter in…
- Queries sensitive BIOS Information…

Classification



Process Tree

- **System is w10x64**
- D6GEVBNNH11111.exe (PID: 3436 cmdline: "C:\Users\user\Desktop\D6GEVBNNH11111.exe" MD5: 9CEF8265C679BAFB06F885678CEAB7BD)
  - geater.exe (PID: 3972 cmdline: "C:\Users\user\AppData\Local\Temp\geater.exe" MD5: 9CEF8265C679BAFB06F885678CEAB7BD)
    - InstallUtil.exe (PID: 3512 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
0000000F.00000000.561341870.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000000.561341870.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000F.00000000.561888828.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000000.561888828.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.668565825.00000000046A6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.geater.exe.47ad7e2.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.geater.exe.47ad7e2.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.geater.exe.47ad7e2.5.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30eba:$s10: logins • 0x30921:$s11: credential • 0x2cec3:$g1: get_Clipboard • 0x2ced1:$g2: get_Keyboard • 0x2cede:$g3: get_Password • 0x2e1e3:$g4: get_CtrlKeyDown • 0x2e1f3:$g5: get_ShiftKeyDown • 0x2e204:$g6: get_AltKeyDown
6.2.geater.exe.47e20b8.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.geater.exe.47e20b8.6.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 73 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)

Persistence and Installation Behavior

Drops executable to a common third party application directory

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)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

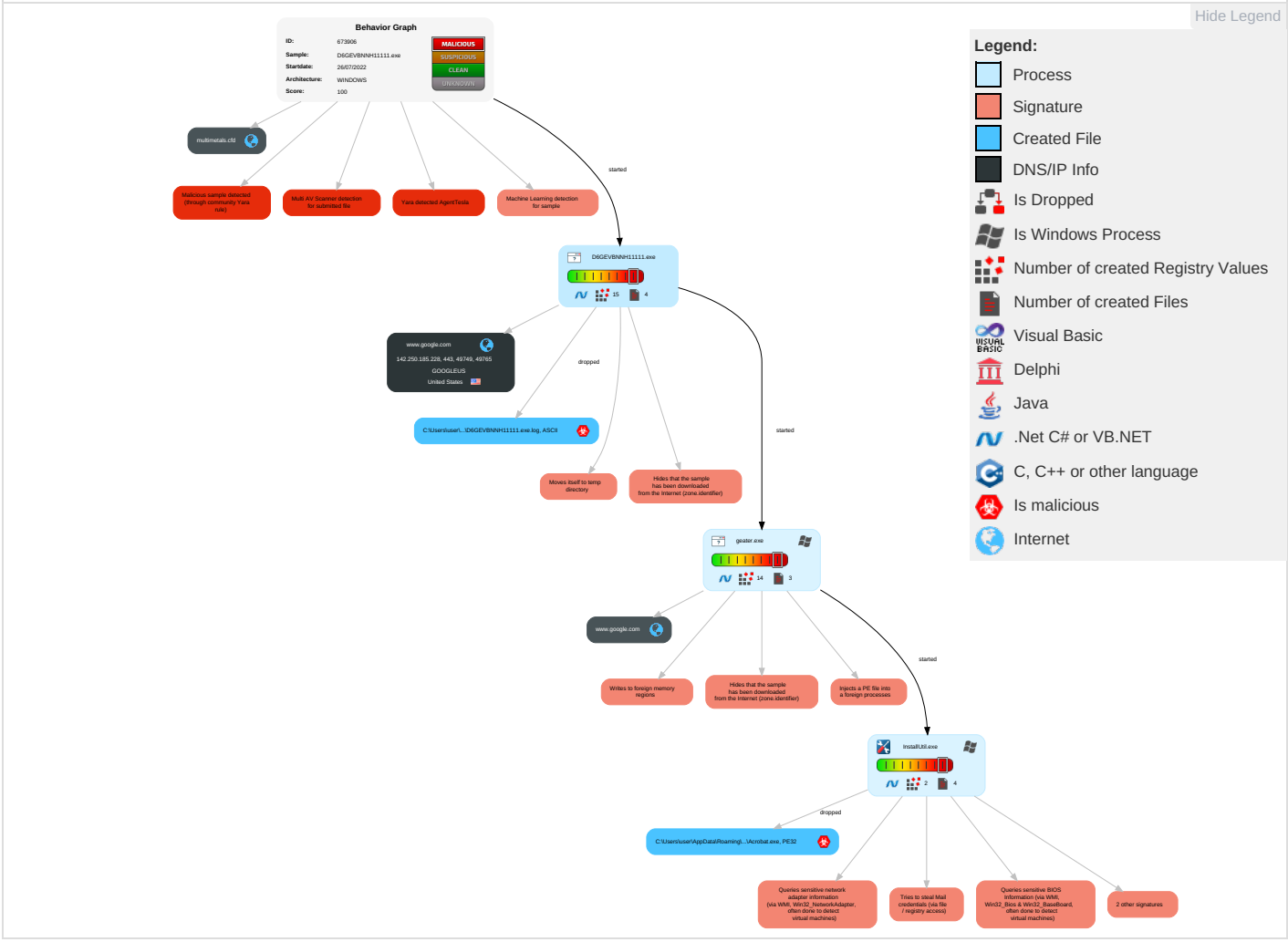
Remote Access Functionality

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
1 Valid Accounts	2 1 1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Disable or Modify Tools	1 Input Capture	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Obfuscated Files or Information	LSASS Memory	1 1 3 System Information Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	2 1 1 Process Injection	1 Software Packing	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Input Capture	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)	1 Registry Run Keys / Startup Folder	2 1 Masquerading	NTDS	1 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Valid Accounts	LSA Secrets	1 Process 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 Access Token Manipulation	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	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	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window 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	2 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

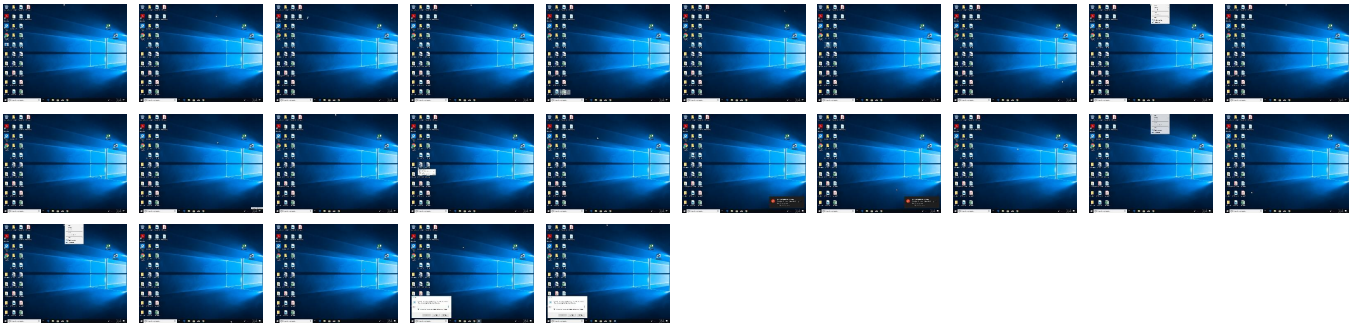
Behavior Graph



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
D6GEVBNNH11111.exe	41%	Virustotal		Browse
D6GEVBNNH11111.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
D6GEVBNNH11111.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.InstallUtil.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.InstallUtil.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.InstallUtil.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.InstallUtil.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://OKJTye.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcar	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://r3.i.lencr.org/0W	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://maKknZWobi.net	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy0	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://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ers	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	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://https://www.google.comT	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/1	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0n	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://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/Y0	0%	URL Reputation	safe	
http://www.carterandcone.comeguKx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.carterandcone.comadi	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/U	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cng	0%	URL Reputation	safe	
http://www.carterandcone.comI	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://www.carterandcone.commpa	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://www.carterandcone.como.ox	0%	Avira URL Cloud	safe	
http://multimetals.cfd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/on	0%	URL Reputation	safe	
http://www.founder.com.cn/cnCh	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaH	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Sue	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/M	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g%%n	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.carterandcone.comint	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/is	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://https://www.google.com3GetManifestResourceStream	0%	Avira URL Cloud	safe	
http://www.carterandcone.comw	0%	URL Reputation	safe	
http://www.founder.com.cn/cn2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://ns.adobe.c/g4	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/rk	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn/w	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	142.250.185.228	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, 0000000F.00000002.686918576.00000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://OKJTye.com	InstallUtil.exe, 0000000F.00000002.686918576.00000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comcar	D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-int0	InstallUtil.exe, 0000000F.00000002.694815599.00000000005FBE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.i.lencr.org/0W	InstallUtil.exe, 0000000F.00000002.691205216.000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.695758505.000000000066C9000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://maKknZWobi.net	InstallUtil.exe, 0000000F.00000002.691023728.000000002DB0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	InstallUtil.exe, 0000000F.00000002.694145293.000000005ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobe.c/g	geater.exe, 00000006.00000003.468594106.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.465086224.000000000C1F0000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.469714782.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.466707799.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.465370000.000000000C1F0000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.475458159.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.466241757.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.474734788.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.467189569.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.545768545.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.475210422.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.474948415.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.474548675.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comypo	D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ers	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/~	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com	D6GEVBNNH11111.exe, D6GEVBNNH11111.exe, 00000000.00000002.450466503.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000002.648331977.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.comT	D6GEVBNNH11111.exe, 00000000.00000002.450466503.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000002.648331977.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comC	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/1	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423114721.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423327035.000000000C17E000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0n	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0	InstallUtil.exe, 0000000F.00000002.694815599.00000000005FBE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	InstallUtil.exe, 0000000F.00000002.696225493.00000000066FC000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.691205216.0000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	InstallUtil.exe, 0000000F.00000002.696225493.00000000066FC000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.691205216.0000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	InstallUtil.exe, 0000000F.00000002.686918576.00000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	InstallUtil.exe, 0000000F.00000002.691205216.00000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.695758505.00000000066C9000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comeguKx	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna	D6GEVBNNH11111.exe, 00000000.00000003.421010083.000000000C181000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comadi	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/U	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.00000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cng	D6GEVBNNH11111.exe, 00000000.00000003.420985402.000000000C1A2000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.421003844.00000000C1A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	D6GEVBNNH11111.exe, 00000000.00000002.450466503.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000002.648331977.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comI	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	InstallUtil.exe, 0000000F.00000002.686918576.0000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.carterandcone.commpa	D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.00000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	InstallUtil.exe, 0000000F.00000002.691205216.0000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.696582451.0000000006725000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.ox	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://multimetals.cfd	InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422003230.00000000C189000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/U	D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423327035.00000000C17E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comc	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://cps.letsencrypt.org0	InstallUtil.exe, 0000000F.00000002.691205216.0000000002DCB000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.694046075.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.690780729.0000000002D8D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000F.00000002.695758505.00000000066C9000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

