

JoeSandbox Cloud BASIC



ID: 679195

Sample Name: 4EBE6@3.exe

Cookbook: default.jbs

Time: 11:56:52

Date: 05/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report 4EBE6@3.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
System Summary	6
Persistence and Installation Behavior	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	17
Public IPs	17
General Information	17
Warnings	18
Simulations	18
Behavior and APIs	18
Joe Sandbox View / Context	18
IPs	18
Domains	18
ASNs	18
JA3 Fingerprints	18
Dropped Files	19
Created / dropped Files	19
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4EBE6@3.exe.log	19
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Acrobat.exe.log	19
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\noise.exe.log	19
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe	20
\Device\ConDrv	20
Static File Info	20
General	20
File Icon	21
Static PE Info	21
General	21
Entrypoint Preview	21
Data Directories	23
Sections	23
Resources	23
Imports	24
Network Behavior	24
Network Port Distribution	24
TCP Packets	24
UDP Packets	26
DNS Queries	26
DNS Answers	26
HTTP Request Dependency Graph	26
HTTPS Proxied Packets	26

Statistics	37
Behavior	37
System Behavior	38
Analysis Process: 4EBE6@3.exePID: 400, Parent PID: 4472	38
General	38
File Activities	38
File Created	38
File Moved	39
File Written	39
File Read	39
Registry Activities	39
Analysis Process: noise.exePID: 1600, Parent PID: 400	40
General	40
File Activities	40
File Created	40
File Written	40
File Read	41
Registry Activities	41
Analysis Process: InstallUtil.exePID: 6036, Parent PID: 1600	41
General	41
File Activities	42
File Created	42
File Written	42
File Read	43
Registry Activities	43
Key Value Created	43
Analysis Process: Acrobat.exePID: 4876, Parent PID: 3968	44
General	44
File Activities	44
File Created	44
File Written	44
File Read	45
Analysis Process: conhost.exePID: 1112, Parent PID: 4876	46
General	46
Disassembly	46

Windows Analysis Report

4EBE6@3.exe

Overview

General Information

Sample Name:

4EBE6@3.exe

Analysis ID:

679195

MD5:

ade71491b076ca..

SHA1:

75623647a35d7b..

SHA256:

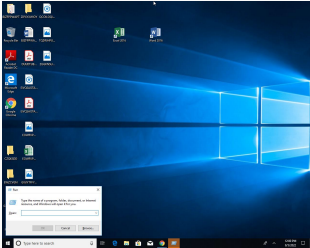
81baf55c19c00e...

Tags:

exe

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Yara detected AgentTesla

Antivirus / Scanner detection for sub...

Tries to steal Mail credentials (via fi...

Writes to foreign memory regions

Drops executable to a common third...

Machine Learning detection for sam...

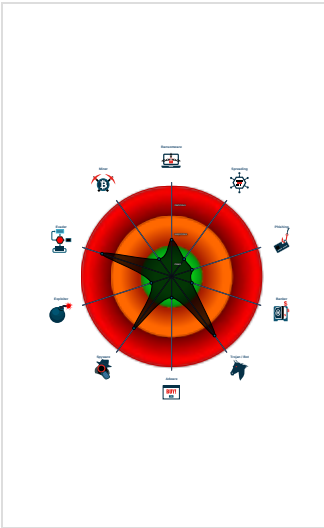
Injects a PE file into a foreign proce...

.NET source code contains very larg...

Hides that the sample has been dow...

Moves itself to temp directory

Classification



Process Tree

System is w10x64

4EBE6@3.exe (PID: 400 cmdline: "C:\Users\user\Desktop\4EBE6@3.exe" MD5: ADE71491B076CA7A43EFAF0214DD030)

noise.exe (PID: 1600 cmdline: "C:\Users\user\AppData\Local\Temp\noise.exe" MD5: ADE71491B076CA7A43EFAF0214DD030)

InstallUtil.exe (PID: 6036 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)

Acrobat.exe (PID: 4876 cmdline: "C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe" MD5: EFEC8C379D165E3F33B536739AEE26A3)

conhost.exe (PID: 1112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cleanup

Malware Configuration

Threatname: Agenttesla

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.342705097.00000000049B5000.0000004.000000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.342705097.00000000049B5000.0000004.000000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Page 4 of 46

Source	Rule	Description	Author	Strings
00000001.00000002.342705097.00000000049B5000.0000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x65a3a:\$a13: get_DnsResolver 0x9a32a:\$a13: get_DnsResolver 0xcec0a:\$a13: get_DnsResolver 0x6421e:\$a20: get_LastAccessed 0x98b0e:\$a20: get_LastAccessed 0xcd3ee:\$a20: get_LastAccessed 0x663cc:\$a27: set_InternalServerPort 0x9acbc:\$a27: set_InternalServerPort 0xcf59c:\$a27: set_InternalServerPort 0x666e8:\$a30: set_GuidMasterKey 0x9afd8:\$a30: set_GuidMasterKey 0xcf8b8:\$a30: set_GuidMasterKey 0x64325:\$a33: get_Clipboard 0x98c15:\$a33: get_Clipboard 0xcd4f5:\$a33: get_Clipboard 0x64333:\$a34: get_Keyboard 0x98c23:\$a34: get_Keyboard 0xcd503:\$a34: get_Keyboard 0x65655:\$a35: get_ShiftKeyDown 0x99f45:\$a35: get_ShiftKeyDown 0xce825:\$a35: get_ShiftKeyDown
0000000D.00000002.532021277.0000000003E1A000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.532021277.0000000003E1A000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
13.2.noise.exe.3ea9c02.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.noise.exe.3ea9c02.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.2.noise.exe.3ea9c02.2.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
13.2.noise.exe.3ea9c02.2.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x2e5d8:\$a13: get_DnsResolver 0x2cdbc:\$a20: get_LastAccessed 0x2ef6a:\$a27: set_InternalServerPort 0x2f286:\$a30: set_GuidMasterKey 0x2cec3:\$a33: get_Clipboard 0x2ced1:\$a34: get_Keyboard 0x2e1f3:\$a35: get_ShiftKeyDown 0x2e204:\$a36: get_AltKeyDown 0x2cede:\$a37: get_Password 0x2d99a:\$a38: get_PasswordHash 0x2e9d8:\$a39: get_DefaultCredentials
1.2.4EBE6@3.exe.4a1ef52.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 79 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

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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