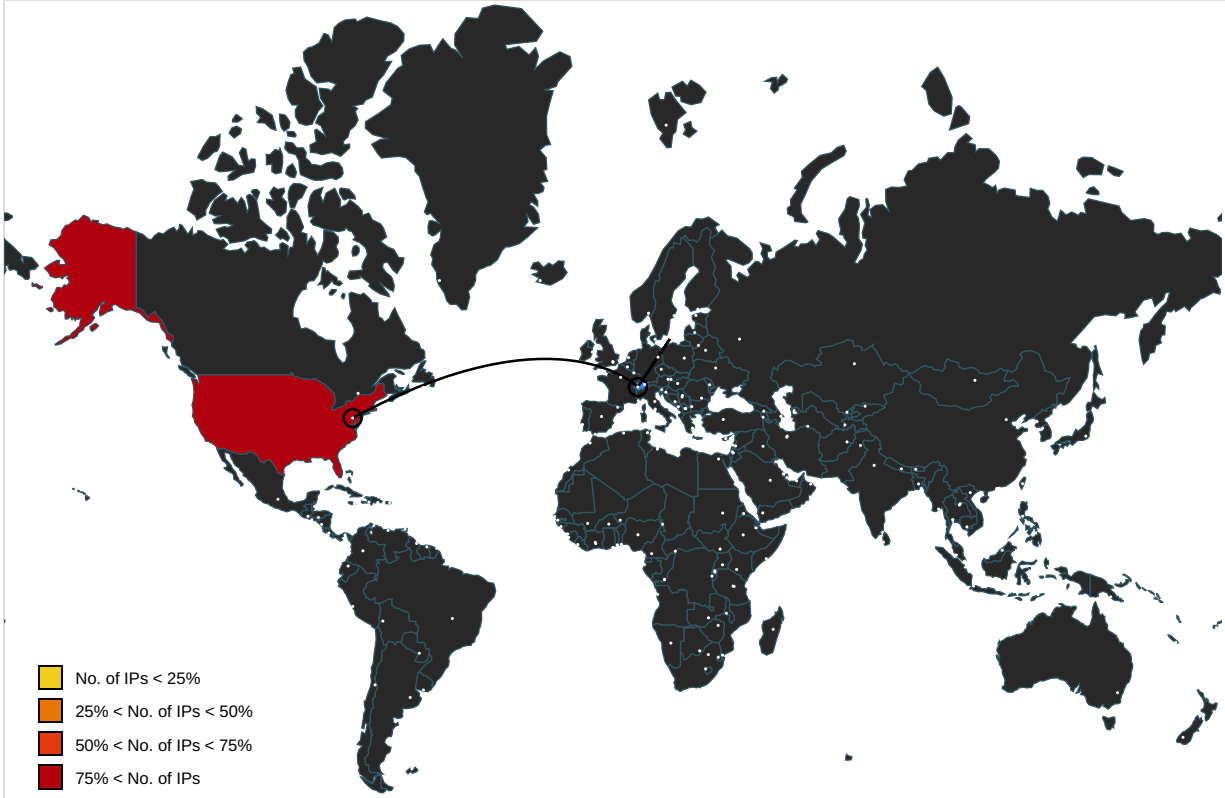
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es/legislacion_c.htm0U	InstallUtil.exe, 0000000F.00000002.694815599.00000005FBE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comTC	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	InstallUtil.exe, 0000000F.00000002.686918576.00000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	InstallUtil.exe, 0000000F.00000002.695795045.000000066E2000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	InstallUtil.exe, 0000000F.00000002.686918576.00000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423327035.000000000C17E000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.00000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/on	D6GEVBNNH11111.exe, 00000000.00000003.423114721.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423327035.000000000C17E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnCh	D6GEVBNNH11111.exe, 00000000.00000003.421412161.000000000C176000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaH	D6GEVBNNH11111.exe, 00000000.00000003.430433465.000000000C189000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000002.460978674.000000000C17B000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.447630466.000000000C17B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	D6GEVBNNH11111.exe, 00000000.00000003.419597185.000000000C182000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Sue	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.00000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/M	D6GEVBNNH11111.exe, 00000000.00000003.421412161.000000000C176000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g%%n	geater.exe, 00000006.00000002.682161073.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.642265092.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	D6GEVBNNH11111.exe, 00000000.00000003.421430217.000000000C17E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comint	D6GEVBNNH11111.exe, 00000000.00000003.422408075.000000000C176000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.421067665.000000000C1A1000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.420985402.000000000C1A2000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.421003844.000000000C1A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	D6GEVBNNH11111.exe, 00000000.00000003.422880183.000000000C179000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/is	D6GEVBNNH11111.exe, 00000000.00000003.423114721.000000000C187000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	D6GEVBNNH11111.exe, 00000000.00000003.429144369.000000000C179000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com3GetManifestResourceStream	D6GEVBNNH11111.exe	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comw	D6GEVBNNH11111.exe, 00000000.00000003.422384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn2	D6GEVBNNH11111.exe, 00000000.00000003.421067665.000000000C1A1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	D6GEVBNNH11111.exe, 00000000.00000003.423641322.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000002.461913156.000000000D382000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423753219.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423114721.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423447686.000000000C180000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.422880183.000000000C179000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423596826.000000000C187000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423327035.000000000C17E000.00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.423662070.000000000C184000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g4	geater.exe, 00000006.00000003.474106682.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp, geater.exe, 00000006.00000003.464715331.000000000C1F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	D6GEVBNNH11111.exe, 00000000.00000003.430433465.000000000C189000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/l	D6GEVBNNH11111.exe, 00000000.00000003.42 3641322.000000000C180000.00000004.000008 00.00020000.00000000.sdmp, D6GEVBNNH1111 1.exe, 00000000.00000003.423753219.00000 0000C180000.00000004.00000800.00020000.0 0000000.sdmp, D6GEVBNNH11111.exe, 000000 00.00000003.423114721.000000000C187000.0 0000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.4 23447686.000000000C180000.00000004.00000 800.00020000.00000000.sdmp, D6GEVBNNH111 11.exe, 00000000.00000003.422880183.0000 00000C179000.00000004.00000800.00020000. 00000000.sdmp, D6GEVBNNH11111.exe, 00000 000.00000003.423596826.000000000C187000. 00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003. 423327035.000000000C17E000.00000004.0000 0800.00020000.00000000.sdmp, D6GEVBNNH11 111.exe, 00000000.00000003.423662070.000 000000C184000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	D6GEVBNNH11111.exe, 00000000.00000002.46 1913156.000000000D382000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/g	D6GEVBNNH11111.exe, 00000000.00000003.42 3641322.000000000C180000.00000004.000008 00.00020000.00000000.sdmp, D6GEVBNNH1111 1.exe, 00000000.00000003.423753219.00000 0000C180000.00000004.00000800.00020000.0 0000000.sdmp, D6GEVBNNH11111.exe, 000000 00.00000003.423114721.000000000C187000.0 0000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.4 23447686.000000000C180000.00000004.00000 800.00020000.00000000.sdmp, D6GEVBNNH111 11.exe, 00000000.00000003.422880183.0000 00000C179000.00000004.00000800.00020000. 00000000.sdmp, D6GEVBNNH11111.exe, 00000 000.00000003.423596826.000000000C187000. 00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003. 423327035.000000000C17E000.00000004.0000 0800.00020000.00000000.sdmp, D6GEVBNNH11 111.exe, 00000000.00000003.423662070.000 000000C184000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/e	D6GEVBNNH11111.exe, 00000000.00000003.42 3641322.000000000C180000.00000004.000008 00.00020000.00000000.sdmp, D6GEVBNNH1111 1.exe, 00000000.00000003.423753219.00000 0000C180000.00000004.00000800.00020000.0 0000000.sdmp, D6GEVBNNH11111.exe, 000000 00.00000003.423447686.000000000C180000.0 0000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.4 23596826.000000000C187000.00000004.00000 800.00020000.00000000.sdmp, D6GEVBNNH111 11.exe, 00000000.00000003.423662070.0000 00000C184000.00000004.00000800.00020000. 00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cns-m	D6GEVBNNH11111.exe, 00000000.00000003.42 1430217.000000000C17E000.00000004.000008 00.00020000.00000000.sdmp, D6GEVBNNH1111 1.exe, 00000000.00000003.421594428.00000 0000C173000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/rk	D6GEVBNNH11111.exe, 00000000.00000003.42 3641322.000000000C180000.00000004.000008 00.00020000.00000000.sdmp, D6GEVBNNH1111 1.exe, 00000000.00000003.423753219.00000 0000C180000.00000004.00000800.00020000.0 0000000.sdmp, D6GEVBNNH11111.exe, 000000 00.00000003.423114721.000000000C187000.0 0000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003.4 23447686.000000000C180000.00000004.00000 800.00020000.00000000.sdmp, D6GEVBNNH111 11.exe, 00000000.00000003.423596826.0000 00000C187000.00000004.00000800.00020000. 00000000.sdmp, D6GEVBNNH11111.exe, 00000 000.00000003.423327035.000000000C17E000. 00000004.00000800.00020000.00000000.sdmp, D6GEVBNNH11111.exe, 00000000.00000003. 423662070.000000000C184000.00000004.0000 0800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn/w	D6GEVBNNH11111.exe, 00000000.00000003.42384405.000000000C173000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	673906
Start date and time: 26/07/202221:51:07	2022-07-26 21:51:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	D6GEVBNNH11111.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 39.7% • Quality standard deviation: 25.6%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, licensing.mp.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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.

Simulations

Behavior and APIs

Time	Type	Description
21:52:28	API Interceptor	1x Sleep call for process: D6GEVBNNH11111.exe modified
21:52:42	API Interceptor	202x Sleep call for process: geater.exe modified
21:54:03	API Interceptor	68x Sleep call for process: InstallUtil.exe modified
21:54:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Acrobat C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
21:54:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Acrobat C:\Users\user\AppData\Roaming\Acrobat\Acrobat.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\D6GEVBNNH11111.exe.log

Process:	C:\Users\user\Desktop\D6GEVBNNH11111.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MIHKov2HKXwYHKhQnoPtHoxHhAHKzvr3
MD5:	90DA70F21E67A8A3197C9F454FA9CB57
SHA1:	FC0B4A2B0F54E399477E168EEAFE962E6589DF91
SHA-256:	FEA95A3982BE3C224FDDFCE307C75459525FDFE66B5A7E6D83625FF51542F54E
SHA-512:	8563365117151AC0F90DFF6352D766F9A06E7AFCE2A2D949EC2A59DFA7078615BBCE59E6B081F351D45F8BB50793129509810EAF97F8D42ECD4F3B21AB3938C
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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\b219d4630d26b880

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

Process:	C:\Users\user\AppData\Local\Temp\geater.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MIHKov2HKXwYHKhQnoPtHoxHhAHKzvr3
MD5:	90DA70F21E67A8A3197C9F454FA9CB57
SHA1:	FC0B4A2B0F54E399477E168EEAFE962E6589DF91
SHA-256:	FEA95A3982BE3C224FDDFCE307C75459525FDFE66B5A7E6D83625FF51542F54E
SHA-512:	8563365117151AC0F90DFF6352D766F9A06E7AFCE2A2D949EC2A59DFA7078615BBCE59E6B081F351D45F8BB50793129509810EAF97F8D42ECD4F3B21AB3938C
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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\b219d4630d26b880

C:\Users\user\AppData\Roaming\Acrobat\Acrobat.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**

Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....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):	6.678403713726006
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	D6GEVBNNH11111.exe
File size:	640512
MD5:	9cef8265c679bafb06f885678ceab7bd
SHA1:	ac7faaa7e8439951eaafd8e02007f33a555cd01b
SHA256:	18f7c9fcf55206644996038b2908aa3871e3ea9affa4c6d62a7460f5b95cca90
SHA512:	ab176b5348a6a69752eb9e47e2ed11f5130a02104f38932f6f88058bed797e0ab8ffabe665c353ba174788cf60d3114961554ce41bef850c4161cc9316451533
SSDEEP:	12288:7yJTxDWRQLg9r91BXxQ/q22ZzGSf1q6B0sQuc9G:7ynWRQerDxxs32NG61q6PQuc
TLSH:	A4D4BE0367988B94C9A4B7BF22D1AB0013F9F0C76B02DB0B6F4B45E565A72C17E1DB49
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q1.4.....P.....N.... .....@.. ....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49d84e
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:	0x34EF3151 [Sat Feb 21 19:56:01 1998 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

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
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	0x9d7f8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0x646	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	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	0x9b854	0x9ba00	False	0.6776276982931727	data	6.690081890735924	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0x646	0x800	False	0.35693359375	data	3.7271367690740242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

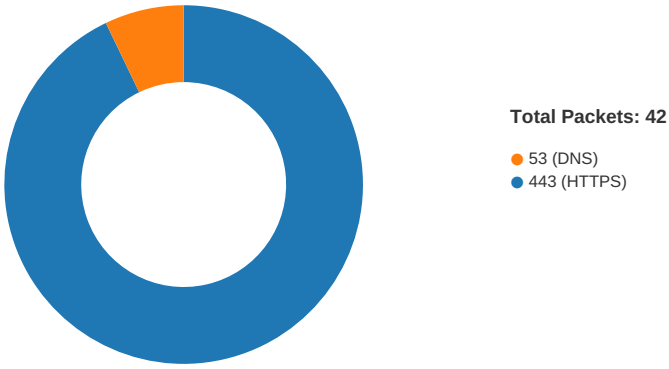
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9e0a0	0x3bc	data		
RT_MANIFEST	0x9e45c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2022 21:52:10.754509926 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:10.754553080 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:10.754661083 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:10.826807022 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:10.826839924 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:10.876451969 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:10.876605034 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:10.879754066 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:10.879767895 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:10.879992962 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:10.929282904 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.224459887 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.267405987 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300113916 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300235033 CEST	443	49749	142.250.185.228	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2022 21:52:11.300316095 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300329924 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.300373077 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300437927 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.300447941 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300479889 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.300575018 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.300846100 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.303319931 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.303416967 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.303435087 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.303461075 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.303527117 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.303903103 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.304688931 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.304757118 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.304810047 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.304826975 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.304898977 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.317186117 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.317454100 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.317547083 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.317639112 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.317677021 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.317768097 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.318171978 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321326971 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321444988 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321506023 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.321526051 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321599007 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.321609020 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321645021 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.321717978 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.322206020 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.323597908 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.323710918 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.323748112 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.323765993 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.323843002 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.324445009 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.325731993 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.325835943 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.325846910 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.325872898 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.325956106 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.326878071 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.327651024 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.327747107 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.327769041 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.327799082 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.327897072 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.328733921 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.329996109 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.330111027 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.330115080 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.330140114 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.330195904 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.331032038 CEST	443	49749	142.250.185.228	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2022 21:52:11.331286907 CEST	443	49749	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:11.331392050 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:11.345297098 CEST	49749	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.001318932 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.001386881 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.001743078 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.052330971 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.052376986 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.102763891 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.102883101 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.107256889 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.107271910 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.107842922 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.227751970 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.569200039 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.611373901 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.645994902 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646119118 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646236897 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.646244049 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646267891 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646332979 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.646361113 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646836996 CEST	443	49765	142.250.185.228	192.168.2.5
Jul 26, 2022 21:52:29.646922112 CEST	49765	443	192.168.2.5	142.250.185.228
Jul 26, 2022 21:52:29.646939039 CEST	443	49765	142.250.185.228	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2022 21:52:10.696971893 CEST	61356	53	192.168.2.5	8.8.8.8
Jul 26, 2022 21:52:10.716706038 CEST	53	61356	8.8.8.8	192.168.2.5
Jul 26, 2022 21:52:28.957506895 CEST	59661	53	192.168.2.5	8.8.8.8
Jul 26, 2022 21:52:28.975078106 CEST	53	59661	8.8.8.8	192.168.2.5
Jul 26, 2022 21:54:17.178013086 CEST	64405	53	192.168.2.5	8.8.8.8
Jul 26, 2022 21:54:17.373930931 CEST	53	64405	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jul 26, 2022 21:53:38.107453108 CEST	192.168.2.5	8.8.8.8	d043	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 26, 2022 21:52:10.696971893 CEST	192.168.2.5	8.8.8.8	0x9cfc	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 26, 2022 21:52:28.957506895 CEST	192.168.2.5	8.8.8.8	0x627d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 26, 2022 21:54:17.178013086 CEST	192.168.2.5	8.8.8.8	0xb788	Standard query (0)	multimetals.cfd	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 26, 2022 21:52:10.716706038 CEST	8.8.8.8	192.168.2.5	0x9cfc	No error (0)	www.google.com		142.250.185.228	A (IP address)	IN (0x0001)
Jul 26, 2022 21:52:28.975078106 CEST	8.8.8.8	192.168.2.5	0x627d	No error (0)	www.google.com		142.250.185.228	A (IP address)	IN (0x0001)
Jul 26, 2022 21:54:17.373930931 CEST	8.8.8.8	192.168.2.5	0xb788	No error (0)	multimetals.cfd		192.185.37.183	A (IP address)	IN (0x0001)