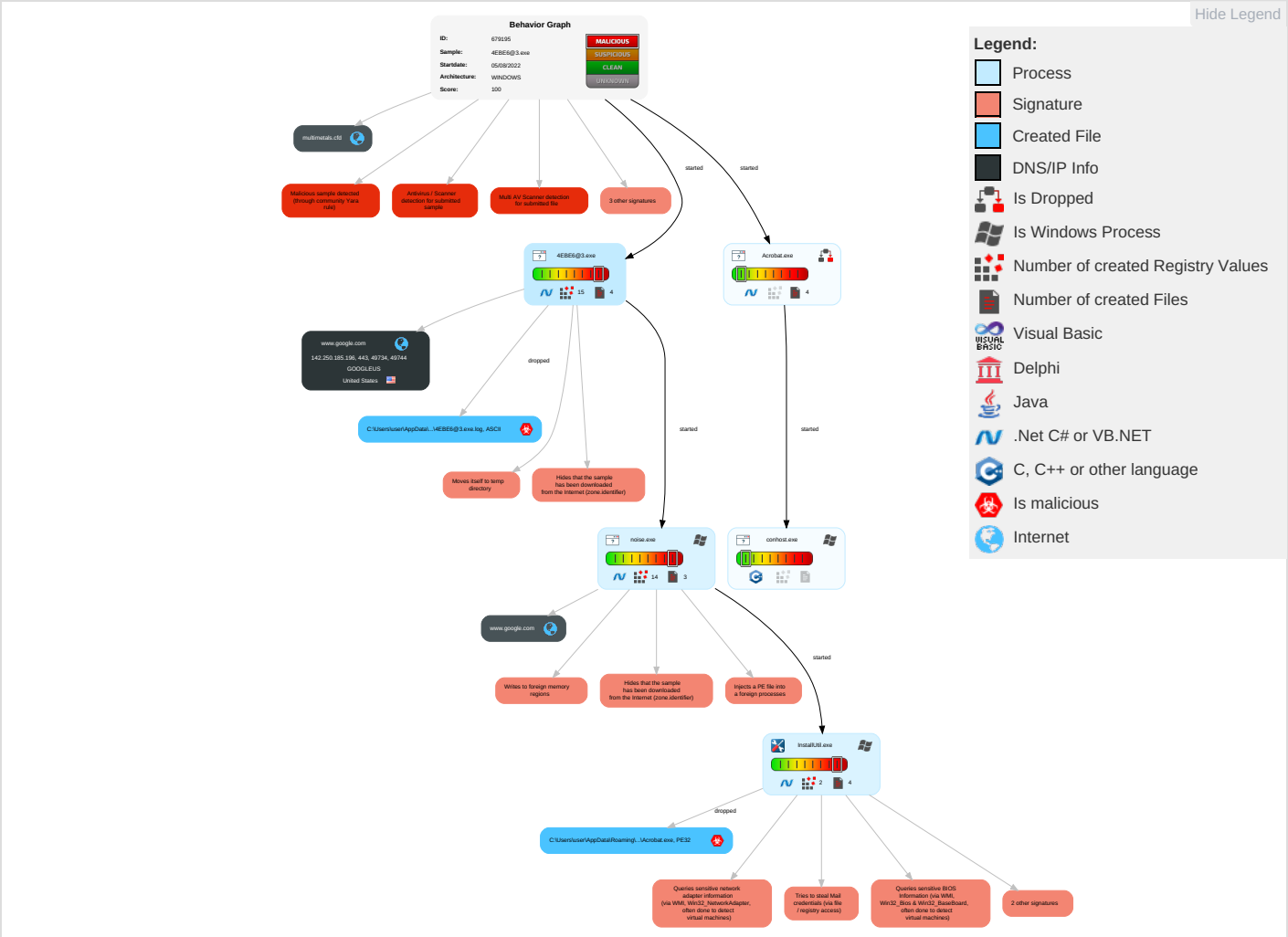
Yara detected AgentTesla

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	2 1 Masquerading	OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	2 1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	NTDS	1 Application Window 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 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 1 Process Injection	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Deobfuscate/Decode Files or Information	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Obfuscated Files or Information	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Software Packing	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
4EBE6@3.exe	62%	Virustotal		Browse
4EBE6@3.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	
4EBE6@3.exe	100%	Avira	TR/Kryptik.avxgd	
4EBE6@3.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
18.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://www.carterandcone.comueto	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnO	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://OKJTye.com	0%	Avira URL Cloud	safe	
http://ns.ado/1=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://r3.i.lencr.org/OW	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tiro.comH	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.tiro.comm4	0%	Avira URL Cloud	safe	
http://www.tiro.X5i	0%	Avira URL Cloud	safe	
http://https://www.google.comT	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://https://XWC3ojCmGHGFT3OQK.com	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://www.founder.com.cn/cnx	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejdpaswordPsi/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.carterandcone.comP	0%	URL Reputation	safe	
http://www.carterandcone.comitk	0%	URL Reputation	safe	
http://www.carterandcone.comO	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.carterandcone.compri9m	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://www.tiro.comg5h	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://multimetals.cfd	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTFGZP	0%	Avira URL Cloud	safe	
http://www.tiro.como5p	0%	Avira URL Cloud	safe	
http://www.carterandcone.comormll	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnt-it	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ns.adobe.cobj=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.tiro.com.57	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://ns.adobe.c/g=	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnJ	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	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	142.250.185.196	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://www.carterandcone.comueto	4EBE6@3.exe, 00000001.00000003.308641145.00000000C4FD000.00000004.00000800.00020000.000000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://www.founder.com.cn/cnO	4EBE6@3.exe, 00000001.00000003.307638553.00000000C51F000.00000004.00000800.00020000.000000000.sdmp	false	URL Reputation: safe	unknown	
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low	
http://www.fontbureau.com/designersG	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000.sdmp	false		high	
http://www.fontbureau.com/designers/?	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000.sdmp	false		high	
http://OKJTye.com	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://ns.ado/1=	noise.exe, 0000000D.00000003.363977934.00000000BA34000.00000004.00000800.00020000.000000000.sdmp, noise.exe, 0000000D.00000003.361734419.00000000BA30000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://www.founder.com.cn/cn/bThe	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000.sdmp	false	URL Reputation: safe	unknown	
http://r3.i.lencr.org/OW	InstallUtil.exe, 00000012.00000002.593597181.0000000062F7000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.592820026.0000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595628659.0000000006BF1000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.00000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://www.fontbureau.com/designers?	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000.sdmp	false		high	
http://www.tiro.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308155481.000000000C522000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	4EBE6@3.exe, 00000001.00000003.311683387.00000000C526000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.313016653.00000000C526000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobe.c/g	noise.exe, 0000000D.00000003.513958247.00000000BA34000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000002.553577663.00000000BA31000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.goodfont.co.kr	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.comH	4EBE6@3.exe, 00000001.00000003.308235544.00000000C524000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308086430.00000000C520000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308155481.00000000C522000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://crl.securetrust.com/SGCA.crl0	InstallUtil.exe, 00000012.00000002.592820026.00000006230000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.com	4EBE6@3.exe, 00000001.00000003.308655177.00000000C507000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308405539.00000000C4F3000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308641145.00000000C4FD000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308788980.00000000C500000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	InstallUtil.exe, 00000012.00000002.592820026.00000006230000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 00000012.00000002.595246005.00000006B70000.00000004.00000001.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypeworks.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.google.com	4EBE6@3.exe	false		high
http://www.founder.com.cn/cn/cThe	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.comm4	4EBE6@3.exe, 00000001.00000003.308235544.00000000C524000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308086430.00000000C520000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308155481.00000000C522000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.X5i	4EBE6@3.exe, 00000001.00000003.308235544.00000000C524000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308086430.00000000C520000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308155481.00000000C522000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.google.comT	4EBE6@3.exe, 00000001.00000002.335489101.0000000030D1000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000002.516839182.000000002591000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 00000012.00000002.595246005.00000006B70000.00000004.00000001.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://XWC3ojCmGHGFT3OQK.com	InstallUtil.exe, 00000012.00000002.589451778.00000000329B000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.588768404.00000000323B000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.574138944.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589525884.0000000032A3000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://x1.c.lencr.org/0	InstallUtil.exe, 00000012.00000002.593597181.0000000062F7000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.592820026.000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595628659.000000006BF1000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.0000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://x1.i.lencr.org/0	InstallUtil.exe, 00000012.00000002.593597181.0000000062F7000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.592820026.000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595628659.000000006BF1000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.0000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cnx	4EBE6@3.exe, 00000001.00000003.307605500.00000000C51E000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.307638553.00000000C51F000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designersd	4EBE6@3.exe, 00000001.00000003.311250923.00000000C526000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designersb	4EBE6@3.exe, 00000001.00000003.312910654.00000000C526000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.312761645.00000000C526000.00000004.00000800.00020000.00000000.sdmp	false		high

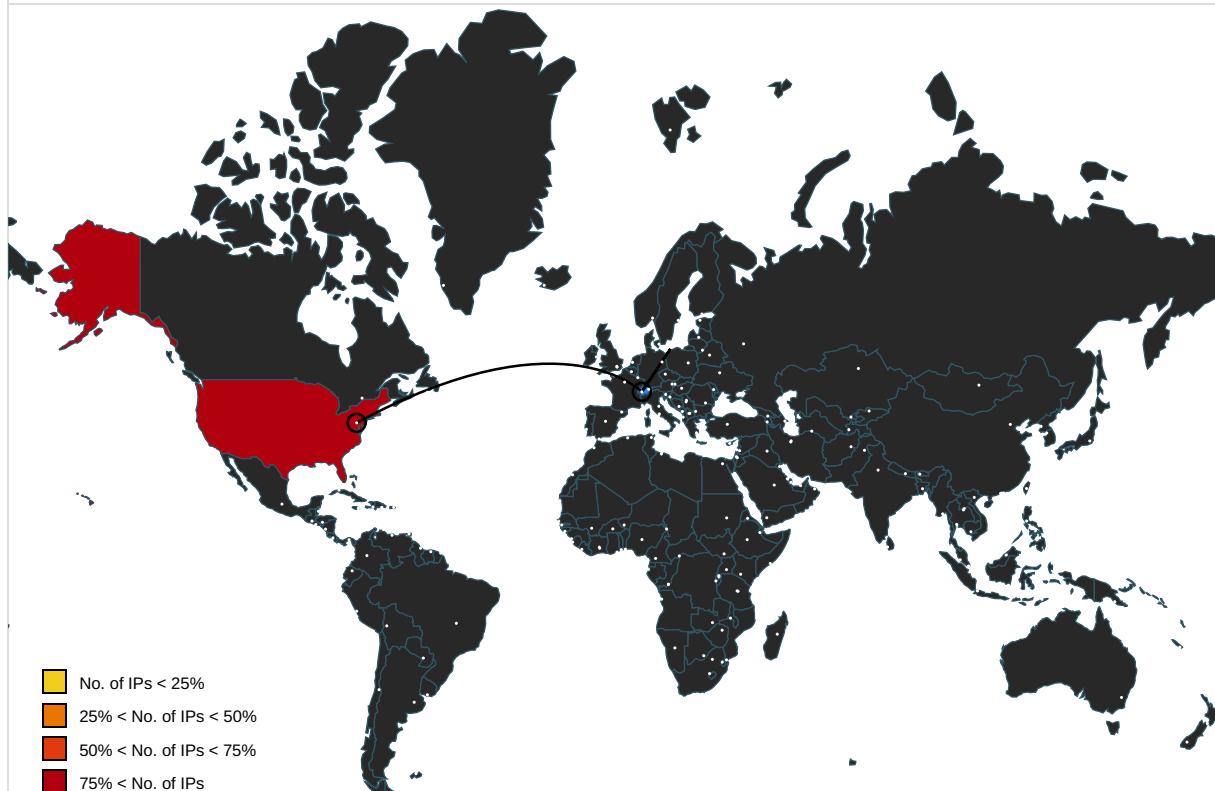
Name	Source	Malicious	Antivirus Detection	Reputation
http://r3.o.lencr.org	InstallUtil.exe, 00000012.00000002.593597181.0000000062F7000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.592820026.000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.0000000002.595628659.0000000006BF1000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.00000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.comP	4EBE6@3.exe, 00000001.00000003.308641145.00000000C4FD000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308788980.00000000C500000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.comitk	4EBE6@3.exe, 00000001.00000003.309064067.00000000C507000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309665888.00000000C509000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309945289.00000000C509000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309255079.00000000C503000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308655177.00000000C507000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308798013.00000000C508000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.310274973.00000000C4FF000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.310221987.00000000C4FF000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309215561.00000000C503000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309215561.00000000C503000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.309316656.00000000C503000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.comO	4EBE6@3.exe, 00000001.00000003.308788980.00000000C500000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fonts.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	4EBE6@3.exe, 00000001.00000002.335489101.0000000030D1000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000002.516839182.0000000002591000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como	4EBE6@3.exe, 00000001.00000003.308405539.00000000C4F3000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sakkal.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.ipify.org%	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://www.carterandcone.compri9m	4EBE6@3.exe, 00000001.00000003.308641145.00000000C4FD000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308788980.00000000C500000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.root-x1.letsencrypt.org	InstallUtil.exe, 00000012.00000002.592820026.000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595628659.0000000006BF1000.00000004.0000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595246005.0000000006B70000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.00000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.comg5h	4EBE6@3.exe, 00000001.00000003.308050243.00000000C520000.00000004.00000800.00020000.000000000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.carterandcone.coma	4EBE6@3.exe, 00000001.00000003.308405539.00000000C4F3000.00000004.00000800.00020000.000000000000.sdmp	false	URL Reputation: safe	unknown
http://multimetals.cfd	InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000000.sdmp	false		high
http://www.fontbureau.com	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.000000000000.sdmp	false		high
http://cps.letsencrypt.org	InstallUtil.exe, 00000012.00000002.593597181.0000000062F7000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.592820026.0000000006230000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.595628659.0000000006BF1000.00000004.00000001.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589226402.000000003279000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000012.00000002.589681230.00000000032B5000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://ns.adobe.cobj	noise.exe, 0000000D.00000003.513958247.00000000BA34000.00000004.00000800.00020000.000000000000.sdmp, noise.exe, 0000000D.00000002.553577663.000000000BA31000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	InstallUtil.exe, 00000012.00000002.574138944.000000002F11000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cnTFGZP	4EBE6@3.exe, 00000001.00000003.307529594.00000000C51D000.00000004.00000800.00020000.000000000000.sdmp, 4EBE6@3.exe, 00000001.00000003.307605500.00000000C51E000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.307461611.00000000C51C000.00000004.00000800.00020000.000000000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.tiro.como5p	4EBE6@3.exe, 00000001.00000003.308235544.00000000C524000.00000004.00000800.00020000.000000000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308050243.00000000C520000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308086430.00000000C520000.00000004.00000800.00020000.000000000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308116259.00000000C528000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308182391.00000000C523000.00000004.00000800.00020000.000000000000.sdmp, 4EBE6@3.exe, 00000001.00000003.308155481.00000000C522000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.carterandcone.comormll	4EBE6@3.exe, 00000001.00000003.308405539.00000000C4F3000.00000004.00000800.00020000.000000000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnt-it	4EBE6@3.exe, 00000001.00000003.307561212.00000000C500000.00000004.00000800.00020000.000000000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com/	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://ns.adobe.cobj=	noise.exe, 0000000D.00000003.362585268.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.3639777934.00000000BA34000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.362153601.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.364534093.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.364534093.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.364314645.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.434325843.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.362339951.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.363235158.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.3642865345.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.364132096.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.364684475.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.363031127.00000000BA38000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.361734419.00000000BA30000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.363500284.00000000BA38000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/	4EBE6@3.exe, 00000001.00000003.311250923.00000000C526000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	4EBE6@3.exe, 00000001.00000003.307561212.00000000C500000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.307605500.00000000C51E000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.307638553.00000000C51F000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.disig.sk/ca0f	InstallUtil.exe, 00000012.00000002.595246005.00000006B70000.00000004.00000001.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com.57	4EBE6@3.exe, 00000001.00000003.308050243.00000000C520000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	4EBE6@3.exe, 00000001.00000002.349782029.00000000D702000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobe.c/g=	noise.exe, 0000000D.00000003.363977934.00000000BA34000.00000004.00000800.00020000.00000000.sdmp, noise.exe, 0000000D.00000003.361734419.00000000BA30000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	4EBE6@3.exe, 00000001.00000003.311208678.00000000C526000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.311319625.00000000C526000.00000004.00000800.00020000.00000000.sdmp, 4EBE6@3.exe, 00000001.00000003.311250923.00000000C526000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn]	4EBE6@3.exe, 00000001.00000003.308405539.00000000C4F3000.00000004.00000800.00020000.00000000.sdmmp	false	Avira URL Cloud: safe	unknown
http://ns.ado/1	noise.exe, 0000000D.00000003.513958247.00000000BA34000.00000004.00000800.000200.00000000.sdmmp, noise.exe, 0000000D.0000002.553577663.00000000BA31000.0000004.00000800.00020000.00000000.sdmmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679195
Start date and time: 05/08/2022 11:56:52	2022-08-05 11:56:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4EBE6@3.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:	30
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@7/5@3/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14
- Excluded domains from analysis (whitelisted): www.bing.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target 4EBE6@3.exe, PID 400 because it is empty
- Not all processes were 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
11:58:36	API Interceptor	1x Sleep call for process: 4EBE6@3.exe modified
11:58:52	API Interceptor	214x Sleep call for process: noise.exe modified
12:00:04	API Interceptor	92x Sleep call for process: InstallUtil.exe modified
12:00:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Acrobat C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
12:00:18	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