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	49749	142.250.185.228	443	C:\Users\user\Desktop\D6GEVBNNH11111.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-07-26 19:52:11 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 26 Jul 2022 19:52:11 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=AakniGMsW-4wpxoyuTYivGkd8FPp-UdNGgpcHa_Os971pn8smUygV4kG7Q; expires=Sun, 22-Jan-2023 19:52:11 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=6.SE=VAmrEV0yWs2eAo9BYyz8TM8ICzr_Rzh6_yA01m5sY2Qgxt-cqlM4kuBpZKC7S6vP4XK36RheRCNRThaWRryBtUQJ1iydpVP3VqrRziocXwLln9VibJHnwC7PVRRMgzG8M2MhARvaFQ9uJnq5nQsYDlOvsXa33nFqldguGFr__r8; expires=Sat, 26-Aug-2023 12:10:29 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+624; expires=Thu, 25-Jul-2024 19:52:11 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
2022-07-26 19:52:11 UTC	1	IN	Data Raw: 35 38 33 39 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 64 65 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 2f 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 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 64 65 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 Data Ascii: 5839<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="de"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content
2022-07-26 19:52:11 UTC	1	IN	Data Raw: 3d 22 2f 6c 6f 67 6f 73 2f 64 6f 6f 64 6c 65 73 2f 32 30 32 32 2f 63 65 6c 65 62 72 61 74 69 6e 67 2d 73 74 65 65 6c 70 61 6e 2d 36 37 35 33 36 35 31 38 33 37 31 30 38 34 36 37 2e 34 2d 6c 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 69 72 20 66 65 69 65 72 6e 20 64 69 65 20 53 74 65 65 6c 20 50 61 6e 22 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 74 69 74 6c 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 69 72 20 66 65 69 65 72 6e 20 64 69 65 20 53 74 65 65 6c 20 50 61 6e 21 20 23 47 6f 6f 67 6c 65 44 6f 6f 64 6c 65 22 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 Data Ascii: ="/logos/doodles/2022/celebrating-steelpan-6753651837108467.4-l.png" itemprop="image"><meta content="Wir feiern die Steel Pan" property="twitter:title"><meta content="Wir feiern die Steel Pan! #GoogleDoodle" property="twitter:description"><meta content="W
2022-07-26 19:52:11 UTC	2	IN	Data Raw: 31 34 2c 31 30 38 2c 33 34 30 36 2c 36 30 36 2c 32 30 32 33 2c 32 32 39 37 2c 31 34 36 37 30 2c 33 32 32 37 2c 32 38 34 35 2c 38 2c 34 38 31 30 2c 31 2c 32 38 39 35 38 2c 31 38 35 30 2c 31 35 37 35 37 2c 31 2c 32 2c 35 37 36 2c 36 31 38 32 2c 32 37 38 2c 31 34 38 2c 31 33 39 37 35 2c 34 2c 31 35 32 38 2c 32 33 30 34 2c 37 30 33 39 2c 32 30 33 30 39 2c 34 37 36 34 2c 32 36 35 38 2c 37 33 35 35 2c 31 38 30 39 37 2c 31 36 37 38 36 2c 35 37 38 38 2c 32 35 36 39 2c 34 30 39 32 2c 32 2c 34 30 35 32 2c 33 2c 33 35 34 31 2c 31 2c 34 32 31 35 34 2c 32 2c 31 34 30 32 32 2c 31 34 31 31 36 2c 31 31 36 32 33 2c 35 36 37 39 2c 31 30 32 30 2c 32 33 38 31 2c 31 34 30 32 33 2c 36 39 33 38 2c 32 2c 31 2c 39 2c 37 37 36 39 2c 34 35 36 37 2c 36 32 35 33 2c 32 33 34 32 34 2c Data Ascii: 14,108,3406,606,2023,2297,14670,3227,2845,8,4810,1,28958,1850,15757,1,2,576,6182,278,148,13975,4,1528,2304,7039,20309,4764,2658,7355,18097,16786,5788,2569,4092,2,4052,3,3541,1,42154,2,14022,14116,11623,5679,1020,2381,14023,6938,2,1,9,7769,4567,6253,23424,
2022-07-26 19:52:11 UTC	3	IN	Data Raw: 3b 21 63 26 26 66 2e 5f 63 73 68 69 64 26 26 2d 31 3d 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 63 73 68 69 64 3d 22 29 26 26 22 73 6c 68 22 21 3d 3d 61 26 26 28 64 3d 22 26 63 73 68 69 64 3d 22 2b 66 2e 5f 63 73 68 69 64 29 3b 63 3d 63 7c 7c 22 2f 22 2b 28 67 7c 7c 22 67 65 6e 5f 32 30 34 22 29 2b 22 3f 61 74 79 70 3d 69 26 63 74 3d 22 2b 61 2b 22 26 63 61 64 3d 22 2b 62 2b 65 2b 22 26 7a 78 3d 22 2b 44 61 74 65 2e 6e 6f 77 28 29 2b 64 3b 2f 5e 68 74 74 70 3a 2f 69 2e 74 65 73 74 28 63 29 26 26 22 68 74 74 70 73 3a 22 3d 3d 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 26 26 28 67 6f 6f 67 6c 65 2e 6d 6c 26 26 67 6f 6f 67 6c 65 2e 6d 6c 28 45 72 72 6f 72 28 22 61 22 29 2c 21 31 2c 7b 73 72 63 3a 63 2c 67 6c 6d 6d 3a 31 7d 29 2c Data Ascii: ;!c&&f._cshid&&-1===b.search("&cshid=")&&"slh"!==a&&(d="&cshid="+f._cshid);c=c||"/"+(g||"gen_204")+"?atyp=i&ct="+a+"&cad="+b+e+"&zx="+Date.now()+d;/^http:/i.test(c)&&"https:"===window.location.protocol&&(google.ml&&google.ml(Error("a"),!1,{src:c,glmm:1}),

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	5	IN	Data Raw: 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 3b 61 3d 61 2e 70 61 72 65 6e 74 45 6c 65 6d 65 6e 74 29 69 66 28 22 41 22 3d 3d 3d 61 2e 74 61 67 4e 61 6d 65 29 7b 61 3d 22 31 22 3d 3d 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 6e 6f 68 72 65 66 22 29 3b 62 72 65 61 6b 20 61 7d 61 3d 21 31 7d 61 26 26 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 7d 2c 21 30 29 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 73 74 79 6c 65 3e 23 67 62 7b 66 6f 6e 74 3a 31 33 70 78 2f 32 37 70 78 20 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 23 67 62 7a 2c 23 67 62 67 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 77 68 69 74 65 2d 73 70 Data Ascii: document.documentElement;a=a.parentElement)if("A"===a.tagName){a="1"===a.getAttribute("data-nohref");break a}a=!1}a&&b.preventDefault()},!0);}).call(this);</script><style>#gb{font:13px/27px Arial,sans-serif;height:30px}#gbz,#gbg{position:absolute;white-sp
2022-07-26 19:52:11 UTC	6	IN	Data Raw: 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 31 70 78 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 74 6f 20 2e 67 62 6d 2c 2e 67 62 74 6f 20 23 67 62 73 7b 74 6f 70 3a 32 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 76 69 73 69 62 6c 65 7d 23 67 62 7a 20 2e 67 62 6d 7b 6c 65 66 74 3a 30 7d 23 67 62 67 20 2e 67 62 6d 7b 72 69 67 68 74 3a 30 7d 2e 67 62 78 6d 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 63 63 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 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 31 3b 74 6f 70 3a 2d 31 70 78 3b 6c 65 66 74 3a 2d 32 70 78 3b 72 69 67 68 74 3a 2d 32 70 78 3b 62 6f 74 74 6f 6d 3a 2d 32 70 78 3b 6f 70 61 63 69 74 79 3a 2e 34 3b 2d 6d 6f 7a 2d 62 Data Ascii: z-box-shadow:1px 1px 1px rgba(0,0,0,.2)}.gbto .gbm,.gbto #gbs{top:29px;visibility:visible}#gbz .gbm{left:0}#gbg .gbm{right:0}.gbxms{background-color:#ccc;display:block;position:absolute;z-index:1;top:-1px;left:-2px;right:-2px;bottom:-2px;opacity:.4;-moz-b
2022-07-26 19:52:11 UTC	7	IN	Data Raw: 7b 63 75 72 73 6f 72 3a 64 65 66 61 75 6c 74 7d 2e 67 62 74 73 7b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 31 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 31 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 3a 30 20 35 70 78 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 30 30 30 7d 2e 67 62 74 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 7a 74 20 2e 67 62 74 73 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 6f 20 2e 67 62 74 73 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: {cursor:default}.gbts{border-left:1px solid transparent;border-right:1px solid transparent;display:block;*display:inline-block;padding:0 5px;position:relative;z-index:1000}.gbts{*display:inline}.gbzt .gbts{display:inline;zoom:1}.gbto .gbts{background:#fff
2022-07-26 19:52:11 UTC	8	IN	Data Raw: 67 34 61 20 2e 67 62 74 73 7b 70 61 64 64 69 6e 67 3a 32 39 70 78 20 35 70 78 20 31 70 78 3b 2a 70 61 64 64 69 6e 67 3a 32 37 70 78 20 35 70 78 20 31 70 78 7d 23 67 62 69 34 69 2c 23 67 62 69 34 69 64 7b 6c 65 66 74 3a 35 70 78 3b 62 6f 72 64 65 72 3a 30 3b 68 65 69 67 68 74 3a 32 34 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 31 70 78 3b 77 69 64 74 68 3a 32 34 70 78 7d 2e 67 62 74 6f 20 23 67 62 69 34 69 2c 2e 67 62 74 6f 20 23 67 62 69 34 69 64 7b 74 6f 70 3a 33 70 78 7d 2e 67 62 69 34 70 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 32 34 70 78 7d 23 67 62 69 34 69 64 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 2d 34 34 70 78 20 2d 31 30 31 70 78 7d 23 67 62 6d 70 69 64 7b 62 61 63 6b Data Ascii: g4a .gbts{padding:29px 5px 1px;*padding:27px 5px 1px}#gbi4i,#gbi4id{left:5px;border:0;height:24px;position:absolute;top:1px;width:24px}.gbto #gbi4i,.gbto #gbi4id{top:3px}.gbi4p{display:block;width:24px}#gbi4id{background-position:-44px -101px}#gbmpid{back
2022-07-26 19:52:11 UTC	10	IN	Data Raw: 72 2c 2e 67 62 6d 6c 31 3a 66 6f 63 75 73 7b 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 75 6e 64 65 72 6c 69 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 70 6d 20 2e 67 62 6d 6c 31 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 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 6c 62 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 67 62 6d 6c 62 2d 68 76 72 2c 2e 67 62 6d 6c 62 3a 66 6f 63 75 73 7b 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 75 6e 64 65 72 6c 69 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 6c 62 77 7b 63 6f 6c Data Ascii: r,.gbml1:focus{outline:none;text-decoration:underline !important}#gbpm .gbml1{display:inline;margin:0;padding:0;white-space:nowrap}.gbmlb,.gbmlb:visited{line-height:27px}.gbmlb-hvr,.gbmlb:focus{outline:none;text-decoration:underline !important}.gbmlbw{col
2022-07-26 19:52:11 UTC	11	IN	Data Raw: 23 67 62 64 34 20 2e 67 62 70 63 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 70 63 20 2e 67 62 70 73 2c 2e 67 62 70 63 20 2e 67 62 70 73 32 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 23 67 62 6d 70 6c 70 2e 67 62 70 73 7b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 70 63 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 2e 67 62 70 63 20 2e 67 62 70 64 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 35 70 78 7d 2e 67 62 70 64 20 2e 67 62 6d 74 2c 2e 67 62 70 64 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 36 36 36 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 20 2e 67 62 6d 74 7b 6f 70 61 63 69 74 79 3a 2e 34 3b 66 69 6c 74 65 72 3a 61 Data Ascii: #gbd4 .gbpc{*display:inline}.gbpc .gbps,.gbpc .gbps2{display:block;margin:0 20px}#gbmplp.gbps{margin:0 10px}.gbpc .gbps{color:#000;font-weight:bold}.gbpc .gbpd{margin-bottom:5px}.gbpd .gbmt,.gbpd .gbps{color:#666 !important}.gbpd .gbmt{opacity:.4;filter:a
2022-07-26 19:52:11 UTC	12	IN	Data Raw: 65 69 67 68 74 3a 61 75 74 6f 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 0a 2e 67 62 71 66 62 2c 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 63 75 72 73 6f 72 3a 64 65 66 61 75 6c 74 20 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 68 65 69 67 68 74 3a 32 39 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 39 70 78 3b 6d 69 6e 2d 77 69 64 74 68 3a 35 34 70 78 3b 2a 6d 69 6e 2d 77 69 64 74 68 3a 37 Data Ascii: eight:auto;margin:10px 0;vertical-align:top}.gbqfb,.gbqfba,.gbqfbb{-moz-border-radius:2px;-webkit-border-radius:2px;border-radius:2px;cursor:default !important;display:inline-block;font-weight:bold;height:29px;line-height:29px;min-width:54px;*min-width:7
2022-07-26 19:52:11 UTC	14	IN	Data Raw: 65 3a 31 31 70 78 7d 2e 67 62 71 66 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 64 39 30 66 65 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 34 64 39 30 66 65 29 2c 74 6f 28 23 34 37 38 37 65 64 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 34 37 38 37 65 64 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 34 37 38 37 65 64 29 3b 62 61 63 6b 67 72 Data Ascii: e:11px}.gbqfb{background-color:#4d90fe;background-image:-webkit-gradient(linear,left top,left bottom,from(#4d90fe),to(#4787ed));background-image:-webkit-linear-gradient(top,#4d90fe,#4787ed);background-image:-moz-linear-gradient(top,#4d90fe,#4787ed);backgr