 No context

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4EBE6@3.exe.log

Process:	C:\Users\user\Desktop\4EBE6@3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MgvjHK5HKXwYHKhQnoPtHoxHhAHKzvr3
MD5:	14823511A171BB647D0EAD502CCA1F8B
SHA1:	C93F72192AA9EDA3AD54C21FECCA44C11C544D59
SHA-256:	82F290E3FEAE38480488B265506CE7949AE3E86E9C8B6619E922EF44615FD28C
SHA-512:	AF9C14E0AF3A03FF518C8EC3688087879249C933519291A6F768500959A28C5E6EC4320BC98309F7DFD4CB30A4A5AAE29EECFAA6A391F4D881145504E4FBC40
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"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",0..3,"C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

Process:	C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
----------	---

File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	5.350971482944737
Encrypted:	false
SSDEEP:	24:MLiKNE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MeIH2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	CEE81B7EB08EE82CFE49E47B81B50D1A
SHA1:	4746C7068BD50E3309BFFDBE8983B8F27D834DFD
SHA-256:	B9A90255691E7C9D3CCBD27D00FC514DDD6087446D8DB03335CEF1B5634CC460
SHA-512:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEf93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AE477
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, 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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\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\fd1d8480152e0da9a60ad49c6d16a3b6d\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\fb219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

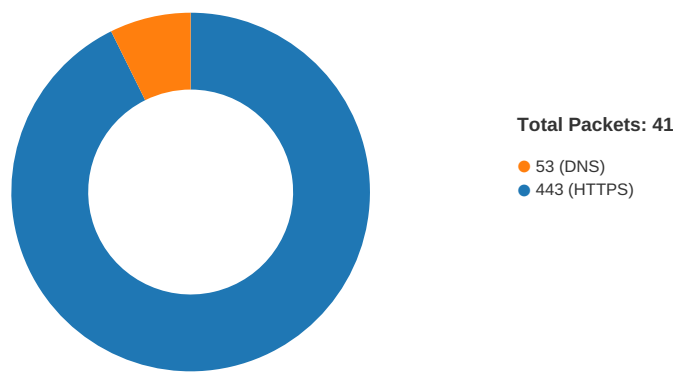
Process:	C:\Users\user\AppData\Local\Temp\noise.exe
----------	--

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MgvjHK5HKXwYHKhQnoPtHoxHhAHKzvr3

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:58:20.946193933 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:20.946221113 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:20.946324110 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:20.990619898 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:20.990653992 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.046631098 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.046761990 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.049889088 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.049900055 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.050126076 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.103869915 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.466084957 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.507370949 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.631510973 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.631634951 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.631748915 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.631772041 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.631809950 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.631877899 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.631896019 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.632299900 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.632366896 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.632389069 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.632416964 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.632555962 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.633527994 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.634821892 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.634882927 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.635107040 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.635143042 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.635399103 CEST	49734	443	192.168.2.3	142.250.185.196

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:58:21.636231899 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.648201942 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.648273945 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.648638964 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.648684025 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.648977995 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.648988008 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.649019003 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.649725914 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.649801016 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.649837017 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.650063038 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.651633024 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.652328968 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.652436972 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.652435064 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.652481079 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.653714895 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.654243946 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.654864073 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.654921055 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.654978991 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.655013084 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.655215025 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.656085968 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.657128096 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.657234907 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.657285929 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.657305956 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.657419920 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.658236980 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.659396887 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.659507036 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.660465956 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.660486937 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.660578012 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.660608053 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.660624981 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.660710096 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.661531925 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.661755085 CEST	443	49734	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:21.661870956 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:21.665785074 CEST	49734	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.084156036 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.084219933 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:38.084332943 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.184114933 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.184163094 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:38.229578018 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:38.229705095 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.245520115 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:38.245553970 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:38.246011019 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:38.366739988 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:39.098844051 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:39.139457941 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.268588066 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.268686056 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.268769979 CEST	443	49744	142.250.185.196	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:58:39.268841982 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.269032955 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:39.269048929 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.269361973 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.269691944 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:39.269706964 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.270729065 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.271147966 CEST	49744	443	192.168.2.3	142.250.185.196
Aug 5, 2022 11:58:39.271167994 CEST	443	49744	142.250.185.196	192.168.2.3
Aug 5, 2022 11:58:39.271718979 CEST	443	49744	142.250.185.196	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:58:20.907394886 CEST	64851	53	192.168.2.3	8.8.8.8
Aug 5, 2022 11:58:20.924711943 CEST	53	64851	8.8.8.8	192.168.2.3
Aug 5, 2022 11:58:38.003500938 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 5, 2022 11:58:38.020128965 CEST	53	56417	8.8.8.8	192.168.2.3
Aug 5, 2022 12:00:24.309473991 CEST	65266	53	192.168.2.3	8.8.8.8
Aug 5, 2022 12:00:24.481308937 CEST	53	65266	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:58:20.907394886 CEST	192.168.2.3	8.8.8.8	0x58c1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:58:38.003500938 CEST	192.168.2.3	8.8.8.8	0xb8a6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:00:24.309473991 CEST	192.168.2.3	8.8.8.8	0x54fa	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
Aug 5, 2022 11:58:20.924711943 CEST	8.8.8.8	192.168.2.3	0x58c1	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 5, 2022 11:58:38.020128965 CEST	8.8.8.8	192.168.2.3	0xb8a6	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 5, 2022 12:00:24.481308937 CEST	8.8.8.8	192.168.2.3	0x54fa	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	192.168.2.3	49734	142.250.185.196	443	C:\Users\user\Desktop\4EBE6@3.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 09:58:21 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: AEC=AakniGMECP0zr5GPVaVTjAqHZbSwe5it9w4XpzpZ0Nnf5kJ9LjiQ-76L5Fw; expires=Wed, 01-Feb-2023 09:58:21 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=Iax Set-Cookie: __Secure-ENID=6.SE=Z7nXl_KjcWxIEJ0AXNx1pM3SkqW0pkfcmHFqayrTNx1PTkHyepKFAnZC_V6TAnY0QgWZTVOBxRBQZmlyhj_5R7NmTzdXeMdN8K0o953x6LYlaRNJTMvZGRRFyRBkNHNiQfpyYUPFzoRKNwOYCdGdc87esXCufsh7uiOuY_EMSg8; expires=Tue, 05-Sep-2023 02:16:39 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=Iax Set-Cookie: CONSENT=PENDING+816; expires=Sun, 04-Aug-2024 09:58:21 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
2022-08-05 09:58:21 UTC	1	IN	Data Raw: 35 36 32 62 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 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 Data Ascii: 562b<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
2022-08-05 09:58:21 UTC	1	IN	Data Raw: 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 51 77 6d 6a 31 36 33 65 63 57 4c 59 67 50 5f 36 33 45 67 67 72 67 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 3d 7b 6b 45 49 3a 27 76 65 6e 73 59 74 57 32 48 37 53 68 69 4c 4d 50 35 73 57 54 6b 41 45 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 31 37 31 30 2c 34 33 34 39 2c 32 30 36 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 36 2c 35 2c Data Ascii: =/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="Qwmj163ecWLYgP_63Eggrg">(function(){window.google={kEl:'vensYtW2H7ShiLMP5sWTkAE',kEXPi:'0,1302536,56873,1710,4349,206,4804,2316,383,246,5,
2022-08-05 09:58:21 UTC	2	IN	Data Raw: 35 39 2c 31 33 35 38 2c 31 32 32 32 30 2c 33 34 30 36 2c 37 31 38 2c 36 34 35 35 2c 31 33 36 30 39 39 36 27 2c 6b 42 4c 3a 27 6c 53 78 70 27 7d 3b 67 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 64 65 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e Data Ascii: 59,1358,12220,3406,718,6455,1360996',kBL:'!Sxp';google.sn='webhp';google.kHL='de'}});(function(){var f=th is self;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute) !(b=a.getAttribute("eid")));a=a.parentNode;return b h}function m(a){for(var b=n
2022-08-05 09:58:21 UTC	3	IN	Data Raw: 5b 61 5d 2c 62 2c 63 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 Data Ascii: [a],b,c));google.loadAll=function(a,b){google.lq.push([a,b]);google.bx=!1;google.lx=function(){}}.call(t his);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a .getAttribute("data-submit
2022-08-05 09:58:21 UTC	5	IN	Data Raw: 73 6f 6c 75 74 65 3b 74 6f 70 3a 33 30 70 78 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 7 0 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 3 9 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 Data Ascii: solute;top:30px;width:100%}.gbtc{position:absolute;visibility:hidden}#gbz .gbtc{right:0}#gbg .gbtc{left:0 }gbx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-in dex:999;top:-999px;visibili
2022-08-05 09:58:21 UTC	6	IN	Data Raw: 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 7 9 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 Data Ascii: list-style:none;margin:0;padding:0}.gbmc{background:ffff;padding:10px 0;position:relative;z-index:2;zoom:1}. gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*d isplay:inline}.gbto{box-sha

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	7	IN	Data Raw: 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 Data Ascii: ackground-color:#4c4c4c;background-image:none;_background-image:none;_background-position:0 -102px; background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm(min-width:99%).gbz0l .gbtb2[border-top-color:#dd4b39!important]#gb
2022-08-05 09:58:21 UTC	8	IN	Data Raw: 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 Data Ascii: .gbmt:visited,.gbnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:v
2022-08-05 09:58:21 UTC	10	IN	Data Raw: 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 6b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 Data Ascii:)box-shadow:0 2px 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:"\0A\0A";white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gb
2022-08-05 09:58:21 UTC	11	IN	Data Raw: 67 3a 31 30 70 78 20 32 30 70 78 20 30 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 62 6d 70 61 6c 61 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 7d 23 67 62 6d 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f Data Ascii: g:10px 20px 0;white-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-blo
2022-08-05 09:58:21 UTC	12	IN	Data Raw: 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 2d 6e 6f 2d 66 6f 63 75 73 3a 66 6f 63 75 73 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 Data Ascii: a(0,0,0,.1)}.gbqfb-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1p
2022-08-05 09:58:21 UTC	14	IN	Data Raw: 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 Data Ascii: 8);background-image:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(to top,#4d90fe,#357ae8)}.gbqfb:active{background
2022-08-05 09:58:21 UTC	15	IN	Data Raw: 31 66 31 66 31 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 Data Ascii: 1f1f1);background-image:linear-gradient(to top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr=#f8f8f8,EndColorStr=#f1f1f1)}.gbqfbb{background-color:ffff;background-image:-webkit-gradient(linear,left top,left bottom,from(
2022-08-05 09:58:21 UTC	16	IN	Data Raw: 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 2e 31 29 3b 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 61 3a 61 63 74 69 76 65 2c 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 Data Ascii: x 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}#gbmpa

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	17	IN	Data Raw: 2e 33 29 3b 74 6f 70 3a 30 7d 2e 67 62 73 62 20 2e 67 62 73 62 62 7b 2d 77 65 62 6b 69 74 2d 6d 61 73 6b 2d 62 6f 78 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 2e 35 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 38 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 2b 62 7f 67 75 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c Data Ascii: .3);top:0}.gbsb .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),
2022-08-05 09:58:21 UTC	19	IN	Data Raw: 69 6e 65 7d 2e 66 6c 20 61 7b 63 6f 6c 6f 72 3a 23 31 35 35 38 64 36 7d 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 34 62 31 31 61 38 7d 2e 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b Data Ascii: ine).fl a{color:#1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadedce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block
2022-08-05 09:58:21 UTC	20	IN	Data Raw: 66 26 26 67 3d 3d 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 26 26 28 66 3d 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 6f 75 74 65 72 48 54 4d 4c 2e 73 70 6c 69 74 28 22 5c 6e 22 29 5b 66 5d 2c 63 2b 3d 22 26 63 61 64 3d 22 2b 62 28 66 3f 66 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 33 30 30 29 3a 22 4e 6f 20 73 63 72 69 70 74 20 66 6f 75 6e 64 2e 22 29 29 29 3b 63 2b 3d 22 26 6a 73 65 6c 3d 22 2b 65 3b 66 6f 72 28 76 61 72 20 75 20 69 6e 20 64 29 63 2b 3d 22 26 22 2c 63 2b 3d 62 28 65 6d 73 67 3d 22 2b 62 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b 63 3d 63 2b 22 26 6a 73 73 74 3d 22 2b 62 28 61 2e Data Ascii: f&g===window.location.href&&(f=document.documentElement.outerHTML.split("\n")[f],c+="-"&cad="+b(f?f.substring(0,300):"No script found.")).c+= "&jsel="+e;for(var u in d)c+="-"&c+=b(u),c+="-"&c+=b(d[u]);c=c+"&msg="+b(a.name+": "+a.message);c=c+"&jsst="+b(a.
2022-08-05 09:58:21 UTC	21	IN	Data Raw: 64 2c 63 29 3b 65 6c 73 65 7b 76 61 72 20 66 3d 61 5b 64 5d 3b 61 5b 64 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6b 3d 66 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 2c 6d 3d 63 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 3b 72 65 74 75 72 6e 20 76 6f 69 64 20 30 3d 3d 6b 3f 6d 3a 76 6f 69 64 20 30 3d 3d 6d 3f 6b 3a 6d 26 26 6b 7d 7d 7d 61 72 20 64 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 67 2e 62 76 2e 6d 3d 3d 61 7d 7d 2c 65 61 3d 64 61 28 31 29 2c 66 61 3d 64 61 28 32 29 3b 70 28 22 73 62 22 2c 65 61 29 3b 70 28 22 6b 6e 22 2c 66 61 29 3b 68 2e 61 3d 5f 74 76 76 3b 68 2e 62 3d 5f 74 76 66 3b 68 2e 63 3d 5f 74 76 6e 3b 68 Data Ascii: d,c);else{var f=a[d];a[d]=function(){var k=f.apply(this,arguments),m=c.apply(this,arguments);return void 0==k?m:void 0==m?k:m&&k}}var da=function(a){return function(){return g.bv.m=-a}},ea=da(1),fa=da(2);p(("kn",fa);h.a=_twv;h.b=_tvf;h.c=_tvn;h
2022-08-05 09:58:21 UTC	22	IN	Data Raw: 65 34 0d 0a 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 7d 2c 75 61 3d 6e 75 6c 6c 2c 76 61 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 75 61 3d 61 7d 2c 73 61 0d 0a Data Ascii: e4head")[0]].appendChild(c)),D=function(a){for(var b=0,c;(c=w[b])&c[0]!=a;++b);c[c[1]].l c[1].l c[1].s c[1].s=!0,sa(2,a),c[1].url&&a[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
2022-08-05 09:58:21 UTC	22	IN	Data Raw: 36 38 66 32 0d 0a 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 75 61 29 7b 61 3d 7b 74 3a 61 2c 62 3a 62 7d 3b 69 66 28 63 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 63 29 61 5b 64 5d 3d 63 5b 64 5d 3b 74 72 79 7b 75 61 28 61 29 7d 63 61 74 63 68 28 66 29 7b 7d 7d 7d 3b 70 28 22 6d 64 63 22 2c 76 29 3b 70 28 22 6d 64 69 22 2c 6c 61 29 3b 70 28 22 62 6e 63 22 2c 77 29 3b 70 28 22 71 47 43 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 42 29 3b 70 28 22 71 64 22 2c 78 29 3b 70 28 22 6c 62 22 2c 44 29 3b 70 28 22 6d 63 66 22 2c 70 61 29 3b 70 28 22 62 63 66 22 2c 6f 61 29 3b 70 28 22 61 71 22 2c 41 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 71 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 73 61 29 3b 69 Data Ascii: 68f2=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("mdi",la);p("bnc",w);p("qGC",ta);p("qm",B);p("qd",x);p("lb",D);p("mcf",pa);p("bcf",oa);p("aq",A);p("mdd",");p("has",qa);p("trh",va);p("tev",sa);i
2022-08-05 09:58:21 UTC	24	IN	Data Raw: 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 7d 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 6f 6f 6f 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 2c 22 26 6a 65 78 70 69 64 3d 22 2c 64 28 22 32 38 38 33 34 22 29 2c 22 26 73 72 63 70 67 3d 22 2c 64 28 22 70 72 6f 70 3d 31 22 29 2c 22 26 6a 73 72 3d 22 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 46 61 29 2c 22 26 6f 67 65 76 3d 22 2c 64 28 22 76 65 6e 73 59 6f 62 2d 49 4b 57 41 69 4c 4d 50 6d 66 53 43 71 41 51 22 29 2c 22 26 6f 67 66 3d 22 2c 67 2e 62 76 2e 66 2c 22 26 6f 67 72 70 3d 22 2c 64 28 Data Ascii: {try{if(1>Ga){Ga++;var c=a;b=b {};var d=encodeURIComponent,f="//www.google.com/gen_204?atyp=i&zx=",(new Date).getTime(),"&jexpid=",d("28834"),"&srcpg=",d("prop=1"),"&jsr=",Math.round(1/Fa),"&ogev=",d("vensYob-IKWaiLMPmFSCqAQ"),"&ogf=",g.bv.f,"&ogrp=",d(
2022-08-05 09:58:21 UTC	25	IN	Data Raw: 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 32 63 74 44 37 74 74 6f 2d 2d 70 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 74 50 4e 4d 68 44 2d 72 38 67 5a 48 5a 58 56 68 6e 56 57 61 43 30 46 53 69 36 6f 67 22 5d 3b 4b 61 26 26 61 2e 70 75 73 68 28 22 3f 68 6f 73 74 3d 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 26 62 75 73 74 3d 6f 67 2e 6f 67 32 2e 65 6e 5f 55 53 2e 62 6d 48 52 47 50 74 37 41 4d 77 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 72 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 4a 29 3b 70 28 22 63 72 22 2c 4b 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 4a 3b Data Ascii: https://www.gstatic.com","/og/_/js/d=1/k=","og.og2.en_US.2ctD7tto-pA.O","/rt=j/m=","a","/rs=","AA2YrTiPNMhD-r8gZXhVhnVWaC0FSi6og"];Ka&&a.push("?host=www.gstatic.com&bust=og.og2.en_US.bmHRGP7AMw.DU")):a=a.join("");ra(a));p("ca",J);p("cr",K);p("cc",H);h.k=J;