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	15	IN	Data Raw: 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 35 66 35 66 35 29 2c 74 6f 28 23 66 31 66 31 66 31 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 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 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 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 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 2c 23 66 31 Data Ascii: und-image:-webkit-gradient(linear,left top,left bottom,from(#f5f5f5),to(#f1f1f1));background-image:-webkit-linear-gradient(top,#f5f5f5,#f1f1f1);background-image:-moz-linear-gradient(top,#f5f5f5,#f1f1f1);background-image:-ms-linear-gradient(top,#f5f5f5,#f1
2022-07-26 19:52:11 UTC	16	IN	Data Raw: 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 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 66 66 66 66 66 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 62 66 62 66 62 27 29 7d 2e 67 62 71 66 62 62 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 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 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a Data Ascii: -o-linear-gradient(top,#fff,#fbfbfb);background-image:linear-gradient(top,#fff,#fbfbfb);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#ffffff',EndColorStr='#fbfbfb')}.gbqfbb-hvr,.gbqfbb-hvr:active{background-color:#fff;background-image:
2022-07-26 19:52:11 UTC	17	IN	Data Raw: 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 3b 6c 65 66 74 3a 30 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 30 3b 6f 70 61 63 69 74 79 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 73 62 20 2e 67 62 73 62 3a 61 66 74 65 72 2c 2e 67 62 73 62 20 2e 67 62 73 62 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 22 22 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 30 3b 6c 65 66 Data Ascii: ent(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)));left:0;margin-right:0;opacity:0;position:absolute;width:100%}.gbsb .gbsbt:after,.gbsb .gbsbb:after{content:"";display:block;height:0;lef
2022-07-26 19:52:11 UTC	19	IN	Data Raw: 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 6f 74 74 6f 6d 3a 30 3b 68 65 69 67 68 74 3a 34 70 78 7d 2e 67 62 73 62 20 2e 67 62 73 62 3a 61 66 74 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 65 62 65 62 65 62 3b 62 Data Ascii: nt(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-o-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));bottom:0;height:4px}.gbsb .gbsbb:after{border-bottom:1px solid #ebebeb;b
2022-07-26 19:52:11 UTC	20	IN	Data Raw: 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 6c 73 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 64 61 64 63 65 30 7d 2e 6c 73 74 3a 66 6f 63 75 73 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 7d 3c 2f 73 74 79 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 66 44 46 72 55 61 53 6d 42 76 53 61 58 55 6c 69 51 49 66 61 58 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 2e 65 72 64 3d 7b 6a 73 72 3a 31 2c 62 76 3a 31 36 32 35 2c 64 65 3a 74 72 75 65 7d 3b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 67 2c 68 3d 6e 75 6c 6c 21 3d 28 67 3d 66 2e 6d 65 69 29 3f 67 3a 31 2c 6d 2c 6e 3d 6e 75 6c 6c 21 3d 28 6d 3d 6f 2e 73 64 6f 29 3f 6d 3a 21 30 2c 70 3d 30 2c 71 2c 72 3d 67 6f Data Ascii: ertical-align:top}.lsb:active{background:#dadce0}.lst:focus{outline:none}</style><script nonce="fDFrUaSmBvSaXUliQIfaXg">(function(){window.google.erd={jsr:1,bv:1625,de:true};var f=this||self;var g,h=null!=(g=f.mei)?g:1,m,n=null!=(m=f.sdo)?m:!0,p=0,q,r=go
2022-07-26 19:52:11 UTC	21	IN	Data Raw: 66 69 6c 65 4e 61 6d 65 3d 62 29 2c 67 6f 6f 67 6c 65 2e 6d 6c 28 61 2c 21 31 2c 76 6f 69 64 20 30 2c 21 31 2c 22 53 79 6e 74 61 78 45 72 72 6f 72 22 3d 3d 3d 61 2e 6e 61 6d 65 7c 7c 22 53 79 6e 74 61 78 45 72 72 6f 72 22 3d 3d 3d 61 2e 6d 65 73 73 61 67 65 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 31 29 7c 7c 30 3c 61 2e 6d 65 73 73 61 67 65 2e 69 6e 64 65 78 4f 66 28 22 53 63 72 69 70 74 20 65 72 72 6f 72 22 29 3f 32 3a 30 29 29 3b 71 3d 6e 75 6c 6c 3b 6e 26 26 70 3e 3d 68 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 Data Ascii: fileName=b),google.ml(a,!1,void 0,!1,"SyntaxError"===a.name||"SyntaxError"===a.message.substring(0,11)||0<a.message.indexOf("Script error")?2:0));q=null;n&&p>=h&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX
2022-07-26 19:52:11 UTC	22	IN	Data Raw: 69 6e 64 6f 77 2e 67 62 61 72 2e 6c 6f 67 67 65 72 3b 76 61 72 20 76 3d 7b 7d 2c 6c 61 3d 7b 7d 2c 77 3d 5b 5d 2c 6d 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 31 29 2c 6e 61 3d 68 2e 61 28 22 31 22 2c 21 30 29 2c 6f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 77 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 2c 70 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 5b 61 5d 3d 62 7d 2c 71 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 20 69 6e 20 76 7d 2c 78 3d 7b 7d 2c 41 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 78 5b 61 5d 7c 7c 28 78 5b 61 5d 3d 5b 5d 29 3b 78 5b 61 5d 2e 70 75 73 68 28 62 29 7d 2c 42 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 6d 22 2c 61 29 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 0d 0a Data Ascii: indow.gbar.logger;var v={},la={},w=[],ma=h.b("0.1",.1),na=h.a("1",!0),oa=function(a,b){w.push([a,b])},pa=function(a,b){v[a]=b},qa=function(a){return a in v},x={},A=function(a,b){x[a]||(x[a]=[]);x[a].push(b)},B=function(a){A("m",a)},ra=function(a,b){v
2022-07-26 19:52:11 UTC	23	IN	Data Raw: 65 33 0d 0a 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 63 2e 73 72 63 3d 61 3b 63 2e 61 73 79 6e 63 3d 6e 61 3b 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 3c 6d 61 26 26 28 63 2e 6f 6e 65 72 72 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 63 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 3b 74 28 45 72 72 6f 72 28 22 42 75 6e 64 6c 65 20 6c 6f 61 64 20 66 61 69 6c 65 64 3a 20 6e 61 6d 65 3d 22 2b 28 62 7c 7c 22 55 4e 4b 22 29 2b 22 20 75 72 6c 3d 22 2b 61 29 29 7d 29 3b 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 78 6a 73 63 22 29 7c 7c 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 0d 0a Data Ascii: e3ar c=document.createElement("script");c.src=a;c.async=na;Math.random()<ma&&(c.onerror=function(){c.onerror=null;t(Error("Bundle load failed: name="+(b||"UNK")+" url="+a))});(document.getElementById("xjsc")||document.getElements

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	23	IN	Data Raw: 36 62 33 64 0d 0a 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 7c 7c 0a 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 63 29 7d 2c 44 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 28 63 3d 77 5b 62 5d 29 26 26 63 5b 30 5d 21 3d 61 3b 2b 2b 62 29 3b 21 63 7c 7c 63 5b 31 5d 2e 6c 7c 7c 63 5b 31 5d 2e 73 7c 7c 28 63 5b 31 5d 2e 73 3d 21 30 2c 73 61 28 32 2c 61 29 2c 63 5b 31 5d 2e 75 72 6c 26 26 72 61 28 63 5b 31 5d 2e 75 72 6c 2c 61 29 2c 63 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 63 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 41 28 22 67 63 22 2c 61 29 Data Ascii: 6b3dByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(c)},D=function(a){for(var b=0,c;(c=w[b])&&c[0]!=a;++b);!c||c[1].l||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].url,a),c[1].libs&&C&&C(c[1].libs))},ta=function(a){A("gc",a)
2022-07-26 19:52:11 UTC	24	IN	Data Raw: 2e 64 70 6f 3d 46 28 47 2e 64 70 6f 2c 22 22 29 3b 78 61 7c 7c 77 2e 70 75 73 68 28 5b 22 67 6c 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 6c 6d 5f 65 37 62 62 33 39 61 37 65 31 61 32 34 35 38 31 66 66 34 66 38 64 31 39 39 36 37 38 62 31 62 39 2e 6a 73 22 7d 5d 29 3b 76 61 72 20 45 61 3d 7b 70 75 3a 79 61 2c 73 68 3a 22 22 2c 73 69 3a 7a 61 2c 68 6c 3a 22 64 65 22 7d 3b 76 2e 67 6c 3d 45 61 3b 77 61 3f 41 61 2e 6c 6f 61 64 7c 7c 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3a 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3b 70 28 22 64 67 6c 22 2c 42 61 29 3b 70 28 22 61 67 6c 22 2c 44 61 29 3b 68 2e 6f 3d 78 61 7d 3b 76 61 72 20 46 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 30 30 31 29 2c 47 Data Ascii: .dpo=F(G.dpo,"");xa||w.push(["gl",{url:"//ssl.gstatic.com/gb/js/abc/glm_e7bb39a7e1a24581ff4f8d199678b1b9.js"}]);var Ea={pu:ya,sh:"",si:za,hl:"de"};v.gl=Ea;wa?Aa.load||p("load",Ba,Aa):p("load",Ba,Aa);p("dgl",Ba);p("agl",Da);h.o=xa};var Fa=h.b("0.1",.001),G
2022-07-26 19:52:11 UTC	26	IN	Data Raw: 26 63 2e 6d 61 74 63 68 28 62 29 26 26 28 61 2e 63 6c 61 73 73 4e 61 6d 65 3d 63 2e 72 65 70 6c 61 63 65 28 62 2c 22 22 29 29 7d 2c 48 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 62 22 2b 62 2b 22 5c 5c 62 22 29 3b 61 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 72 65 74 75 72 6e 21 28 21 61 7c 7c 21 61 2e 6d 61 74 63 68 28 62 29 29 7d 2c 4d 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 48 28 61 2c 62 29 3f 4b 28 61 2c 62 29 3a 4a 28 61 2c 62 29 7d 2c 4e 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 7d Data Ascii: &c.match(b)&&(a.className=c.replace(b,""))},H=function(a,b){b=new RegExp("\\b"+b+"\\b");a=a.className;return!(!a||!a.match(b))},Ma=function(a,b){H(a,b)?K(a,b):J(a,b)},Na=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})}}
2022-07-26 19:52:11 UTC	27	IN	Data Raw: 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 3b 4a 28 63 2c 22 67 62 70 64 6a 73 22 29 3b 50 28 29 3b 5a 61 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 3b 69 66 28 62 26 26 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 29 7b 76 61 72 20 64 3d 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 6f 77 6e 73 22 29 3b 69 66 28 64 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 66 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 64 29 3b 69 66 28 66 29 7b 76 61 72 20 6b 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 69 66 28 4f 3d 3d 64 29 4f 3d 76 6f 69 64 20 30 2c 0a 4b 28 6b 2c 22 67 62 74 6f 22 29 Data Ascii: c=document.getElementById("gb");J(c,"gbpdjs");P();Za(document.getElementById("gb"))&&J(c,"gbrtl");if(b&&b.getAttribute){var d=b.getAttribute("aria-owns");if(d.length){var f=document.getElementById(d);if(f){var k=b.parentNode;if(O==d)O=void 0,K(k,"gbto")
2022-07-26 19:52:11 UTC	28	IN	Data Raw: 74 68 29 7b 76 61 72 20 56 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2b 31 5d 3b 48 28 56 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d 68 22 29 7c 7c 66 62 28 56 2c 45 29 7c 7c 28 6c 3d 64 2b 31 29 7d 65 6c 73 65 20 69 66 28 30 3c 3d 64 2d 31 29 7b 76 61 72 20 57 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2d 31 5d 3b 48 28 57 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d 68 22 29 7c 7c 66 62 28 57 2c 45 29 7c 7c 28 6c 3d 64 2b 31 29 7d 62 72 65 61 6b 7d 30 3c 64 26 26 64 2b 31 3c 6e 26 26 64 2b 2b 7d 69 66 28 30 3c 3d 6c 29 7b 76 61 72 20 79 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 79 2e 63 6c 61 73 73 4e 61 Data Ascii: th){var V=k.childNodes[d+1];H(V.firstChild,"gbmh")||fb(V,E)||(l=d+1)}else if(0<=d-1){var W=k.childNodes[d-1];H(W.firstChild,"gbmh")||fb(W,E)||(l=d)}break}0<d&&d+1<n&&d++}if(0<=l){var y=document.createElement("li"),z=document.createElement("div");y.classNa
2022-07-26 19:52:11 UTC	29	IN	Data Raw: 74 74 65 20 76 65 72 73 75 63 68 65 20 65 73 20 73 70 e4 74 65 72 20 6e 6f 63 68 20 65 69 6e 6d 61 6c 2e 22 2c 22 25 31 24 73 22 29 2c 51 28 62 2c 21 30 29 29 7d 63 61 74 63 68 28 63 29 7b 72 28 63 2c 22 73 62 22 2c 22 73 64 68 65 22 29 7d 7d 2c 72 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 26 26 62 29 7b 76 61 72 20 64 3d 24 61 28 61 29 3b 69 66 28 64 29 7b 69 66 28 63 29 7b 64 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 22 22 3b 62 3d 62 2e 73 70 6c 69 74 28 63 29 3b 63 3d 30 3b 66 6f 72 28 76 61 72 20 66 3b 66 3d 62 5b 63 5d 3b 63 2b 2b 29 7b 76 61 72 20 6b 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 0a 6b 2e 69 6e 6e 65 72 48 54 4d 4c 3d 66 3b 64 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 Data Ascii: tte versuche es spter noch einmal.","%1$s"),Q(b,!0))}catch(c){r(c,"sb","sdhe")}},rb=function(a,b,c){if(a&&b){var d=$a(a);if(d){if(c){d.textContent="";b=b.split(c);c=0;for(var f;f=b[c];c++){var k=document.createElement("div");k.innerHTML=f;d.appendChild(
2022-07-26 19:52:11 UTC	31	IN	Data Raw: 2e 63 28 22 35 30 30 30 22 2c 30 29 2c 74 65 74 3a 68 2e 62 28 22 30 2e 35 22 2c 30 29 7d 3b 76 2e 77 6d 3d 7a 62 3b 69 66 28 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 41 62 3d 68 2e 61 28 22 22 29 3b 77 2e 70 75 73 68 28 5b 22 67 63 22 2c 7b 61 75 74 6f 3a 41 62 2c 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 6c 69 62 73 3a 22 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6c 69 65 6e 74 3a 67 61 70 69 2e 69 66 72 61 6d 65 73 22 7d 5d 29 3b 76 61 72 20 42 62 3d 7b 76 65 72 73 69 6f 6e 3a 22 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 Data Ascii: .c("5000",0),tet:h.b("0.5",0)};v.wm=zb;if(h.a("1")){var Ab=h.a("");w.push(["gc",{auto:Ab,url:"//ssl.gstatic.com/gb/js/abc/gci_91f30755d6a6b787dcc2a4062e6e9824.js",libs:"googleapis.client:gapi.iframes"}]);var Bb={version:"gci_91f30755d6a6b787dcc2a4062e6e98
2022-07-26 19:52:11 UTC	32	IN	Data Raw: 69 66 28 21 52 29 7b 52 3d 7b 7d 3b 66 6f 72 28 76 61 72 20 6b 3d 30 3b 6b 3c 4b 62 2e 6c 65 6e 67 74 68 3b 6b 2b 2b 29 7b 76 61 72 20 6d 3d 4b 62 5b 6b 5d 3b 52 5b 6d 5d 3d 21 30 7d 7d 69 66 28 66 3d 21 21 52 5b 66 5d 29 63 3d 4d 62 2c 64 3d 4f 62 3b 69 66 28 64 29 7b 64 3d 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 3b 69 66 28 67 2e 72 70 29 7b 76 61 72 20 6e 3d 67 2e 72 70 28 29 3b 6e 3d 22 2d 31 22 21 3d 6e 3f 6e 3a 22 22 7d 65 6c 73 65 20 6e 3d 22 22 3b 66 3d 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 6b 3d 64 28 22 28 38 38 33 34 22 29 3b 6d 3d 64 28 22 36 30 58 67 59 74 44 51 44 36 6d 38 78 63 38 50 32 59 6d 57 75 41 4d 22 29 3b 76 61 72 20 6c 3d 67 2e 62 76 2e 66 2c 71 3d 64 28 22 31 22 29 3b 6e 3d 64 28 6e 29 3b 63 Data Ascii: if(!R){R={};for(var k=0;k<Kb.length;k++){var m=Kb[k];R[m]=!0}}if(f=!!R[f])c=Mb,d=Ob;if(d){d=encodeURIComponent;if(g.rp){var n=g.rp();n="-1"!=n?n:""}else n="";f=(new Date).getTime();k=d("28834");m=d("60XgYtDQD6m8xc8P2YmWuAM");var l=g.bv.f,q=d("1");n=d(n);c