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	26	IN	Data Raw: 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 74 42 79 49 64 28 6e 29 3b 6c 26 26 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 4b 28 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 2 2 67 62 74 6f 22 29 7d 7d 7d 24 61 28 66 29 26 26 61 62 28 66 29 3b 4f 3d 64 3b 4a 28 6b 2c 22 67 62 74 6f 22 29 7d 7d 7d 7d 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 74 67 28 61 2c 62 2c 21 30 29 7d 29 3b 62 62 28 61 29 7d 63 61 74 63 68 28 71 29 7b 72 28 71 2c 22 73 62 22 2c 22 74 67 22 29 7d 7d 2c Data Ascii: getElementById(O);if(m&&m.getAttribute){var n=m.getAttribute("aria-owner");if(n.length){var l=document.getElementByld(n);l&&l.parentNode&&K(l.parentNode,"gbto")}}}\$a(f)&&ab(f);O=d;J(k,"gbto")}}}}B(function(){g.tg(a,b,l,0));bb(a) }catch(q){r(q,"sb","tg")}}, Data Raw: 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 67 24 7d 63 61 74 63 68 28 45 62 29 7b 72 28 45 62 2c 22 73 62 22 2c 22 61 6c 22 29 7d 7d 2c 66 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 6 6 6f 72 28 76 61 72 20 63 3d 62 2e 6c 65 6e 67 74 68 2c 0a 64 3d 30 3b 64 3c 63 3b 64 2b 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 Data Ascii: t gbmh";y.appendChild(z);k.insertBefore(y,k.childNodes[0])}g.addHover&&g.addHover(a)}else k.append Child(m)}catch(Eb){r(Eb,"sb","al")}},fb=function(a,b){for(var c=b.length,d=0;d<c;d++)if(H(a,b[d]))return 0;return 1},hb =function(a,b,c){gb(a,b,c)},ib=funct Data Raw: 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 64 65 73 5b 62 5d 3b 62 2b 2b 29 69 66 28 48 28 63 2c 22 67 62 6d 73 67 22 29 72 65 74 75 72 6e 20 63 7d 2c 50 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 71 62 26 26 77 69 6e 64 6f 77 2e 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 71 62 29 7d 2c 75 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 22 69 6e 6e 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 6 1 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e Data Ascii: !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.childNodes[b];b++)if(H(c,"gbmsg"))return c},P=function(){qb&&window.clearTimeout(qb)},ub=function(a){var b="inner "+a;a="offset"+a;return window[b]?win Data Raw: 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 6c 43 62 29 3b 68 2e 61 28 22 31 22 29 26 26 70 28 22 6c 50 57 46 22 2c 43 62 29 7d 3b 77 69 6e 64 6f 77 2e 5f 5f 50 56 54 3d 22 3b 69 66 28 68 2e 61 28 22 31 22 29 26 26 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 44 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 62 28 66 75 6e 63 74 69 6f 6e 2 8 29 7b 41 28 22 70 77 22 2c 61 29 3b 44 28 22 70 77 22 29 7d 29 7d 3b 70 28 22 6c 50 57 22 2c 44 62 29 3b 77 2e 70 75 73 68 28 5b 22 70 77 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 Data Ascii: v.gc=Bb;var Cb=function(a){window.googleapis&&window.iframe?a&&a():(a&&ta(a),D("gc"))};p("IGC",Cb);h.a("1")&&p("IPWF",Cb);window.__PVT="";if(h.a("1")&&h.a("1")){var Db=function(a){Cb(function(){A("pw"),D("pw")});p ("IPW",Db);w.push(["pw",{url:"/ssl.g Data Raw: 36 34 34 33 35 35 39 35 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 37 30 36 2e 30 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 2e 61 28 22 22 29 26 26 28 79 7c 3d 32 29 3b 68 2e 61 28 22 22 29 26 26 28 79 7c 3d 34 29 3b 61 3d 5b 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 66 2c 22 26 6f 67 65 3d 22 2c 61 2c 22 26 6f 67 65 78 3d 22 2c 6b 2c 22 26 6f 67 65 76 3d 22 2c 6d 2c 22 26 6f 67 66 3d 22 2c 6c 2c 22 26 6f 67 70 3d 22 2c 71 2c 22 26 6f 67 72 70 3d 22 2c 6e 2c 22 26 6f Data Ascii: 64435595.0"),U="&oggv="+d("es_plusone_gc_20220706.0_p0"),l=d("com"),V=d("de"),W=d("DEU");var y=0;h .a("")&&(y =1);h.a("")&&(y =2);h.a("")&&(y =4);a=["/www.google.com/gen_204?atyp=i&zx=",f,"&oge=",a,"&ogex=",k ,"&ogev=",m,"&ogf=",l,"&ogp=",q,"&ogrp=",n,"&o Data Raw: 3b 6d 62 28 22 67 62 64 3a 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 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 28 22 31 22 29 2c 6d 67 3a 22 25 31 24 73 20 28 64 65 6c 65 67 69 65 72 74 29 22 2c 6d 64 3a 22 25 31 24 73 20 28 53 74 61 6e 64 61 72 64 29 22 2c 6d 68 3a 22 32 32 30 22 2c 73 3a 22 31 22 2c 70 70 3a 5a 62 2c 70 70 6c 3a 68 2e 61 28 22 22 29 2c 70 70 61 3a 68 2e 61 28 22 22 29 2c 0a 70 70 6d 3a 22 47 6f 6f 67 6c 65 2b 20 53 65 69 74 65 22 7d 3b 76 2e 70 Data Ascii: :mb("gbd4",Ub);if(h.a("")){var ac=[d:h.a(""),e:"",sanw:h.a(""),p:"https://lh3.googleusercontent.com/ogw/default-user=s96",cp:"1",xp:h.a("1"),mg:"%1\$s (delegiert)",md:"%1\$s (Standard)",mh:"220",s:"1",pp:Zb,ppl:h.a(""),ppa:h.a("") ,ppm:"Google+ Seite"];v.p Data Raw: 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 66 20 61 2e 6c 6f 61 64 7d 2c 6d 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 74 72 79 7b 6a 63 28 64 6f 63 75 6d 65 6e 74 29 7c 7c 28 64 7c 7c 28 62 3d 22 6f 67 2d 75 70 2d 22 2b 62 29 2c 6b 63 28 29 3f 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 73 65 74 49 74 65 6d 28 62 2c 63 29 3a 6c 63 28 61 29 26 26 28 61 2e 73 65 74 41 74 74 72 6 9 62 75 74 65 28 62 2c 63 29 2c 61 2e 73 61 76 65 28 61 2e 69 64 Data Ascii: "!==typeof e.localStorage}catch(a){return!1}},lc=function(a){return a&&a.style&&a.style.behavior&&"undefined" !=typeof a.load},mc=function(a,b,c,d){try{j(c(document))}([d]([b="og-up-"+b),kc()?)e.localStorage.setItem(b,c):lc(a)&&(a.se tAttribute(b,c),a.save(a.id Data Raw: 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 26 26 43 26 26 43 28 6c 5b 31 5d 2e 6c 69 62 73 29 29 3b 6d 3c 6b 2e 6c 65 6e 67 74 68 26 26 73 65 74 54 69 6d 65 6f 75 74 28 61 2c 30 29 7d 66 75 6e 63 74 69 6f 6e 20 62 28 29 7b 30 3c 66 2d 2d 3f 73 65 74 54 69 6d 65 6f 75 74 28 62 2c 30 29 3a 61 28 29 7d 76 61 72 20 63 3d 68 2e 61 28 22 31 22 29 2c 64 3d 68 2e 61 28 22 22 29 2c 66 3d 33 2c 6b 3d 77 2c 6d 3d 30 2c 6e 3d 77 69 6e 64 6f 77 2e 67 62 61 72 4f 6e 52 65 Data Ascii: c(){function a(){for(var l;(l=k[m++]!)&&"m"!=[0]&&![1],auto);l&&(sa([2,[0],[1],url&&ra([1],url,[0],[1],libs&&C &&C([1],libs));m<k.length&&setTimeout(a,0))function b(){0<!--?setTimeout(b,0):a()}var c=h.a("1"),d=h.a(""),f=3,k=w,m=0, n=window.gbarOnRe
2022-08-05 09:58:21 UTC	28	IN	Data Raw: 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 67 24 7d 63 61 74 63 68 28 45 62 29 7b 72 28 45 62 2c 22 73 62 22 2c 22 61 6c 22 29 7d 7d 2c 66 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 6 6 6f 72 28 76 61 72 20 63 3d 62 2e 6c 65 6e 67 74 68 2c 0a 64 3d 30 3b 64 3c 63 3b 64 2b 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 Data Ascii: t gbmh";y.appendChild(z);k.insertBefore(y,k.childNodes[0])}g.addHover&&g.addHover(a)}else k.append Child(m)}catch(Eb){r(Eb,"sb","al")}},fb=function(a,b){for(var c=b.length,d=0;d<c;d++)if(H(a,b[d]))return 0;return 1},hb =function(a,b,c){gb(a,b,c)},ib=funct Data Raw: 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 64 65 73 5b 62 5d 3b 62 2b 2b 29 69 66 28 48 28 63 2c 22 67 62 6d 73 67 22 29 72 65 74 75 72 6e 20 63 7d 2c 50 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 71 62 26 26 77 69 6e 64 6f 77 2e 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 71 62 29 7d 2c 75 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 22 69 6e 6e 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 6 1 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e Data Ascii: !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.childNodes[b];b++)if(H(c,"gbmsg"))return c},P=function(){qb&&window.clearTimeout(qb)},ub=function(a){var b="inner "+a;a="offset"+a;return window[b]?win Data Raw: 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 6c 43 62 29 3b 68 2e 61 28 22 31 22 29 26 26 70 28 22 6c 50 57 46 22 2c 43 62 29 7d 3b 77 69 6e 64 6f 77 2e 5f 5f 50 56 54 3d 22 3b 69 66 28 68 2e 61 28 22 31 22 29 26 26 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 44 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 43 62 28 66 75 6e 63 74 69 6f 6e 2 8 29 7b 41 28 22 70 77 22 2c 61 29 3b 44 28 22 70 77 22 29 7d 29 7d 3b 70 28 22 6c 50 57 22 2c 44 62 29 3b 77 2e 70 75 73 68 28 5b 22 70 77 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 Data Ascii: v.gc=Bb;var Cb=function(a){window.googleapis&&window.iframe?a&&a():(a&&ta(a),D("gc"))};p("IGC",Cb);h.a("1")&&p("IPWF",Cb);window.__PVT="";if(h.a("1")&&h.a("1")){var Db=function(a){Cb(function(){A("pw"),D("pw")});p ("IPW",Db);w.push(["pw",{url:"/ssl.g Data Raw: 36 34 34 33 35 35 39 35 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 37 30 36 2e 30 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 2e 61 28 22 22 29 26 26 28 79 7c 3d 32 29 3b 68 2e 61 28 22 22 29 26 26 28 79 7c 3d 34 29 3b 61 3d 5b 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 66 2c 22 26 6f 67 65 3d 22 2c 61 2c 22 26 6f 67 65 78 3d 22 2c 6b 2c 22 26 6f 67 65 76 3d 22 2c 6d 2c 22 26 6f 67 66 3d 22 2c 6c 2c 22 26 6f 67 70 3d 22 2c 71 2c 22 26 6f 67 72 70 3d 22 2c 6e 2c 22 26 6f Data Ascii: 64435595.0"),U="&oggv="+d("es_plusone_gc_20220706.0_p0"),l=d("com"),V=d("de"),W=d("DEU");var y=0;h .a("")&&(y =1);h.a("")&&(y =2);h.a("")&&(y =4);a=["/www.google.com/gen_204?atyp=i&zx=",f,"&oge=",a,"&ogex=",k ,"&ogev=",m,"&ogf=",l,"&ogp=",q,"&ogrp=",n,"&o Data Raw: 3b 6d 62 28 22 67 62 64 3a 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 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 28 22 31 22 29 2c 6d 67 3a 22 25 31 24 73 20 28 64 65 6c 65 67 69 65 72 74 29 22 2c 6d 64 3a 22 25 31 24 73 20 28 53 74 61 6e 64 61 72 64 29 22 2c 6d 68 3a 22 32 32 30 22 2c 73 3a 22 31 22 2c 70 70 3a 5a 62 2c 70 70 6c 3a 68 2e 61 28 22 22 29 2c 70 70 61 3a 68 2e 61 28 22 22 29 2c 0a 70 70 6d 3a 22 47 6f 6f 67 6c 65 2b 20 53 65 69 74 65 22 7d 3b 76 2e 70 Data Ascii: :mb("gbd4",Ub);if(h.a("")){var ac=[d:h.a(""),e:"",sanw:h.a(""),p:"https://lh3.googleusercontent.com/ogw/default-user=s96",cp:"1",xp:h.a("1"),mg:"%1\$s (delegiert)",md:"%1\$s (Standard)",mh:"220",s:"1",pp:Zb,ppl:h.a(""),ppa:h.a("") ,ppm:"Google+ Seite"];v.p Data Raw: 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 66 20 61 2e 6c 6f 61 64 7d 2c 6d 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 74 72 79 7b 6a 63 28 64 6f 63 75 6d 65 6e 74 29 7c 7c 28 64 7c 7c 28 62 3d 22 6f 67 2d 75 70 2d 22 2b 62 29 2c 6b 63 28 29 3f 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 73 65 74 49 74 65 6d 28 62

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	36	IN	Data Raw: 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 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 5f 22 2b 61 29 3b 62 66 2e 6c 28 62 2c 68 2e 74 65 73 74 28 62 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 3b 63 26 26 66 2 e 6b 28 63 2c 68 2e 74 65 73 74 28 63 2e 63 6c 61 73 73 4e 61 6d Data Ascii: che-2.0*/var d=window.gbar.i.i;var e=window.gbar;var f=e.i;var g=f.c("1",0),h=Abgbmtlb,k=function(a){try{var b=document.getElementById("gb_"+g),c=document.getElementById("gb_"+a);b&&f.l(b,h.test(b.className))?gbm0l": "gbz0l";c&&f.k(c,h.test(c.classNam
2022-08-05 09:58:21 UTC	38	IN	Data Raw: 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 67 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7 d 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 Data Ascii: "+h[0]);for(var l;h.length&&(!=h.shift());)h.length void 0===g?k[l]&&k[l]==Object.prototype[l]?k[l]:k[l]={:k[l]=g ;}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"","cfg.init"});})();(function(){try{/* Copyright The Closure Library Autho
2022-08-05 09:58:21 UTC	39	IN	Data Raw: 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 6c 65 2e 63 6f 6d 2f 3f 68 6c 3d 64 65 26 74 61 62 3d 77 38 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 50 6c 61 79 3c 2f 73 70 61 6e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 33 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 Data Ascii: n class=gbtb2>Maps<li class=gbt>Play<li cl ass=gbt><a class=gbzt id=gb_36 href="https://ww
2022-08-05 09:58:21 UTC	40	IN	Data Raw: 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 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 35 31 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 74 72 61 6e 73 6c 61 74 65 2e 67 6f 6f 67 6c 65 2e 64 65 2f 3f 68 6c 3d 64 65 26 74 61 62 3d 77 54 22 3e dc 62 65 72 73 65 74 7a 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 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 31 30 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f Data Ascii: bmtc>Kalender<li class=gbmtc>bersetzer<li cl ass=gbmtc><a class=gbmt id=gb_10 href="https:/
2022-08-05 09:58:21 UTC	42	IN	Data Raw: 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 67 3e 3c 68 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 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 74 61 72 67 65 74 3d 5f 74 6f 70 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 63 63 6f 75 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 53 65 72 76 69 63 65 4c 6f 67 69 6e 3f 68 6c 3d 64 65 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 26 65 63 3d 47 41 5a 41 41 51 Data Ascii: iv></div></div></div><div id=gbg><h2 class=gbxx>Account Options</h2><ol class=gbtc><li class=gbt><a target=_top href="https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ
2022-08-05 09:58:21 UTC	43	IN	Data Raw: 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 61 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 69 6d 67 20 61 6c 74 3d 22 47 6f 6f 67 6c 65 22 20 68 65 69 67 68 74 3d 22 39 32 22 20 73 72 63 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 2f 31 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 77 68 69 74 65 5f 62 61 63 6b 67 72 6f 75 6e 64 5f 63 6f 6c 6f 72 5f 32 37 32 78 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 32 38 70 78 20 30 21 31 34 70 78 22 20 77 69 64 74 68 3d 22 32 37 32 22 20 69 64 3d 22 68 70 6c 6f 67 6f 22 3e 3c 62 72 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 66 Data Ascii: lp()</script></div></div><center><br clear="all" id="lgpd"><div id="lga">