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	33	IN	Data Raw: 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 2c 22 32 37 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 5a 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 28 61 3d 59 62 5b 61 5d 29 7c 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 0a 24 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 64 28 29 7d 29 7d 3b 70 28 22 73 70 6e 22 2c 56 62 29 3b 70 28 22 73 70 70 22 2c 58 62 29 3b 70 28 22 73 70 73 22 2c 57 62 29 3b 70 28 22 73 70 64 22 2c Data Ascii: /default-user=s24","27":"https://lh3.googleusercontent.com/ogw/default-user=s24"},Zb=function(a){return(a=Yb[a])||"https://lh3.googleusercontent.com/ogw/default-user=s24"},$b=function(){B(function(){g.spd()})};p("spn",Vb);p("spp",Xb);p("sps",Wb);p("spd",
2022-07-26 19:52:11 UTC	34	IN	Data Raw: 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 65 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 59 28 5b 32 5d 2c 22 73 73 70 22 29 29 7b 76 61 72 20 62 3d 21 62 63 5b 61 5d 3b 54 26 26 28 62 3d 62 26 26 21 21 54 5b 61 5d 29 3b 72 65 74 75 72 6e 20 62 7d 7d 3b 63 63 3d 21 31 3b 53 3d 7b 7d 3b 62 63 3d 7b 7d 3b 54 3d 6e 75 6c 6c 3b 58 3d 31 3b 0a 76 61 72 20 6a 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 21 31 3b 74 72 79 7b 62 3d 61 2e 63 6f 6f 6b 69 65 26 26 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 22 50 52 45 46 22 29 7d 63 61 74 63 68 28 63 29 7b 7d 72 65 74 75 72 6e 21 62 7d 2c 6b 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 72 65 74 75 Data Ascii: r(d,"up","tp")}}}catch(d){r(d,"up","mtp")}},ec=function(a){if(Y([2],"ssp")){var b=!bc[a];T&&(b=b&&!!T[a]);return b}};cc=!1;S={};bc={};T=null;X=1;var jc=function(a){var b=!1;try{b=a.cookie&&a.cookie.match("PREF")}catch(c){}return !b},kc=function(){try{retu
2022-07-26 19:52:11 UTC	36	IN	Data Raw: 61 70 3a 67 63 2c 61 6f 70 3a 68 63 2c 74 70 3a 69 63 2c 73 73 70 3a 65 63 2c 73 70 64 3a 6d 63 2c 67 70 64 3a 6e 63 2c 61 65 68 3a 6f 63 2c 61 61 6c 3a 70 63 2c 67 63 63 3a 71 63 7d 29 3b 76 61 72 20 5a 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 7d 3b 5a 28 67 2e 75 70 2c 22 73 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 73 69 22 29 3b 5a 28 67 2e 75 70 2c 22 73 70 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 64 70 63 22 29 3b 5a 28 67 2e 75 70 2c 22 69 69 63 22 29 3b 67 2e 6d 63 66 28 22 75 70 22 2c 7b 73 70 3a 68 2e 62 28 22 30 2e 30 31 22 2c 31 29 2c 74 6c 64 Data Ascii: ap:gc,aop:hc,tp:ic,ssp:ec,spd:mc,gpd:nc,aeh:oc,aal:pc,gcc:qc});var Z=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})}};Z(g.up,"sl");Z(g.up,"si");Z(g.up,"spl");Z(g.up,"dpc");Z(g.up,"iic");g.mcf("up",{sp:h.b("0.01",1),tld
2022-07-26 19:52:11 UTC	37	IN	Data Raw: 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 61 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 61 2e 6d 63 66 28 22 6d 6d 22 2c 7b 73 3a 22 31 22 7d 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 Data Ascii: right The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var a=window.gbar;a.mcf("mm",{s:"1"});}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Library Authors. S
2022-07-26 19:52:11 UTC	38	IN	Data Raw: 2c 65 73 72 3a 65 28 22 30 2e 31 22 29 2c 65 76 74 73 3a 5b 22 6d 6f 75 73 65 64 6f 77 6e 22 2c 22 74 6f 75 63 68 73 74 61 72 74 22 2c 22 74 6f 75 63 68 6d 6f 76 65 22 2c 22 77 68 65 65 6c 22 2c 22 6b 65 79 64 6f 77 6e 22 5d 2c 67 62 6c 3a 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 32 30 36 30 37 2e 31 5f 70 30 22 2c 68 64 3a 22 63 6f 6d 22 2c 68 6c 3a 22 64 65 22 2c 69 72 70 3a 64 28 22 22 29 2c 70 69 64 3a 65 28 22 31 22 29 2c 0a 73 6e 69 64 3a 65 28 22 32 38 38 33 34 22 29 2c 74 6f 3a 65 28 22 33 30 30 30 30 30 22 29 2c 75 3a 65 28 22 22 29 2c 76 66 3a 22 2e 36 36 2e 22 7d 2c 67 3d 66 2c 68 3d 5b 22 62 6e 64 63 66 67 22 5d 2c 6b 3d 61 3b 68 5b 30 5d 69 6e 20 6b 7c 7c 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6b 2e 65 78 65 Data Ascii: ,esr:e("0.1"),evts:["mousedown","touchstart","touchmove","wheel","keydown"],gbl:"es_plusone_gc_20220607.1_p0",hd:"com",hl:"de",irp:d(""),pid:e("1"),snid:e("28834"),to:e("300000"),u:e(""),vf:".66."},g=f,h=["bndcfg"],k=a;h[0]in k||"undefined"==typeof k.exe
2022-07-26 19:52:11 UTC	40	IN	Data Raw: 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 53 75 63 68 65 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 32 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 64 65 2f 69 6d 67 68 70 3f 68 6c 3d 64 65 26 74 61 62 3d 77 69 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 42 69 6c 64 65 72 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 70 73 2e 67 6f 6f 67 6c 65 Data Ascii: >Suche <li class=gbt>Bilder <li class=gbt><a class=gbzt id=gb_8 href="https://maps.google
2022-07-26 19:52:11 UTC	41	IN	Data Raw: 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 66 44 46 72 55 61 53 6d 42 76 53 61 58 55 6c 69 51 49 66 61 58 67 27 3e 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 67 62 7a 74 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 74 67 28 65 76 65 6e 74 2c 74 68 69 73 29 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 20 69 64 3d 67 62 64 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 7a 74 6d 3e 3c 64 69 76 20 69 64 3d 67 62 6d 6d 62 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 20 67 62 73 62 69 73 22 3e 3c 6f 6c 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 Data Ascii: /a><script nonce='fDFrUaSmBvSaXUliQIfaXg'>document.getElementById('gbztm').addEventListener('click', function clickHandler() { gbar.tg(event,this); });</script> <ol id=gbmm class
2022-07-26 19:52:11 UTC	42	IN	Data Raw: 74 6c 2f 64 65 2f 61 62 6f 75 74 2f 70 72 6f 64 75 63 74 73 3f 74 61 62 3d 77 68 22 20 63 6c 61 73 73 3d 67 62 6d 74 3e 4e 6f 63 68 20 6d 65 68 72 20 26 72 61 71 75 6f 3b 3c 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 66 44 46 72 55 61 53 6d 42 76 53 61 58 55 6c 69 51 49 66 61 58 67 27 3e 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 27 6c 69 20 3e 20 61 2e 67 62 6d 74 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 31 2c 7b 74 3a 36 36 7d 29 3b 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 73 62 74 Data Ascii: tl/de/about/products?tab=wh" class=gbmt>Noch mehr »<script nonce='fDFrUaSmBvSaXUliQIfaXg'>document.querySelector('li > a.gbmt').addEventListener('click', function clickHandler() { gbar.logger.il(1,{t:66});; });</script> <div class=gbsbt