</div><f
2022-08-05 09:58:21 UTC	44	IN	Data Raw: 6f 70 2e 6c 6f 63 61 74 69 6f 6e 6c 3d 27 2f 64 6f 6f 64 6c 65 73 2f 27 3b 7d 3b 7d 29 28 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 69 6e 70 75 74 20 76 61 6c 75 65 3d 22 41 4a 69 4b 30 65 38 41 41 41 41 59 75 7a 33 7a 54 4d 71 5a 5a 39 2d 70 31 35 6c 52 7a 57 49 79 66 72 5f 63 31 4e 63 4b 70 59 38 22 20 6e 61 6d 65 3d 22 69 66 6c 73 69 67 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 74 64 3e 3c 74 64 20 63 6c 61 73 73 3d 22 66 6c 20 73 62 6c 63 22 20 61 6c 69 67 6e 3d 22 6c 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 76 61 6e 63 65 64 5f 73 65 61 72 63 68 3f 68 6c 3d 64 65 26 61 6d 70 3b 61 75 74 68 75 73 65 72 3d 30 22 3e 45 72 77 65 69 Data Ascii: op.location="/doodles/");})();</script><input value="AJiK0e8AAAAAYuz3TmqZ9p-15IRzWlyfr_c1NcKpY8" name="iflsig" type="hidden"></td><td class="fl sbcl" align="left" nowrap="" width="25%">Erwei
2022-08-05 09:58:21 UTC	45	IN	Data Raw: 43 43 6b 31 69 59 30 4c 6e 58 34 44 66 72 6f 58 67 33 5a 6a 43 6c 71 51 25 33 44 22 3e 47 6f 6f 67 6c 65 2e 64 65 3c 2f 61 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 70 74 3b 63 6f 6c 6f 72 3a 23 37 30 37 35 37 61 22 3e 26 63 6f 70 79 3b 20 32 30 32 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 64 65 2f 70 6f 6c 69 63 69 65 73 2f 70 72 69 76 61 63 73 79 2f 32 3e 44 61 74 65 6e 73 63 68 75 74 7a 65 72 6b 6c e4 72 75 6e 67 3c 2f 61 3e 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 64 65 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 4e 75 74 7a 75 6e 67 73 62 65 64 69 6e 67 75 6e 67 65 6e 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 Data Ascii: CCK1iYOLnX4DfroXg3ZClqQ%3D">Google.de</div></div><p style="font-size:8pt;color:#70757a">&copy; 2022 - Datenschutzerklrung - Nutzungsbedin gungen</p></center><scrip

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:21 UTC	47	IN	Data Raw: 6f 61 64 26 26 67 6f 6f 67 6c 65 2e 74 69 63 6b 26 26 67 6f 6f 67 6c 65 2e 74 69 63 6b 28 22 6c 6f 61 64 22 2c 22 78 6a 73 6c 73 22 29 3b 76 61 72 20 62 3d 64 6f 63 75 6d 65 6e 74 3b 76 61 72 20 63 3d 22 53 43 52 49 50 54 22 3b 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 22 3d 3d 3d 62 2e 63 6f 6e 74 65 6e 74 54 79 70 65 26 26 28 63 3d 63 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 3b 63 3d 62 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 63 29 3b 69 66 28 76 6f 69 64 20 30 3d 3d 3d 67 29 7b 62 3d 6e 75 6c 6c 3b 76 61 72 20 6b 3d 64 2e 74 72 75 73 74 65 64 54 79 70 65 73 3b 69 66 28 6b 26 26 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 29 7b 74 72 79 7b 62 3d 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 28 22 67 6f 6f 67 23 68 74 6d 6c 22 Data Ascii: oad&&google.tick&&google.tick("load","xjsls");var b=document;var c="SCRIPT";"application/xhtml+xml" ===b.contentType&&(c=c.toLowerCase());c=b.createElement(c);if(void 0===g){b=null;var k=d.trustedTypes;if(k&&k.createPolicy){try{b=k.createPolicy("goog#html"
2022-08-05 09:58:21 UTC	48	IN	Data Raw: 78 32 32 6a 73 6f 6e 70 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6c 6d 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6d 73 67 73 5c 78 32 32 3a 7b 5c 78 32 32 63 69 62 6c 5c 78 32 32 3a 5c 78 32 32 53 75 63 68 65 20 6c f6 73 63 68 65 6e 5c 78 32 32 2c 5c 78 32 32 64 79 6d 5c 78 32 32 3a 5c 78 32 32 4d 65 69 6e 74 65 73 74 20 64 75 3a 5c 78 32 32 2c 5c 78 32 32 6c 63 6b 79 5c 78 32 32 3a 5c 78 32 32 41 75 66 20 67 75 74 20 47 6c fc 63 6b 21 5c 78 32 32 2c 5c 7 8 32 32 6c 6d 6c 5c 78 32 32 3a 5c 78 32 32 57 65 69 74 65 72 65 20 49 6e 66 6f 72 6d 61 74 69 6f 6e 65 6e 5c 78 32 32 2c 5c 78 32 32 6f 73 6b 74 5c 78 32 32 3a 5c 78 32 32 45 69 6e 67 61 62 65 74 6f 6f 6c 73 5c 78 32 32 2c 5c 78 32 32 70 73 72 63 5c 78 32 32 3a 5c 78 32 32 44 69 65 73 65 20 53 75 63 68 Data Ascii: x22jsonplx22:true,x22lmplx22:true,x22msgslx22:{x22ciblplx22:x22Suche Ischenlx22,x22dymplx22:x22 Meintest du:x22,x22lckylx22:x22Auf gut Glck!lx22,x22lmplx22:x22Weitere Informationenlx22,x22osktx22:x2 2Eingabetoolsx22,x22psrcx22:x22Diese Such
2022-08-05 09:58:21 UTC	49	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	142.250.185.196	443	C:\Users\user\Desktop\4EBE6@3.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	49	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-08-05 09:58:39 UTC	49	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 09:58:39 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=AakniGOAL6F9KPEZAKOJKonBHQENoNTVXP9k6XPvYreh2m3WEQaw1IYh4A; expires=Wed, 01-Feb-2023 09:58:39 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=6.SE=JwBdYDAvxPuGuQMM-KmJ5Zc55RvTPU92lHdr1tblJ3F-67_slmM0z2G6b_fYg474_LU89jb7IVPdPI3SIldYWqfmCNS2uTXD0reCEruLhntLTG5sYE_Ihl7STyBV_gMfnQtDTBldTh3TYS48WDJ7tAFANMX7RbajrZmBajrZmBPSYFsQ; expires=Tue, 05-Sep-2023 02:16:57 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+795; expires=Sun, 04-Aug-2024 09:58:39 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
2022-08-05 09:58:39 UTC	50	IN	Data Raw: 35 36 61 36 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 5f 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 Data Ascii: 56a6<!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
2022-08-05 09:58:39 UTC	50	IN	Data Raw: 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 36 48 58 4e 59 6d 71 4a 4f 67 6f 47 6c 31 75 59 50 45 51 58 48 67 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 3d 7b 6b 45 49 3a 27 7a 2d 6e 73 59 74 4f 44 43 61 4b 7a 35 4e 6f 50 70 49 71 49 36 41 67 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 36 30 35 39 2c 32 30 36 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 36 2c 35 2c 35 33 36 37 2c Data Ascii: =/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="6HXNYmqJOGogI1uYPEQXHg">(function(){window.google={kEl:'z-nsYtODCaKz5NoPplql6Ag',kEXPI:'0,1 302536,56873,6059,206,4804,2316,383,246,5,5367,

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	51	IN	Data Raw: 67 6f 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 64 65 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e 75 6c 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 6c 65 69 64 Data Ascii: google.sn=webhp;google.kHL=de;})();(function(){var f=this self;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute (b=a.getAttribute("eid"))));a=a.parentNode;return b h}function m(a){for(var b=null;a&&(!a.getAttribute (b=a.getAttribute("leid
2022-08-05 09:58:39 UTC	53	IN	Data Raw: 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 67 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 7c 7c 22 71 22 3d 3d 3d 63 26 26 21 61 2e 65 6c 65 6d 65 6e 74 73 2e 71 2e 76 61 6c 75 65 3f 21 Data Ascii: .push([a,b]);google.bx=1;google.lx=function(){}}.call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfalse");a="1"===c "q"===c&&!a.elements.q.value?!
2022-08-05 09:58:39 UTC	54	IN	Data Raw: 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 7d 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2b 69 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 Data Ascii: te;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility:hidden;text-align:left;border:1px solid #bebeb
2022-08-05 09:58:39 UTC	55	IN	Data Raw: 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 6a 3d 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 Data Ascii: nd:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgba(0,0 ,0,.2);-moz-box-shadow:0 2p
2022-08-05 09:58:39 UTC	56	IN	Data Raw: 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 3a 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 3a 73 2c 23 67 62 69 3a 73 31 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 23 67 62 67 36 2e 67 62 67 74 2d 68 76 72 2c 23 67 62 67 36 Data Ascii: ckground-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbg6t-hvr,#gbg6
2022-08-05 09:58:39 UTC	58	IN	Data Raw: 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 Data Ascii: lor:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited ,gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited
2022-08-05 09:58:39 UTC	59	IN	Data Raw: 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 37 70 78 7d 23 67 62 64 34 20 2e 67 62 70 67 73 20 2e 67 Data Ascii: elative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc ,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpps .g
2022-08-05 09:58:39 UTC	60	IN	Data Raw: 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 7d 23 67 62 6d 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 6f 72 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f Data Ascii: -left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbf{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-to

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	61	IN	Data Raw: 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 Data Ascii: d #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none;.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);.gbqfb::-moz-focus-inner,.gb
2022-08-05 09:58:39 UTC	63	IN	Data Raw: 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 7 6 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 Data Ascii: 0fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8));.gbqfb:active{background-color:inherit;-webkit-box-shadow:inset 0 1px 2px
2022-08-05 09:58:39 UTC	64	IN	Data Raw: 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 62 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 Data Ascii: f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr=#f8f8f8,EndColorStr=#f1f1f1);.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#fff),to(#fbbfbb));background-image:-webkit-linear
2022-08-05 09:58:39 UTC	65	IN	Data Raw: 30 2c 30 2c 2e 31 29 3b 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 61 3a 61 63 74 69 76 65 2c 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70 78 7d 23 67 62 6d 6d 7b 6d 61 78 2d 68 65 69 67 68 74 3a 35 33 30 70 78 7d 2e 67 62 73 62 7b 2d Data Ascii: 0,0,.1);color:#222 !important;.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1);#gbmpas{max-height:220px;}#gbmm{max-height:530px;}.gbsb{-
2022-08-05 09:58:39 UTC	67	IN	Data Raw: 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 30 2c 72 67 62 61 28 30 2c 30 2c 2e 38 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 2e 38 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c 74 6f 28 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 Data Ascii: bkkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0)));background-image:-webkit-linear
2022-08-05 09:58:39 UTC	68	IN	Data Raw: 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 74 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 32 70 78 7d 2e 6c 73 Data Ascii: sbcl(padding-top:5px);sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px;}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px;}.lsbb{display:block;}#WqQANb a{display:inline-block;margin:0 12px;}.ls
2022-08-05 09:58:39 UTC	69	IN	Data Raw: 45 6c 65 6d 65 6e 74 2e 6f 75 74 65 72 48 54 4d 4c 2e 73 70 6c 69 74 28 22 5c 6e 22 5b 66 5d 2c 63 2b 3d 22 26 63 61 64 3d 22 2b 62 28 66 3f 66 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 33 30 30 29 3a 22 4e 6f 20 73 63 72 69 70 74 20 66 6f 75 6e 64 2e 22 29 29 29 3b 63 2b 3d 22 26 6a 73 65 6c 3d 22 2b 65 3b 66 6f 72 28 76 61 72 20 75 20 69 6e 20 64 29 63 2b 3d 22 26 22 2c 63 2b 3d 62 28 75 29 2c 63 2b 3d 22 3d 22 2c 63 2b 3d 62 28 64 5b 75 5d 29 3b 63 3d 63 2b 22 26 65 6d 73 67 3d 22 2b 62 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b 63 3d 63 2b 22 26 6a 73 73 74 3d 22 2b 62 28 61 2e 73 74 61 63 6b 7c 7c 22 4e 2f 41 22 29 3b 31 32 32 38 38 3c 63 2e 6c 65 6e 67 74 68 26 26 28 63 3d 63 2e 73 75 62 73 74 72 28 30 2c 31 32 32 32 38 Data Ascii: Element.outerHTML.split("\n")[fj].c+="#&cad="+b(f?f.substring(0,300)):~No script found.);c+="#&jsel="+e;for(var u in d)c+="#&".c+="#&b(u).c+="#&".c+="#&b(d[u]);c+="#&emsgs="+b(a.name+":"+a.message);c+="#&jsst="+b(a.stack[0]~N/A");12288&c=length&(c=c.substr(0,1228
2022-08-05 09:58:39 UTC	70	IN	Data Raw: 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 2c 6d 3d 63 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 3b 72 65 74 75 72 6e 20 76 6f 69 64 20 30 3d 3d 6b 3f 6d 3a 76 6f 69 64 20 30 3d 3d 6d 3f 6b 3a 6d 26 26 6b 7d 7d 7d 76 61 72 20 64 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 67 2e 62 76 2e 6d 3d 3d 61 7d 7d 2c 65 61 3d 64 61 28 31 29 2c 66 61 3d 64 61 28 32 29 3b 70 28 22 73 62 22 2c 65 61 29 3b 70 28 22 6b 6e 22 2c 66 61 29 3b 68 2e 61 3d 5f 74 76 76 3b 68 2e 62 3d 5f 74 76 66 3b 68 2e 63 3d 5f 74 76 6e 3b 68 2e 69 3d 61 61 3b 76 61 72 20 72 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 2e 69 3b 76 61 72 20 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 2c 68 61 Data Ascii: y(this,arguments),m=c.apply(this,arguments);return void 0==k?m:void 0==m?k:m&&k}}var da=function(a){return function(){return g.bv.m==a}},ea=da(1),fa=da(2);p("sb",ea);p("kn",fa);h.a=_tvw;h.b=_tvf;h.c=_tvn;h.i=aa;var f=window.gbar.i.i;var t=function(){},ha