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:11 UTC	43	IN	Data Raw: 20 63 6c 61 73 73 3d 22 67 62 6d 74 20 67 62 6d 68 22 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 70 20 67 62 6d 74 63 22 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 67 6c 65 2e 64 65 2f 68 69 73 74 6f 72 79 2f 6f 70 74 6f 75 74 3f 68 6c 3d 64 65 22 3e 57 65 62 70 72 6f 74 6f 6b 6f 6c 6c 3c 2f 61 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 33 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 34 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 66 44 46 72 55 61 53 6d 42 76 53 61 58 55 6c 69 51 49 66 61 58 67 27 3e 77 69 Data Ascii: class="gbmt gbmh"> <li class="gbkp gbmtc">Webprotokoll <script nonce='fDFrUaSmBvSaXUliQIfaXg'>wi
2022-07-26 19:52:11 UTC	45	IN	Data Raw: 72 3a 23 30 30 30 22 20 61 75 74 6f 63 6f 6d 70 6c 65 74 65 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 75 63 68 65 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 75 63 68 65 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 Data Ascii: r:#000" autocomplete="off" value="" title="Google Suche" maxlength="2048" name="q" size="57"> <br style="line-height:0"><input class="lsb" value="Google Suche" name="btnG" type="submit"><span class="d
2022-07-26 19:52:11 UTC	46	IN	Data Raw: 22 29 29 7b 76 61 72 20 66 3d 67 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 73 70 61 6e 20 69 64 3d 22 66 6f 6f 74 65 72 22 3e 3c 64 69 76 Data Ascii: "))}var f=google.gbvu,g=document.getElementById("gbv");g&&(g.value=a);f&&window.setTimeout(function(){location.href=f},0)};}).call(this);</script></form> <div
2022-07-26 19:52:11 UTC	47	IN	Data Raw: 6f 67 6c 65 2e 78 6a 73 3d 7b 63 6b 3a 27 78 6a 73 2e 68 70 2e 77 6d 41 44 68 50 41 49 6c 69 77 2e 4c 2e 58 2e 4f 27 2c 63 73 3a 27 41 43 54 39 30 6f 46 6c 78 67 62 76 56 42 4b 69 51 78 70 54 6d 4a 73 47 4d 49 70 6e 77 79 38 59 65 41 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 66 44 46 72 55 61 53 6d 42 76 53 61 58 55 6c 69 51 49 66 61 58 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 45 64 2d 6e 4d 73 6a 61 37 64 63 2e 4f 2f 61 6d 5c 78 33 64 41 4d 41 54 41 49 41 45 41 45 67 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 45 71 59 63 78 37 44 65 Data Ascii: ogle.xjs={ck:'xjs.hp.wmADhPAIliw.L.X.O',cs:'ACT90oFlxgbvVBKiQxpTmJsGMIpnwy8YeA',excm:[]};})();</script> <script nonce="fDFrUaSmBvSaXUliQIfaXg">(function(){var u='/xjs/_/js/k\x3dxjs.hp.en.Ed-nMsja7dc.O/am\x3dAMATAIAEAEg/d\x3d1/ed\x3d1/rs\x3dACT90oEqYcx7De
2022-07-26 19:52:11 UTC	48	IN	Data Raw: 2e 70 73 61 3d 21 30 7d 3b 67 6f 6f 67 6c 65 2e 78 6a 73 75 3d 75 3b 73 65 74 54 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 61 74 74 6e 3a 66 61 6c 73 65 2c 62 6c 74 3a 27 6e 6f 6e 65 27 2c 63 68 6e 6b 3a 30 2c 64 77 3a 66 61 6c 73 65 2c 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 Data Ascii: .psa=!0};google.xjsu=u;setTimeout(function(){n()},0);})();function _DumpException(e){throw e;}function _F_installCss(c){}(function(){google.jl={attn:false,blt:'none',chnk:0,dw:false,dwu:true,emtn:0,end:0,ine:false,injs:'none',injt:0,injth:0,injv2:false,
2022-07-26 19:52:11 UTC	50	IN	Data Raw: 32 32 3a 66 61 6c 73 65 7d 7d 27 3b 67 6f 6f 67 6c 65 2e 70 6d 63 3d 4a 53 4f 4e 2e 70 61 72 73 65 28 70 6d 63 29 3b 7d 29 28 29 3b 3c 2f 73 63 72 69 70 74 3e 20 20 20 20 20 20 20 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 22:false}}';google.pmc=JSON.parse(pmc);})();</script> </body></html>
2022-07-26 19:52:11 UTC	50	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	49765	142.250.185.228	443	C:\Users\user\Desktop\D6GEVBNNH11111.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	50	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	50	IN	HTTP/1.1 200 OK Date: Tue, 26 Jul 2022 19:52:29 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=AakniGPQGNTOXTn2U_dfUdlkgNz27QLxm6ype6mzSutvzm-aw4GaD4KAIBQ; expires=Sun, 22-Jan-2023 19:52:29 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=6.SE=Gy_CFQfOKbc429rgImfYMiXgU-UJSjnZkhfkkxv_JDQ2UipYvpCD4N1jxm0LeZ9gMs8R_j3Lh0Yhk2hwGFooETRGiucrCiziTm9DJtJEL6poy_Y9pyPu3HSOoNBtTJ5mX2e6N1PdWWWAfOE1OQ4ocHY7jB4SvY9Tl7nkYrLxRHo; expires=Sat, 26-Aug-2023 12:10:47 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+716; expires=Thu, 25-Jul-2024 19:52:29 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
2022-07-26 19:52:29 UTC	51	IN	Data Raw: 35 38 62 33 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 64 65 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e Data Ascii: 58b3<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="de"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta conten
2022-07-26 19:52:29 UTC	51	IN	Data Raw: 74 3d 22 2f 6c 6f 67 6f 73 2f 64 6f 6f 64 6c 65 73 2f 32 30 32 32 2f 63 65 6c 65 62 72 61 74 69 6e 67 2d 73 74 65 65 6c 70 61 6e 2d 36 37 35 33 36 35 31 38 33 37 31 30 38 34 36 37 2e 34 2d 6c 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 69 72 20 66 65 69 65 72 6e 20 64 69 65 20 53 74 65 65 6c 20 50 61 6e 22 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 74 69 74 6c 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 57 69 72 20 66 65 69 65 72 6e 20 64 69 65 20 53 74 65 65 6c 20 50 61 6e 21 20 23 47 6f 6f 67 6c 65 44 6f 6f 64 6c 65 22 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 Data Ascii: t="/logos/doodles/2022/celebrating-steelpan-6753651837108467.4-l.png" itemprop="image"><meta content="Wir feiern die Steel Pan" property="twitter:title"><meta content="Wir feiern die Steel Pan! #GoogleDoodle" property="twitter:description"><meta content="
2022-07-26 19:52:29 UTC	52	IN	Data Raw: 30 31 2c 33 35 31 34 2c 36 30 36 2c 32 30 32 33 2c 31 37 37 37 2c 35 32 30 2c 36 33 34 34 2c 38 33 32 36 2c 33 32 32 37 2c 32 38 34 35 2c 37 2c 35 35 39 39 2c 32 38 31 37 31 2c 31 38 35 31 2c 36 33 39 38 2c 39 33 35 38 2c 31 2c 32 2c 33 34 36 2c 32 33 30 2c 36 31 38 32 2c 32 37 37 2c 31 34 39 2c 31 33 39 37 35 2c 34 2c 31 35 32 38 2c 32 33 30 34 2c 37 30 33 39 2c 32 30 33 30 39 2c 34 37 36 34 2c 32 36 35 38 2c 37 33 35 36 2c 31 33 36 35 39 2c 34 34 33 37 2c 31 36 37 38 36 2c 35 38 32 31 2c 32 35 33 36 2c 34 30 39 32 2c 32 2c 34 30 35 32 2c 33 2c 33 35 34 31 2c 31 2c 34 32 31 35 34 2c 32 2c 31 34 30 32 32 2c 31 34 31 31 36 2c 31 31 36 32 33 2c 35 36 37 39 2c 31 30 32 31 2c 32 33 37 39 2c 32 30 39 36 32 2c 32 2c 31 2c 39 2c 37 37 36 38 2c 34 35 36 39 2c 36 Data Ascii: 01,3514,606,2023,1777,520,6344,8326,3227,2845,7,5599,28171,1851,6398,9358,1,2,346,230,6182,277,149,13975,4,1528,2304,7039,20309,4764,2658,7356,13659,4437,16786,5821,2536,4092,2,4052,3,3541,1,42154,2,14022,14116,11623,5679,1021,2379,20962,2,1,9,7768,4569,6
2022-07-26 19:52:29 UTC	54	IN	Data Raw: 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 63 73 68 69 64 3d 22 29 26 26 22 73 6c 68 22 21 3d 3d 61 26 26 28 64 3d 22 26 63 73 68 69 64 3d 22 2b 66 2e 5f 63 73 68 69 64 29 3b 63 3d 63 7c 7c 22 2f 22 2b 28 67 7c 7c 22 67 65 6e 5f 32 30 34 22 29 2b 22 3f 61 74 79 70 3d 69 26 63 74 3d 22 2b 61 2b 22 26 63 61 64 3d 22 2b 62 2b 65 2b 22 26 7a 78 3d 22 2b 44 61 74 65 2e 6e 6f 77 28 29 2b 64 3b 2f 5e 68 74 74 70 3a 2f 69 2e 74 65 73 74 28 63 29 26 26 22 68 74 74 70 73 3a 22 3d 3d 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 26 26 28 67 6f 6f 67 6c 65 2e 6d 6c 26 26 67 6f 6f 67 6c 65 2e 6d 6c 28 45 72 72 6f 72 28 22 61 22 29 2c 21 31 2c 7b 73 72 63 3a 63 2c 67 6c 6d 6d 3a 31 7d 29 2c 63 3d 22 22 29 3b 72 65 74 75 72 6e 20 63 7d 3b 68 3d Data Ascii: ==b.search("&cshid=")&&"slh"!==a&&(d="&cshid="+f._cshid);c=c||"/"+(g||"gen_204")+"?atyp=i&ct="+a+"&cad="+b+e+"&zx="+Date.now()+d;/^http:/i.test(c)&&"https:"===window.location.protocol&&(google.ml&&google.ml(Error("a"),!1,{src:c,glmm:1}),c="");return c};h=
2022-07-26 19:52:29 UTC	55	IN	Data Raw: 6c 65 6d 65 6e 74 3b 61 3d 61 2e 70 61 72 65 6e 74 45 6c 65 6d 65 6e 74 29 69 66 28 22 41 22 3d 3d 3d 61 2e 74 61 67 4e 61 6d 65 29 7b 61 3d 22 31 22 3d 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 6e 6f 68 72 65 66 22 29 3b 62 72 65 61 6b 20 61 7d 61 3d 21 31 7d 61 26 26 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 7d 2c 21 30 29 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 73 74 79 6c 65 3e 23 67 62 7b 66 6f 6e 74 3a 31 33 70 78 2f 32 37 70 78 20 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 23 67 62 7a 2c 23 67 62 67 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 3b 74 6f 70 3a 30 3b 68 Data Ascii: lement;a=a.parentElement)if("A"===a.tagName){a="1"===a.getAttribute("data-nohref");break a}a=!1}a&&b.preventDefault()},!0);}).call(this);</script><style>#gb{font:13px/27px Arial,sans-serif;height:30px}#gbz,#gbg{position:absolute;white-space:nowrap;top:0;h
2022-07-26 19:52:29 UTC	56	IN	Data Raw: 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 74 6f 20 2e 67 62 6d 2c 2e 67 62 74 6f 20 23 67 62 73 7b 74 6f 70 3a 32 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 76 69 73 69 62 6c 65 7d 23 67 62 7a 20 2e 67 62 6d 7b 6c 65 66 74 3a 30 7d 23 67 62 67 20 2e 67 62 6d 7b 72 69 67 68 74 3a 30 7d 2e 67 62 78 6d 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 63 63 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 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 31 3b 74 6f 70 3a 2d 31 70 78 3b 6c 65 66 74 3a 2d 32 70 78 3b 72 69 67 68 74 3a 2d 32 70 78 3b 62 6f 74 74 6f 6d 3a 2d 32 70 78 3b 6f 70 61 63 69 74 79 3a 2e 34 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 3b 66 Data Ascii: px 1px rgba(0,0,0,.2)}.gbto .gbm,.gbto #gbs{top:29px;visibility:visible}#gbz .gbm{left:0}#gbg .gbm{right:0}.gbxms{background-color:#ccc;display:block;position:absolute;z-index:1;top:-1px;left:-2px;right:-2px;bottom:-2px;opacity:.4;-moz-border-radius:3px;f

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	57	IN	Data Raw: 62 74 73 7b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 31 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 31 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 3a 30 20 35 70 78 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 30 30 30 7d 2e 67 62 74 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 7a 74 20 2e 67 62 74 73 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 6f 20 2e 67 62 74 73 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 62 65 62 Data Ascii: bts{border-left:1px solid transparent;border-right:1px solid transparent;display:block;*display:inline-block;padding:0 5px;position:relative;z-index:1000}.gbts{*display:inline}.gbzt .gbts{display:inline;zoom:1}.gbto .gbts{background:#fff;border-color:#beb
2022-07-26 19:52:29 UTC	59	IN	Data Raw: 32 39 70 78 20 35 70 78 20 31 70 78 3b 2a 70 61 64 64 69 6e 67 3a 32 37 70 78 20 35 70 78 20 31 70 78 7d 23 67 62 69 34 69 2c 23 67 62 69 34 69 64 7b 6c 65 66 74 3a 35 70 78 3b 62 6f 72 64 65 72 3a 30 3b 68 65 69 67 68 74 3a 32 34 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 31 70 78 3b 77 69 64 74 68 3a 32 34 70 78 7d 2e 67 62 74 6f 20 23 67 62 69 34 69 2c 2e 67 62 74 6f 20 23 67 62 69 34 69 64 7b 74 6f 70 3a 33 70 78 7d 2e 67 62 69 34 70 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 32 34 70 78 7d 23 67 62 69 34 69 64 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 2d 34 34 70 78 20 2d 31 30 31 70 78 7d 23 67 62 6d 70 69 64 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 Data Ascii: 29px 5px 1px;*padding:27px 5px 1px}#gbi4i,#gbi4id{left:5px;border:0;height:24px;position:absolute;top:1px;width:24px}.gbto #gbi4i,.gbto #gbi4id{top:3px}.gbi4p{display:block;width:24px}#gbi4id{background-position:-44px -101px}#gbmpid{background-position:0
2022-07-26 19:52:29 UTC	60	IN	Data Raw: 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 75 6e 64 65 72 6c 69 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 70 6d 20 2e 67 62 6d 6c 31 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 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 6c 62 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 67 62 6d 6c 62 2d 68 76 72 2c 2e 67 62 6d 6c 62 3a 66 6f 63 75 73 7b 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 75 6e 64 65 72 6c 69 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 6c 62 77 7b 63 6f 6c 6f 72 3a 23 63 63 63 3b 6d 61 72 67 69 6e 3a 30 20 31 Data Ascii: line:none;text-decoration:underline !important}#gbpm .gbml1{display:inline;margin:0;padding:0;white-space:nowrap}.gbmlb,.gbmlb:visited{line-height:27px}.gbmlb-hvr,.gbmlb:focus{outline:none;text-decoration:underline !important}.gbmlbw{color:#ccc;margin:0 1
2022-07-26 19:52:29 UTC	61	IN	Data Raw: 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 70 63 20 2e 67 62 70 73 2c 2e 67 62 70 63 20 2e 67 62 70 73 32 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 23 67 62 6d 70 6c 70 2e 67 62 70 73 7b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 70 63 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 2e 67 62 70 63 20 2e 67 62 70 64 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 35 70 78 7d 2e 67 62 70 64 20 2e 67 62 6d 74 2c 2e 67 62 70 64 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 36 36 36 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 20 2e 67 62 6d 74 7b 6f 70 61 63 69 74 79 3a 2e 34 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 34 30 29 7d 2e Data Ascii: ay:inline}.gbpc .gbps,.gbpc .gbps2{display:block;margin:0 20px}#gbmplp.gbps{margin:0 10px}.gbpc .gbps{color:#000;font-weight:bold}.gbpc .gbpd{margin-bottom:5px}.gbpd .gbmt,.gbpd .gbps{color:#666 !important}.gbpd .gbmt{opacity:.4;filter:alpha(opacity=40)}.
2022-07-26 19:52:29 UTC	63	IN	Data Raw: 31 30 70 78 20 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 0a 2e 67 62 71 66 62 2c 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 32 70 78 3b 63 75 72 73 6f 72 3a 64 65 66 61 75 6c 74 20 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 68 65 69 67 68 74 3a 32 39 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 39 70 78 3b 6d 69 6e 2d 77 69 64 74 68 3a 35 34 70 78 3b 2a 6d 69 6e 2d 77 69 64 74 68 3a 37 30 70 78 3b 70 61 64 64 69 6e 67 3a 30 20 38 70 78 3b Data Ascii: 10px 0;vertical-align:top}.gbqfb,.gbqfba,.gbqfbb{-moz-border-radius:2px;-webkit-border-radius:2px;border-radius:2px;cursor:default !important;display:inline-block;font-weight:bold;height:29px;line-height:29px;min-width:54px;*min-width:70px;padding:0 8px;
2022-07-26 19:52:29 UTC	64	IN	Data Raw: 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 64 39 30 66 65 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 34 64 39 30 66 65 29 2c 74 6f 28 23 34 37 38 37 65 64 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 34 37 38 37 65 64 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 34 37 38 37 65 64 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 34 37 38 37 65 64 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 Data Ascii: ground-color:#4d90fe;background-image:-webkit-gradient(linear,left top,left bottom,from(#4d90fe),to(#4787ed));background-image:-webkit-linear-gradient(top,#4d90fe,#4787ed);background-image:-moz-linear-gradient(top,#4d90fe,#4787ed);background-image:-ms-lin
2022-07-26 19:52:29 UTC	65	IN	Data Raw: 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 35 66 35 29 2c 74 6f 28 23 66 31 66 31 66 31 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 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 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 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 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 35 66 35 66 35 2c 23 66 31 66 31 66 31 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 Data Ascii: gradient(linear,left top,left bottom,from(#f5f5f5),to(#f1f1f1));background-image:-webkit-linear-gradient(top,#f5f5f5,#f1f1f1);background-image:-moz-linear-gradient(top,#f5f5f5,#f1f1f1);background-image:-ms-linear-gradient(top,#f5f5f5,#f1f1f1);background-i
2022-07-26 19:52:29 UTC	66	IN	Data Raw: 28 74 6f 70 2c 23 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 66 2c 23 66 62 66 62 66 62 29 3b 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 66 66 66 66 66 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 62 66 62 66 62 27 29 7d 2e 67 62 71 66 62 62 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 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 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 Data Ascii: (top,#fff,#fbfbfb);background-image:linear-gradient(top,#fff,#fbfbfb);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#ffffff',EndColorStr='#fbfbfb')}.gbqfbb-hvr,.gbqfbb-hvr:active{background-color:#fff;background-image:-webkit-gradient(l