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	72	IN	Data Raw: 65 37 0d 0a 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 29 7b 75 61 3d 61 7d 2c 73 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 75 61 29 7b 61 3d 7b 74 3a 61 2c 62 3a 62 7d 3b 69 66 28 63 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 63 29 61 5b 64 5d 3d 63 5b 64 5d 3b 74 72 79 7b 75 61 28 61 29 7d 63 61 74 63 68 28 66 29 7b 7d 7d 7d 3b 70 28 22 6d 64 63 22 2c 76 29 3b 70 28 22 6d 64 69 22 2c 6c 61 29 3b 70 28 22 62 6e 63 22 2c 77 29 3b 70 28 22 71 47 42 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 42 29 3b 70 28 22 71 64 22 2c 78 29 3b 70 28 22 6c 62 22 2c 44 29 3b 70 28 22 6d 63 66 22 2c 70 61 0d 0a Data Ascii: e7a=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("mdi",la);p("bnc",w);p("qGC",ta);p("qm",B);p("qd",x);p("lb",D);p("mcf",pa
2022-08-05 09:58:39 UTC	72	IN	Data Raw: 36 38 34 33 0d 0a 29 3b 70 28 22 62 63 66 22 2c 6f 61 29 3b 70 28 22 61 71 22 2c 41 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 71 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 73 61 29 3b 69 66 28 68 2e 61 28 22 6d 3b 2f 5f 2f 73 63 73 2f 61 62 63 2d 73 74 61 74 69 63 2f 5f 2f 6a 73 2f 6b 3d 67 67 70 69 2e 67 61 70 69 2e 65 6e 2e 74 39 7a 37 56 50 73 45 4d 46 67 2e 4f 2f 64 3d 31 2f 72 73 3d 41 48 70 4f 6f 68 6f 44 5f 35 46 51 57 33 6b 54 33 6b 73 57 77 6d 58 49 57 76 68 68 71 62 4b 64 77 2f 6d 3d 5f 5f 66 65 61 74 75 72 65 73 5f 5f 22 29 29 7b 76 61 72 20 46 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 77 61 3f 61 7c 7c 62 3a 62 7d 2c 78 61 3d 68 2e 61 28 22 31 22 29 2c 79 61 3d 68 Data Ascii: 6843);p("bcf",oa);p("aq",A);p("mdd","");p("has",qa);p("trh",va);p("tev",sa);if(h.a(""/_/_scs/abc-static/_/_js/_/k=gapi.gapi.en.t9z7VPsEMFg.O/d=1/rs=AHpOoo8oD_5FQW3kT3ksWwmXIWvhqbKdw/m=__features__")){var F=function(a,b){return wa?a b:b},xa=h.a("1"),ya=h
2022-08-05 09:58:39 UTC	73	IN	Data Raw: 61 74 68 2e 72 6f 75 6e 64 28 31 2f 46 61 29 2c 22 26 6f 67 65 76 3d 22 2c 64 28 22 7a 2d 6e 73 59 73 2d 4f 43 73 4c 54 79 74 4d 50 72 76 43 69 71 41 77 22 29 2c 22 26 6f 67 66 3d 22 2c 67 2e 62 76 2e 66 2c 22 26 6f 67 72 70 3d 22 2c 64 28 22 22 29 2c 22 26 6f 67 76 3d 22 2c 64 28 22 34 36 34 33 35 35 39 35 2e 30 22 29 2c 22 26 6f 67 67 76 3d 22 2b 64 28 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 32 30 37 30 36 2e 30 5f 70 30 22 29 2c 22 26 6f 67 64 3d 22 2c 64 28 22 63 6f 6d 22 29 2c 22 26 6f 67 63 3d 22 2c 64 28 22 44 45 55 22 29 2c 22 26 6f 67 6c 3d 22 2c 64 28 22 64 65 22 29 5d 3b 62 2e 5f 73 6e 26 26 28 62 2e 5f 73 6e 3d 0a 22 6f 67 2e 22 2b 62 2e 5f 73 6e 29 3b 66 6f 72 28 76 61 72 20 6b 20 69 6e 20 62 29 66 2e 70 75 73 68 28 22 26 22 Data Ascii: ath.round(1/Fa),"&ogev=",d("z-nsYs-OCsLTytMPrvCiqAw"),"&ogf=",g.bv.f,"&ogrp=",d(""),"&ogv=",d("464435595.0"),"&oggv="+d("es_plusone_gc_20220706.0_p0"),"&ogd=",d("com"),"&ogc=",d("DEU"),"&ogl=",d("de"));b._sn&&(b._sn="og."+b._sn);for(k in b)f.push("&
2022-08-05 09:58:39 UTC	74	IN	Data Raw: 2e 65 6e 5f 55 53 2e 62 6d 48 52 47 50 74 37 41 4d 77 2e 44 55 22 29 3b 61 3d 61 2e 6a 6f 69 6e 28 22 22 29 3b 72 61 28 61 29 7d 3b 70 28 22 63 61 22 2c 4a 29 3b 70 28 22 63 72 22 2c 4b 29 3b 70 28 22 63 63 22 2c 48 29 3b 68 2e 6b 3d 4a 3b 68 2e 6c 3d 4b 3b 68 2e 6d 3d 48 3b 68 2e 6e 3d 4d 61 3b 68 2e 70 3d 4f 61 3b 68 2e 71 3d 4e 61 3b 76 61 72 20 50 61 3d 5b 22 67 62 5f 37 31 22 2c 22 67 62 5f 31 35 35 22 5d 2c 51 61 3b 66 75 6e 63 74 69 6f 6e 20 52 61 28 61 29 7b 51 61 3d 61 7d 66 75 6e 63 74 69 6f 6e 20 53 61 28 61 29 7b 61 72 20 62 3d 51 61 26 63 21 51 2e 68 72 65 66 2e 6d 61 74 63 68 28 2f 2e 2a 5c 2f 61 63 63 6f 75 6e 74 73 5c 2f 43 6c 65 61 72 53 49 44 5b 3f 5d 2f 29 26 26 65 6e 6 3 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 51 61 28 29 29 Data Ascii: .en_US.bmHRGPt7AMw.DU");a=a.join("");ra(a));p("ca",J);p("cr",K);p("cc",H);h.k=J;h.l=K;h.m=H;h.n=Ma;h.p=Oa;h.q=Na;var Pa=["gb_71","gb_155"],Qa=function Ra(a){Qa=a}function Sa(a){var b=Qa&&!a.href.match(/.*Vac countsVClearSID[?])&&encodeURIComponentComponent(Qa())
2022-08-05 09:58:39 UTC	76	IN	Data Raw: 3b 4f 3d 64 3b 4a 28 6b 2c 22 67 62 74 6f 22 29 7d 7d 7d 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 74 67 28 61 2c 62 2c 21 30 29 7d 29 3b 62 62 28 61 29 7d 63 61 74 63 68 28 61 29 7b 72 28 71 2c 22 73 62 22 2c 22 74 67 22 29 7d 7d 2c 64 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 63 6f 73 65 28 61 29 7d 29 7d 2c 65 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 72 64 64 28 61 29 7d 29 7d 2c 5a 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 2c 63 3d 64 6f 63 75 6d 65 6e 74 2 e 64 65 66 61 75 6c 74 56 69 65 77 3b 63 26 26 63 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 61 2c 22 22 29 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 61 2c 22 22 29 Data Ascii: ;O=d;J(k,"gbto"))}}B(function(){g.tg(a,b,l0));bb(a)}catch(q){r(q,"sb","tg"))};db=function(a){B(function(){g.close(a)});eb=function(a){B(function(){g.rdd(a)});Za=function(a){var b,c=document.defaultView;c&&c.getComputedStyle?a=c.getComputedStyle(a,"")
2022-08-05 09:58:39 UTC	77	IN	Data Raw: 30 3b 64 3c 63 3b 64 2b 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 62 28 61 2c 22 67 62 65 22 2c 62 29 7d 2c 6a 62 3d 66 75 6e 63 74 69 6 f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 63 6d 26 26 67 2e 70 63 6d 28 29 7d 29 7d 2c 6b 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 63 61 26 26 67 2e 70 63 61 28 29 7d 29 7d 2c 6c 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 2c 66 2c 6b 2c 6d 2c 6e 2c 6c 2c 21 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 70 61 61 26 26 67 2e 70 61 61 28 61 2c Data Ascii: 0;d<c;d++if(H(a,b[d]))return!0;return!1},hb=function(a,b,c){gb(a,b,c)},ib=function(a,b){gb(a,"gbe",b)},jb=f unction(){B(function(){g.pcm&&g.pcm()});kb=function(){B(function(){g.pca&&g.pca()});lb=function(a,b,c,d,f,k,m,n,l,q){B (function(){g.paa&&g.paa(a,
2022-08-05 09:58:39 UTC	78	IN	Data Raw: 65 61 72 54 69 6d 65 6f 75 74 28 71 62 29 7d 2c 75 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 22 69 6e 6e 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 61 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e 64 6f 77 5b 62 5d 3a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3f 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3a 30 7d 2c 76 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 31 7d 2c 77 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 21 4f 7d 3b 70 28 22 73 6f 22 2c 57 61 29 3b 70 28 22 73 6f 73 22 2c 56 61 29 3b 70 28 22 73 69 22 2c 58 61 29 3b Data Ascii: earTimeout(qb)),ub=function(a){var b="inner"+a;a="offset"+a;return window[b]?window[b]:document.do cumentElement&&document.documentElement[a]?document.documentElement[a]:0},vb=function(){return!1},wb=function() {return!!O};p("so",Wa);p("sos",Va);p("si",Xa);
2022-08-05 09:58:39 UTC	79	IN	Data Raw: 69 6f 6e 28 61 29 7b 43 62 28 66 75 6e 63 74 69 6f 6e 28 29 7b 41 28 22 70 77 22 2c 61 29 3b 44 28 22 70 77 22 29 7d 29 7d 3b 70 28 22 6c 50 57 22 2c 44 62 29 3b 77 2e 70 75 73 68 28 5b 22 70 77 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 70 77 6d 5f 34 35 66 37 33 65 34 64 66 30 37 61 30 65 33 38 38 62 30 66 61 31 66 33 64 33 30 65 37 32 38 30 2e 6a 73 22 7d 5d 29 3b 76 61 72 20 46 62 3d 5b 5d 2c 47 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 46 62 5b 30 5d 3d 61 7d 2c 48 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 6 2 29 7b 62 3d 62 7c 7c 7b 7d 3b 62 2e 5f 73 6e 3d 22 70 77 22 3b 74 28 61 2c 62 29 7d 2c 49 62 3d 7b 73 69 67 6e 65 64 3a 46 62 2c 65 6c 6f 67 3a 48 62 2c 62 61 73 65 3a 22 68 74 74 70 Data Ascii: ion(a){Cb(function(){A("pw",a);D("pw"))});p("IPW",Db);w.push(["pw",{url:"/ssl.gstatic.com/gb/js/abc/pwm_45f73e4df07a0e388b0fa1f3d30e7280.js"}]);var Fb=[],Gb=function(a){Fb[0]=a},Hb=function(a,b){b=b {};b._sn="pw";t(a,b)},lb= {signed:Fb,elog:Hb,base:"http