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	68	IN	Data Raw: 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 3b 6c 65 66 74 3a 30 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 30 3b 6f 70 61 63 69 74 79 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 73 62 20 2e 67 62 73 62 74 3a 61 66 74 65 72 2c 2e 67 62 73 62 20 2e 67 62 73 62 62 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 22 22 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 30 3b 6c 65 66 74 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c Data Ascii: p,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)));left:0;margin-right:0;opacity:0;position:absolute;width:100%}.gbsb .gbsbt:after,.gbsb .gbsbb:after{content:"";display:block;height:0;left:0;position:absol
2022-07-26 19:52:29 UTC	69	IN	Data Raw: 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 6f 74 74 6f 6d 3a 30 3b 68 65 69 67 68 74 3a 34 70 78 7d 2e 67 62 73 62 20 2e 67 62 73 62 62 3a 61 66 74 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 65 62 65 62 65 62 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 Data Ascii: ,0,.2),rgba(0,0,0,0));background-image:-o-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));bottom:0;height:4px}.gbsb .gbsbb:after{border-bottom:1px solid #ebebeb;border-color:rgba(0
2022-07-26 19:52:29 UTC	70	IN	Data Raw: 2e 6c 73 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 64 61 64 63 65 30 7d 2e 6c 73 74 3a 66 6f 63 75 73 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 7d 3c 2f 73 74 79 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 6c 41 56 42 49 34 71 6e 50 67 54 6a 6e 5a 41 7a 32 31 79 4d 65 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 2e 65 72 64 3d 7b 6a 73 72 3a 31 2c 62 76 3a 31 36 32 35 2c 64 65 3a 74 72 75 65 7d 3b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 67 2c 68 3d 6e 75 6c 6c 21 3d 28 67 3d 66 2e 6d 65 69 29 3f 67 3a 31 2c 6d 2c 6e 3d 6e 75 6c 6c 21 3d 28 6d 3d 66 2e 73 64 6f 29 3f 6d 3a 21 30 2c 70 3d 30 2c 71 2c 72 3d 67 6f 6f 67 6c 65 2e 65 72 64 2c 75 3d 72 2e 6a 73 72 3b 67 Data Ascii: .lsb:active{background:#dadce0}.lst:focus{outline:none}</style><script nonce="lAVBI4qnPgTjnZAz21yMeg">(function(){window.google.erd={jsr:1,bv:1625,de:true};var f=this||self;var g,h=null!=(g=f.mei)?g:1,m,n=null!=(m=f.sdo)?m:!0,p=0,q,r=google.erd,u=r.jsr;g
2022-07-26 19:52:29 UTC	71	IN	Data Raw: 2e 6d 6c 28 61 2c 21 31 2c 76 6f 69 64 20 30 2c 21 31 2c 22 53 79 6e 74 61 78 45 72 72 6f 72 22 3d 3d 3d 61 2e 6e 61 6d 65 7c 7c 22 53 79 6e 74 61 78 45 72 72 6f 72 22 3d 3d 3d 61 2e 6d 65 73 73 61 67 65 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 31 29 7c 7c 30 3c 61 2e 6d 65 73 73 61 67 65 2e 69 6e 64 65 78 4f 66 28 22 53 63 72 69 70 74 20 65 72 72 6f 72 22 29 3f 32 3a 30 29 29 3b 71 3d 6e 75 6c 6c 3b 6e 26 26 70 3e 3d 68 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 Data Ascii: .ml(a,!1,void 0,!1,"SyntaxError"===a.name||"SyntaxError"===a.message.substring(0,11)||0<a.message.indexOf("Script error")?2:0));q=null;n&&p>=h&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifie
2022-07-26 19:52:29 UTC	73	IN	Data Raw: 76 61 72 20 76 3d 7b 7d 2c 6c 61 3d 7b 7d 2c 77 3d 5b 5d 2c 6d 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 31 29 2c 6e 61 3d 68 2e 61 28 22 31 22 2c 21 30 29 2c 6f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 77 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 2c 70 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 5b 61 5d 3d 62 7d 2c 71 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 20 69 6e 20 76 7d 2c 78 3d 7b 7d 2c 41 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 78 5b 61 5d 3d 62 7d 2c 42 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 6d 22 2c 61 29 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 Data Ascii: var v={},la={},w=[],ma=h.b("0.1",.1),na=h.a("1",!0),oa=function(a,b){w.push([a,b])},pa=function(a,b){v[a]=b},qa=function(a){return a in v},x={},A=function(a,b){x[a]||(x[a]=[]);x[a].push(b)},B=function(a){A("m",a)},ra=function(a,b){var c=document.createEle
2022-07-26 19:52:29 UTC	73	IN	Data Raw: 64 65 0d 0a 6e 61 6d 65 3d 22 2b 28 62 7c 7c 22 55 4e 4b 22 29 2b 22 20 75 72 6c 3d 22 2b 61 29 29 7d 29 3b 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 78 6a 73 63 22 29 7c 7c 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 7c 7c 0a 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 63 29 7d 2c 44 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 28 63 3d 77 5b 62 5d 29 26 26 63 5b 30 5d 21 3d 61 3b 2b 2b 62 29 3b 21 63 7c 7c 0d 0a Data Ascii: dename="+(b||"UNK")+" url="+a))});(document.getElementById("xjsc")||document.getElementsByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(c)},D=function(a){for(var b=0,c;(c=w[b])&&c[0]!=a;++b);!c||
2022-07-26 19:52:29 UTC	73	IN	Data Raw: 36 61 61 63 0d 0a 63 5b 31 5d 2e 6c 7c 7c 63 5b 31 5d 2e 73 7c 7c 28 63 5b 31 5d 2e 73 3d 21 30 2c 73 61 28 32 2c 61 29 2c 63 5b 31 5d 2e 75 72 6c 26 26 72 61 28 63 5b 31 5d 2e 75 72 6c 2c 61 29 2c 63 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 63 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 41 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 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 63 22 2c 76 29 3b 70 28 22 Data Ascii: 6aacc[1].l||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].url,a),c[1].libs&&C&&C(c[1].libs))},ta=function(a){A("gc",a)},ua=null,va=function(a){ua=a},sa=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",v);p("
2022-07-26 19:52:29 UTC	75	IN	Data Raw: 61 2c 68 6c 3a 22 64 65 22 7d 3b 76 2e 67 6c 3d 45 61 3b 77 61 3f 41 61 2e 6c 6f 61 64 7c 7c 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3a 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3b 70 28 22 64 67 6c 22 2c 42 61 29 3b 70 28 22 61 67 6c 22 2c 44 61 29 3b 68 2e 6f 3d 78 61 7d 3b 76 61 72 20 46 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 30 30 31 29 2c 47 61 3d 30 3b 0a 66 75 6e 63 74 69 6f 6e 20 5f 6d 6c 54 6f 6b 65 6e 28 61 2c 62 29 7b 74 72 79 7b 69 66 28 31 3e 47 61 29 7b 47 61 2b 2b 3b 76 61 72 20 63 3d 61 3b 62 3d 62 7c 7c 7b 3b 76 61 72 20 64 3d 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 2c 66 3d 5b 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 Data Ascii: a,hl:"de"};v.gl=Ea;wa?Aa.load||p("load",Ba,Aa):p("load",Ba,Aa);p("dgl",Ba);p("agl",Da);h.o=xa};var Fa=h.b("0.1",.001),Ga=0;function _mlToken(a,b){try{if(1>Ga){Ga++;var c=a;b=b||{};var d=encodeURIComponent,f=["//www.google.com/gen_204?atyp=i&zx=",(new Dat

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	76	IN	Data Raw: 28 61 2c 62 29 7b 48 28 61 2c 62 29 3f 4b 28 61 2c 62 29 3a 4a 28 61 2c 62 29 7d 2c 4e 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 7d 2c 4f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 0a 5b 4c 61 3f 22 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 22 2c 22 2f 6f 67 2f 5f 2f 6a 73 2f 64 3d 31 2f 6b 3d 22 2c 22 6f 67 2e 6f 67 32 2e 65 6e 5f 55 53 2e 68 79 6a 56 6d 61 75 61 37 79 41 2e 4f 22 2c 22 2f 72 74 3d 6a 2f 6d 3d 22 2c 61 2c 22 2f 72 73 3d 22 2c 22 41 41 32 59 72 54 76 32 59 6d 4e 78 6b 6f 64 75 52 48 6c Data Ascii: (a,b){H(a,b)?K(a,b):J(a,b)},Na=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})}},Oa=function(a){a=[La?"":"https://www.gstatic.com","/og/_/js/d=1/k=","og.og2.en_US.hyjVmaua7yA.O","/rt=j/m=",a,"/rs=","AA2YrTv2YmNxkoduRHl
2022-07-26 19:52:29 UTC	77	IN	Data Raw: 74 65 28 22 61 72 69 61 2d 6f 77 6e 73 22 29 3b 69 66 28 64 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 66 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 64 29 3b 69 66 28 66 29 7b 76 61 72 20 6b 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 69 66 28 4f 3d 3d 64 29 4f 3d 76 6f 69 64 20 30 2c 0a 4b 28 6b 2c 22 67 62 74 6f 22 29 3b 65 6c 73 65 7b 69 66 28 4f 29 7b 76 61 72 20 6d 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 4f 29 3b 69 66 28 6d 26 26 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 29 7b 76 61 72 20 6e 3d 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 6f 77 6e 65 72 22 29 3b 69 66 28 6e 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 6c 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e Data Ascii: te("aria-owns");if(d.length){var f=document.getElementById(d);if(f){var k=b.parentNode;if(O==d)O=void 0,K(k,"gbto");else{if(O){var m=document.getElementById(O);if(m&&m.getAttribute){var n=m.getAttribute("aria-owner");if(n.length){var l=document.getElemen
2022-07-26 19:52:29 UTC	78	IN	Data Raw: 29 7c 7c 28 6c 3d 64 29 7d 62 72 65 61 6b 7d 30 3c 64 26 26 64 2b 31 3c 6e 26 26 64 2b 2b 7d 69 66 28 30 3c 3d 6c 29 7b 76 61 72 20 79 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 79 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 63 22 3b 7a 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 20 67 62 6d 68 22 3b 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 7a 29 3b 6b 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 79 2c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 6c 5d 29 7d 67 2e 61 64 64 48 6f 76 65 72 26 26 67 2e 61 64 64 48 6f 76 65 72 28 61 29 7d 65 6c 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 7d 63 61 74 63 Data Ascii:)||(l=d)}break}0<d&&d+1<n&&d++}if(0<=l){var y=document.createElement("li"),z=document.createElement("div");y.className="gbmtc";z.className="gbmt gbmh";y.appendChild(z);k.insertBefore(y,k.childNodes[l])}g.addHover&&g.addHover(a)}else k.appendChild(m)}}catc
2022-07-26 19:52:29 UTC	80	IN	Data Raw: 74 43 6f 6e 74 65 6e 74 3d 22 22 3b 62 3d 62 2e 73 70 6c 69 74 28 63 29 3b 63 3d 30 3b 66 6f 72 28 76 61 72 20 66 3b 66 3d 62 5b 63 5d 3b 63 2b 2b 29 7b 76 61 72 20 6b 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 0a 6b 2e 69 6e 6e 65 72 48 54 4d 4c 3d 66 3b 64 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6b 29 7d 7d 65 6c 73 65 20 64 2e 69 6e 6e 65 72 48 54 4d 4c 3d 62 3b 51 28 61 2c 21 30 29 7d 7d 7d 2c 51 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 28 62 3d 76 6f 69 64 20 30 21 3d 3d 62 3f 62 3a 21 30 29 3f 4a 28 61 2c 22 67 62 6d 73 67 6f 22 29 3a 4b 28 61 2c 22 67 62 6d 73 67 6f 22 29 7d 2c 24 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 63 3d 61 2e 63 68 69 6c 64 4e 6f Data Ascii: tContent="";b=b.split(c);c=0;for(var f;f=b[c];c++){var k=document.createElement("div");k.innerHTML=f;d.appendChild(k)}}else d.innerHTML=b;Q(a,!0)}}},Q=function(a,b){(b=void 0!==b?b:!0)?J(a,"gbmsgo"):K(a,"gbmsgo")},$a=function(a){for(var b=0,c;c=a.childNo
2022-07-26 19:52:29 UTC	81	IN	Data Raw: 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 6c 69 62 73 3a 22 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6c 69 65 6e 74 3a 67 61 70 69 2e 69 66 72 61 6d 65 73 22 7d 5d 29 3b 76 61 72 20 42 62 3d 7b 76 65 72 73 69 6f 6e 3a 22 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 69 6e 64 65 78 3a 22 22 2c 6c 61 6e 67 3a 22 64 65 22 7d 3b 76 2e 67 63 3d 42 62 3b 76 61 72 20 43 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 61 70 69 73 26 26 77 69 6e 64 6f 77 2e 69 66 72 61 6d 65 73 3f 61 26 26 61 28 29 3a 28 61 26 26 74 61 28 61 29 2c 44 28 22 67 63 22 29 29 7d 3b 70 28 22 6c 47 43 22 2c 43 62 29 3b 68 2e 61 28 22 31 22 29 26 26 70 28 Data Ascii: 787dcc2a4062e6e9824.js",libs:"googleapis.client:gapi.iframes"}]);var Bb={version:"gci_91f30755d6a6b787dcc2a4062e6e9824.js",index:"",lang:"de"};v.gc=Bb;var Cb=function(a){window.googleapis&&window.iframes?a&&a():(a&&ta(a),D("gc"))};p("lGC",Cb);h.a("1")&&p(
2022-07-26 19:52:29 UTC	82	IN	Data Raw: 21 3d 6e 3f 6e 3a 22 22 7d 65 6c 73 65 20 6e 3d 22 22 3b 66 3d 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 6b 3d 64 28 22 32 38 38 33 34 22 29 3b 6d 3d 64 28 22 5f 55 58 67 59 74 6a 6b 4a 4a 6d 44 78 63 38 50 6e 74 73 37 22 29 3b 76 61 72 20 6c 3d 67 2e 62 76 2e 66 2c 71 3d 64 28 22 31 22 29 3b 6e 3d 64 28 6e 29 3b 63 3d 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 63 29 3b 76 61 72 20 45 3d 64 28 22 34 36 31 35 31 31 30 38 39 2e 30 22 29 2c 55 3d 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 36 30 37 2e 31 5f 70 30 22 29 2c 49 3d 64 28 22 63 6f 6d 22 29 2c 56 3d 64 28 22 64 65 22 29 2c 57 3d 0a 64 28 22 44 45 55 22 29 3b 76 61 72 20 79 3d 30 3b 68 2e 61 28 22 22 29 26 26 28 79 7c 3d 31 29 3b 68 Data Ascii: !=n?n:""}else n="";f=(new Date).getTime();k=d("28834");m=d("_UXgYtjkJJmDxc8Pnts7");var l=g.bv.f,q=d("1");n=d(n);c=Math.round(1/c);var E=d("461511089.0"),U="&oggv="+d("es_plusone_gc_20220607.1_p0"),I=d("com"),V=d("de"),W=d("DEU");var y=0;h.a("")&&(y|=1);h
2022-07-26 19:52:29 UTC	84	IN	Data Raw: 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 0a 24 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 6d 28 29 7d 29 3b 70 28 22 73 70 6e 22 2c 56 62 29 3b 70 28 22 73 70 70 22 2c 58 62 29 3b 70 28 22 73 70 70 22 2c 57 62 29 3b 70 28 22 73 70 6d 22 2c 24 62 29 3b 70 28 22 70 61 61 22 2c 54 62 29 3b 70 28 22 70 72 6d 22 2c 55 62 29 3b 6d 62 28 22 67 62 64 34 22 2c 55 62 29 3b 0a 69 66 28 68 2e 61 28 22 22 29 29 7b 76 61 72 20 61 63 3d 7b 64 3a 68 2e 61 28 22 22 29 2c 65 3a 22 22 2c 73 61 6e 77 3a 68 2e 61 28 22 22 29 2c 70 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 Data Ascii: nt.com/ogw/default-user=s24"},$b=function(){B(function(){g.spd()})};p("spn",Vb);p("spp",Xb);p("sps",Wb);p("spd",$b);p("paa",Tb);p("prm",Ub);mb("gbd4",Ub);if(h.a("")){var ac={d:h.a(""),e:"",sanw:h.a(""),p:"https://lh3.googleusercontent.com/ogw/default-us
2022-07-26 19:52:29 UTC	85	IN	Data Raw: 3d 31 3b 0a 76 61 72 20 6a 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 21 31 3b 74 72 79 7b 62 3d 61 2e 63 6f 6f 6b 69 65 26 26 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 22 50 52 45 46 22 29 7d 63 61 74 63 68 28 63 29 7b 7d 72 65 74 75 72 6e 21 62 7d 2c 6b 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 72 65 74 75 72 6e 21 21 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 7d 63 61 74 63 68 28 61 29 7b 72 65 74 75 72 6e 21 31 7d 7d 2c 6c 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 26 26 61 2e 73 74 79 6c 65 26 26 61 2e 73 74 79 6c 65 2e 62 65 68 61 76 69 6f 72 26 26 22 75 6e 64 65 66 69 6e 65 64 22 21 3d 74 79 70 65 6f Data Ascii: =1;var jc=function(a){var b=!1;try{b=a.cookie&&a.cookie.match("PREF")}catch(c){}return!b},kc=function(){try{return!!e.localStorage&&"object"==typeof e.localStorage}catch(a){return!1}},lc=function(a){return a&&a.style&&a.style.behavior&&"undefined"!=typeo

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	86	IN	Data Raw: 28 74 68 69 73 2c 64 29 7d 29 7d 7d 3b 5a 28 67 2e 75 70 2c 22 73 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 73 69 22 29 3b 5a 28 67 2e 75 70 2c 22 73 70 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 64 70 63 22 29 3b 5a 28 67 2e 75 70 2c 22 69 69 63 22 29 3b 67 2e 6d 63 66 28 22 75 70 22 2c 7b 73 70 3a 68 2e 62 28 22 30 2e 30 31 22 2c 31 29 2c 74 6c 64 3a 22 64 65 22 2c 70 72 69 64 3a 22 31 22 7d 29 3b 66 75 6e 63 74 69 6f 6e 20 72 63 28 29 7b 66 75 6e 63 74 69 6f 6e 20 61 28 29 7b 66 6f 72 28 76 61 72 20 6c 3b 28 6c 3d 6b 5b 6d 2b 2b 5d 29 26 26 22 6d 22 21 3d 6c 5b 30 5d 26 26 21 6c 5b 31 5d 2e 61 75 74 6f 3b 29 3b 6c 26 26 28 73 61 28 32 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 75 72 6c 26 26 72 61 28 6c 5b 31 5d 2e 75 72 6c 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 6c 69 62 73 Data Ascii: (this,d)}}}};Z(g.up,"sl");Z(g.up,"si");Z(g.up,"spl");Z(g.up,"dpc");Z(g.up,"iic");g.mcf("up",{sp:h.b("0.01",1),tld:"de",prid:"1"});function rc(){function a(){for(var l;(l=k[m++])&&"m"!=l[0]&&!l[1].auto;);l&&(sa(2,l[0]),l[1].url&&ra(l[1].url,l[0]),l[1].libs
2022-07-26 19:52:29 UTC	87	IN	Data Raw: 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 64 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 2e 69 3b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 76 61 72 20 66 3d 65 2e 69 3b 76 61 72 20 67 3d 66 2e 63 28 22 31 22 2c 30 29 2c 68 3d 2f 5c 62 67 62 6d 74 5c 62 2f 2c 6b 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 74 72 79 7b 76 61 72 20 62 3d Data Ascii: ogger&&gbar.logger.ml(e,{"_sn":"cfg.init"})});})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var d=window.gbar.i.i;var e=window.gbar;var f=e.i;var g=f.c("1",0),h=/\bgbmt\b/,k=function(a){try{var b=
2022-07-26 19:52:29 UTC	89	IN	Data Raw: 22 29 2c 0a 73 6e 69 64 3a 65 28 22 32 38 38 33 34 22 29 2c 74 6f 3a 65 28 22 33 30 30 30 30 30 22 29 2c 75 3a 65 28 22 22 29 2c 76 66 3a 22 2e 36 36 2e 22 7d 2c 67 3d 66 2c 68 3d 5b 22 62 6e 64 63 66 67 22 5d 2c 6b 3d 61 3b 68 5b 30 5d 69 6e 20 6b 7c 7c 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6b 2e 65 78 65 63 53 63 72 69 70 74 7c 7c 6b 2e 65 78 65 63 53 63 72 69 70 74 28 22 76 61 72 20 22 2b 68 5b 30 5d 29 3b 66 6f 72 28 76 61 72 20 6c 3b 68 2e 6c 65 6e 67 74 68 26 26 28 6c 3d 68 2e 73 68 69 66 74 28 29 29 3b 29 68 2e 6c 65 6e 67 74 68 7c 7c 76 6f 69 64 20 30 3d 3d 3d 67 3f 6b 3d 6b 5b 6c 5d 26 26 6b 5b 6c 5d 21 3d 3d 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 5b 6c 5d 3f 6b 5b 6c 5d 3a 6b 5b 6c 5d 3d 7b 7d 3a 6b 5b 6c 5d 3d 67 Data Ascii: "),snid:e("28834"),to:e("300000"),u:e(""),vf:".66."},g=f,h=["bndcfg"],k=a;h[0]in k||"undefined"==typeof k.execScript||k.execScript("var "+h[0]);for(var l;h.length&&(l=h.shift());)h.length||void 0===g?k=k[l]&&k[l]!==Object.prototype[l]?k[l]:k[l]={}:k[l]=g
2022-07-26 19:52:29 UTC	90	IN	Data Raw: 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 42 69 6c 64 65 72 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 70 73 2e 67 6f 6f 67 6c 65 2e 64 65 2f 6d 61 70 73 3f 68 6c 3d 64 65 26 74 61 62 3d 77 6c 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 4d 61 70 73 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 37 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 6c 61 79 2e 67 6f 6f 67 Data Ascii: b2>Bilder <li class=gbt>Maps <li class=gbt><a class=gbzt id=gb_78 href="https://play.goog
2022-07-26 19:52:29 UTC	91	IN	Data Raw: 29 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 20 69 64 3d 67 62 64 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 7a 74 6d 3e 3c 64 69 76 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 20 67 62 73 62 69 73 22 3e 3c 6f 6c 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 69 63 22 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 34 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 61 6c 65 6e 64 61 72 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 63 61 6c 65 6e 64 61 72 3f 74 61 62 3d 77 63 22 3e 4b 61 6c 65 6e 64 65 72 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 Data Ascii:); });</script> <ol id=gbmm class="gbmcc gbsbic"><li class=gbmtc>Kalender <li class=gbmtc><a cla
2022-07-26 19:52:29 UTC	92	IN	Data Raw: 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 31 2c 7b 74 3a 36 36 7d 29 3b 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 73 62 74 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 73 62 62 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 32 20 63 6c 61 73 73 3d 67 62 78 78 3e 41 63 63 6f 75 6e 74 20 4f 70 74 69 6f 6e 73 3c 2f 68 32 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 63 62 3e 3c 2f 73 70 61 6e 3e 3c 6f 6c 20 63 6c 61 73 73 3d 67 62 74 63 3e Data Ascii: tListener('click', function clickHandler() { gbar.logger.il(1,{t:66});; });</script> <h2 class=gbxx>Account Options</h2><ol class=gbtc>
2022-07-26 19:52:29 UTC	94	IN	Data Raw: 69 76 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 33 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 34 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 6c 41 56 42 49 34 71 6e 50 67 54 6a 6e 5a 41 7a 32 31 79 4d 65 67 27 3e 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 65 6c 70 26 26 67 62 61 72 2e 65 6c 70 28 29 3c 2f 73 63 72 69 70 74 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 63 65 6e 74 65 72 3e 3c 62 72 20 63 6c 65 61 72 3d 22 6c 6c 22 20 69 64 3d 22 6c 67 70 64 22 3e 3c 64 69 76 20 69 64 3d 22 6c 67 61 22 3e 3c 61 20 68 72 65 66 3d 22 2f 73 65 61 72 63 68 3f 69 65 3d 55 54 46 2d 38 26 61 6d 70 3b 71 3d 53 74 65 65 6c 2b 50 61 6e 26 61 6d 70 Data Ascii: iv> <script nonce='lAVBI4qnPgTjnZAz21yMeg'>window.gbar&&gbar.elp&&gbar.elp()</script> <br clear="all" id="lgpd"> <a href="/search?ie=UTF-8&q=Steel+Pan&amp
2022-07-26 19:52:29 UTC	95	IN	Data Raw: 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 75 63 68 65 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 31 22 20 76 61 6c 75 65 3d 22 41 75 66 20 67 75 74 20 47 6c fc 63 6b 21 22 20 6e 61 6d 65 3d 22 62 74 6e 49 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 6c 41 56 42 49 34 71 6e 50 67 54 6a 6e 5a 41 7a 32 31 79 4d 65 67 22 3e 28 66 75 6e Data Ascii: an class="lsbb"><input class="lsb" value="Google Suche" name="btnG" type="submit"><input class="lsb" id="tsuid1" value="Auf gut Glck!" name="btnI" type="submit"><script nonce="lAVBI4qnPgTjnZAz21yMeg">(fun

Timestamp	kBytes transferred	Direction	Data
2022-07-26 19:52:29 UTC	96	IN	Data Raw: 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 3a 63 65 6e 74 65 72 22 20 69 64 3d 22 57 71 51 41 4e 62 22 3e 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 64 65 2f 61 64 73 2f 22 3e 57 65 72 62 65 6e 20 6d 69 74 20 47 6f 6f 67 6c 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 2f 73 65 72 76 69 63 Data Ascii: ></form> Werben mit Google<a href="/servic
2022-07-26 19:52:29 UTC	98	IN	Data Raw: 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 45 64 2d 6e 4d 73 6a 61 37 64 63 2e 4f 2f 61 6d 5c 78 33 64 41 4d 41 54 41 49 41 45 41 45 67 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 45 71 59 63 78 37 44 65 5a 6e 41 7a 68 7a 75 36 45 6b 48 42 49 66 4e 42 2d 67 78 67 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 61 72 20 67 3b 76 61 72 20 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 68 69 73 2e 67 3d 62 3d 3d 3d 68 3f 61 3a 22 22 7d 3b 6c 2e 70 72 6f 74 6f 74 79 70 65 2e 74 6f 53 74 72 69 6e 67 3d 66 Data Ascii: function(){var u='/xjs/_/js/k\x3dxjs.hp.en.Ed-nMsja7dc.O/am\x3dAMATAIAEAEg/d\x3d1/ed\x3d1/rs\x3dAC T90oEqYcx7DeZnAzhzu6EkHBIfNB-gxg/m\x3dsb_he,d';var d=this||self,e=function(a){return a};var g;var l=function(a,b){this.g=b===h?a:"";l.prototype.toString=f
2022-07-26 19:52:29 UTC	99	IN	Data Raw: 7b 61 74 74 6e 3a 66 61 6c 73 65 2c 62 6c 74 3a 27 6e 6f 6e 65 27 2c 63 68 6e 6b 3a 30 2c 64 77 3a 66 61 6c 73 65 2c 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 72 74 3a 30 2c 75 62 6d 3a 66 61 6c 73 65 2c 75 77 70 3a 74 72 75 65 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 70 6d 63 3d 27 7b 5c 78 32 32 64 5c 78 32 32 3a 7b 7d 2c 5c 78 32 32 73 62 5f 68 65 5c 78 32 32 3a 7b 5c 78 32 32 61 67 65 6e 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 63 67 65 6e 5c Data Ascii: {attn:false,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='{\x22d\x22:{},\x22sb_he\x22:{\x22agen\x22:true,\x22cgen\
2022-07-26 19:52:29 UTC	100	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: D6GEVBNNH11111.exe PID: **3436**, Parent PID: **5716**

General

Target ID:	0
Start time:	21:52:08
Start date:	26/07/2022
Path:	C:\Users\user\Desktop\D6GEVBNNH11111.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\D6GEVBNNH11111.exe"
Imagebase:	0xb20000
File size:	640512 bytes
MD5 hash:	9CEF8265C679BAFB06F885678CEAB7BD
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: 00000000.00000002.456920390.000000000491D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.456920390.000000000491D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.456040536.0000000004817000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.456040536.0000000004817000.00000004.00000800.00020000.00000000.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	6D68CF06	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	6D68CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\D6GEVBNNH11111.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D99C78D	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D6GEVBNNH11111.exe	C:\Users\user\AppData\Local\Temp\geater.exe	success or wait	1	D999BFF	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\D6GEVBNNH11111.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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",02,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.	success or wait	1	6D99C907	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	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	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: geater.exe PID: **3972**, Parent PID: **3436**

General

Target ID:	6
Start time:	21:52:26
Start date:	26/07/2022
Path:	C:\Users\user\AppData\Local\Temp\geater.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\geater.exe"
Imagebase:	0xb20000
File size:	640512 bytes
MD5 hash:	9CEF8265C679BAFB06F885678CEAB7BD
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: 00000006.00000002.668565825.00000000046A6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.668565825.00000000046A6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.667459782.000000000464C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.667459782.000000000464C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.671650352.00000000047AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.671650352.00000000047AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D68CF06	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	6D68CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\geater.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D99C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\geater.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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",02,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.	success or wait	1	6D99C907	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	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	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: **3512**, Parent PID: **3972**

General

Target ID:	15
Start time:	21:53:19
Start date:	26/07/2022
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:	0x760000
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: 0000000F.00000000.561341870.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.561341870.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.561888828.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.561888828.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.682815690.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.682815690.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.562345029.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.562345029.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.560518912.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.560518912.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.686918576.000000002A21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.686918576.000000002A21000.00000004.00000800.00020000.00000000.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	6D68CF06	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	6D68CF06	unknown
C:\Users\user\AppData\Roaming\Acrobat	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C4DBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.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	6C4DDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.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	6C4DDD66	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	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D66CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Acrobat	unicode	C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe	success or wait	1	6C4D646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Acrobat	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C4DDE2E	RegSetValueExW

Disassembly

No disassembly