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	81	IN	Data Raw: 61 74 79 70 3d 69 26 7a 78 3d 22 2c 66 2c 22 26 6f 67 65 3d 22 2c 61 2c 22 26 6f 67 65 78 3d 22 2c 6b 2c 22 26 6f 67 65 76 3d 22 2c 6d 2c 22 26 6f 67 66 3d 22 2c 6c 2c 22 26 6f 67 70 3d 22 2c 71 2c 22 26 6f 67 72 70 3d 22 2c 6e 2c 22 26 6f 67 73 72 3d 22 2c 63 2c 22 26 6f 67 76 3d 22 2c 45 2c 55 2c 22 26 6f 67 64 3d 22 2c 49 2c 22 26 6f 67 6c 3d 22 2c 56 2c 22 26 6f 67 63 3d 22 2c 57 2c 22 26 6f 67 75 73 3d 22 2c 79 5d 3b 69 66 68 62 29 7b 22 6f 67 77 22 69 6e 20 62 26 26 28 61 2e 70 75 73 68 28 22 26 6f 67 77 3d 22 2b 62 2e 6f 67 77 29 2c 63 62 58 3d 30 2c 64 63 6d 65 6c 65 74 65 62 2e 6f 67 77 29 3b 66 3d 5b 5d 3b 66 6f 72 28 7a 20 69 6e 20 62 29 30 21 3d 66 2e 6c 65 6e 67 74 68 26 26 66 2e 70 75 73 68 28 22 2c 22 29 2c 66 2e 70 75 73 68 28 52 62 28 7a 29 29 2c 66 2e 70 75 Data Ascii: atyp=i&zx=",f,"&oge=",a,"&ogex=",k,"&ogev=",m,"&ogf=",l,"&ogp=",q,"&ogrp=",n,"&ogsr=",c,"&ogv=",E,U,"&ogd=",l,"&ogl=",V,"&ogc=",W,"&ogus=",y);if(b){t"ogw"in b&&(a.push(t"&ogw="+b.ogw),delete b.ogw);f=[];for(z in b)0!=f.length&&f.push(",");f.push(Rb(z)),f.pu
2022-08-05 09:58:39 UTC	82	IN	Data Raw: 74 61 6e 64 61 72 64 29 22 2c 6d 68 3a 22 32 32 30 22 2c 73 3a 22 31 22 2c 70 70 3a 5a 62 2c 70 70 6c 3a 68 2e 61 28 22 22 29 2c 70 61 3a 68 2e 61 28 22 22 29 2c 0a 70 70 6d 3a 22 47 6f 6f 67 6c 65 2b 20 53 65 69 74 65 22 7d 3b 76 2e 70 72 66 3d 61 63 7d 3b 76 61 72 20 53 2c 62 63 2c 54 63 2c 63 62 63 2c 64 63 6d 65 6c 65 74 65 62 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 61 2e 69 6e 64 65 78 4f 66 28 62 2c 63 29 3b 69 66 28 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 28 61 2c 62 2c 63 29 3b 66 6f 72 28 63 3d 6e 75 6c 6c 3d 63 3f 30 3a 30 3e 63 3f 4d 61 74 68 2e 6d 61 78 28 30 2c 61 2e 6c 65 6e 67 74 68 2b 63 29 3a 63 3b 63 3c 61 2e 6c 65 Data Ascii: tandard)" ,mh:"220",s:"1",pp:Zb,ppl:h.a(""),ppa:h.a(""),ppm:"Google+ Seite");v.prf=ac};var S,b,c,T,cx,X=0,dc=function(a,b,c){if(a.indexOf)return a.indexOf(b,c);if(Array.indexOf)return Array.indexOf(a,b,c);for(c=null==c?0:0>c?Math.max(0,a.length+c):c;c<a.le
2022-08-05 09:58:39 UTC	83	IN	Data Raw: 75 70 2d 22 2b 62 29 2c 6b 63 28 29 3f 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 73 65 74 49 74 65 6d 28 62 2c 63 29 3a 6c 63 28 61 29 26 26 28 61 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 62 2c 63 29 2c 61 2e 73 61 76 65 28 61 2e 69 64 29 29 7d 63 61 74 63 68 28 66 29 7b 66 2e 63 6f 64 65 21 3d 44 4f 4d 45 78 63 65 70 74 69 6f 6e 2e 51 55 4f 54 41 5f 45 58 43 45 45 44 45 4f 45 52 52 26 26 72 28 66 2c 22 75 70 22 2c 22 73 70 64 22 29 7d 7d 2c 6e 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 74 72 79 7b 69 66 28 6a 63 28 64 63 75 6d 65 6e 74 29 72 65 7 4 75 72 6e 22 22 3b 0a 63 7c 7c 28 62 3d 22 6f 67 2d 75 70 2d 22 2b 62 29 3b 69 66 28 6b 63 28 29 29 72 65 74 75 72 6e 20 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 Data Ascii: up-"+b),kc())?e.localStorage.setItem(b,c):lc(a)&&(a.setAttribute(b,c),a.save(a.id))}}catch(f){f.code!=DOMException.QUOTA_EXCEEDED_ERR&&(f,"up","spd"))},nc=function(a,b,c){try{if(jc(document))return"";c (b="og-up-"+b);if(kc())return e.localStorage.gettite
2022-08-05 09:58:39 UTC	84	IN	Data Raw: 30 3c 66 2d 2d 3f 73 65 74 54 69 6d 65 6f 75 74 28 62 2c 30 29 3a 61 28 29 7d 76 61 72 20 63 3d 68 2e 61 28 22 31 22 29 2c 64 3d 68 2e 61 28 22 22 29 2c 66 3d 33 2c 6b 3d 77 2c 6d 3d 30 2c 6e 3d 77 69 6e 64 6f 77 2e 67 62 61 72 4f 6e 52 65 61 64 79 3b 69 66 28 6e 29 74 72 79 7b 6e 28 29 7d 63 61 74 63 68 28 6c 29 7b 72 28 6c 2c 22 6d 6c 22 2c 22 6f 72 22 29 7d 64 3f 70 28 22 6c 64 62 22 2c 61 29 3a 63 3f 63 61 28 77 69 6e 64 6f 77 2c 22 6c 6f 61 64 22 2c 62 29 3a 62 28 29 7d 70 28 22 72 64 6c 22 2c 72 63 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 2 6 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 Data Ascii: 0<-f-?setTimeout(b,0);a())var c=h.a("1"),d=h.a(""),f=3,k=w,m=0,n=window.gbarOnReady;if(n)try{n()}catch(l){r(l,"ml","or"))d?p("ldb",a):c?ca(window,"load",b):b()}p("rdl",rc);}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{_sn":"cfg.init");}})}(fu
2022-08-05 09:58:39 UTC	86	IN	Data Raw: 67 62 5f 22 2b 61 29 3b 62 26 26 66 2e 6c 28 62 2c 68 2e 74 65 73 74 28 62 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 3b 63 26 26 66 2e 6b 28 63 2c 68 2e 74 65 73 74 28 63 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 7d 63 61 74 63 68 28 6c 29 7b 64 28 6c 2c 22 73 6a 22 2c 22 73 73 70 22 29 7d 67 3d 61 7d 2c 6d 3d 65 2e 71 73 2c 6e 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 7 2 20 62 3d 61 2e 68 72 65 66 3b 76 61 72 20 63 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 6d 61 74 63 68 28 2f 2e 2a 3f 3a 5c 2f 5c 2f 5b 5e 5c 2f 5d 2a 2f 29 5b 30 5d 3b 63 3d 6e 65 77 20 52 65 67 45 70 28 22 5e 2 2 2b 63 2b 22 2f 73 65 61 72 63 68 5c 5c 3f 22 29 3b 28 62 3d 63 Data Ascii: gb_"+a);b&&f.l(b,h.test(b.className)?"gbm0l":"gbz0l");c&&f.k(c,h.test(c.className)?"gbm0l":"gbz0l"))catch(l){d(l,"sj","ssp");g=a},m=e.qs,n=function(a){var b=a.href,var c=window.location.href.match(/.*?:VV[V*V]*/)[0];c=new RegExp("(^"+c+"/search\\?") (b=c
2022-08-05 09:58:39 UTC	87	IN	Data Raw: 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 77 69 6e 64 6f 77 2e 67 62 61 72 2e 72 64 6c 28 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 66 Data Ascii: sn":"cfg.init");}})}(function(){try{/* Copyright The Closure Library Authors. SPDIX-License-Identifier: Apache-2.0*/window.gbar.rdl();}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{_sn":"cfg.init");}})});</script></head><body bgcolor="#ff
2022-08-05 09:58:39 UTC	88	IN	Data Raw: 73 3d 67 62 74 73 3e 50 6c 61 79 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 33 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 3f 67 6c 3d 44 45 26 74 61 62 3d 77 31 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 59 6f 75 54 75 62 65 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 34 32 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6e 65 77 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 3f 74 61 62 3d 77 6e 22 3e 3c 73 70 61 Data Ascii: s=gbts>Play<li class=gbt>YouTube<li class=gbt><spa
2022-08-05 09:58:39 UTC	90	IN	Data Raw: 26 74 61 62 3d 77 54 22 3e dc 62 65 72 73 65 74 7a 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 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 31 30 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6f 6b 73 2e 67 6f 6f 67 6c 65 2e 64 65 2f 3f 68 6c 3d 64 65 26 74 61 62 3d 77 70 22 3e 42 6f 6f 6b 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 64 65 2f 73 68 6f 70 70 69 6e 67 3f 68 6c 3d 64 65 26 73 6f 75 72 63 65 3d 6f 67 26 74 61 62 3d 77 66 22 3e 53 68 6f 70 70 69 6e 67 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d Data Ascii: &tab=wT">bersetzer<li class=gbmtc>Books<li class=gbmtc>Shopping<li class=gbm

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:58:39 UTC	91	IN	Data Raw: 65 2e 63 6f 6d 2f 53 65 72 76 69 63 65 4c 6f 67 69 6e 3f 68 6c 3d 64 65 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 26 65 63 3d 47 41 5a 41 41 51 22 20 6f 6e 63 6c 69 63 6b 3d 22 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 39 2c 7b 6c 3a 27 69 27 7d 29 22 20 69 64 3d 67 62 5f 37 30 20 63 6c 61 73 73 3d 67 62 67 74 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 69 64 3d 67 62 67 73 34 2d 63 6c 61 73 73 3d 67 62 74 73 3e 3c 73 70 61 6e 20 69 64 3d 67 62 69 34 73 31 3e 41 6e 6d 65 6c 64 65 6e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 74 20 67 62 74 62 Data Ascii: e.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ" onclick="gbar.lo gger.il(9,{l:'f'})" id=gb_70 class=gbgtAnm elden <li class="gbt gbtb
2022-08-05 09:58:39 UTC	92	IN	Data Raw: 32 78 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 32 38 70 78 20 30 20 31 34 70 78 22 20 77 69 64 74 68 3d 22 32 37 32 22 20 69 64 3d 22 68 70 6c 6f 67 6f 22 3e 3c 62 72 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 66 6f 72 6d 20 61 63 74 69 6f 6e 3d 22 2f 73 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 66 22 3e 3c 74 61 62 6c 65 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 30 22 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 22 30 22 3e 3c 74 72 20 76 61 6c 69 67 6e 3d 22 74 6f 70 22 3e 3c 74 64 20 77 69 64 74 68 3d 22 32 35 25 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 3c 74 64 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 20 6e 6f 77 72 61 70 3d 22 22 3e 3c 69 6e 70 75 74 20 6e 61 6d 65 3d 22 69 65 22 20 76 61 6c 75 65 3d 22 49 53 4f 2d 38 38 35 39 2d Data Ascii: 2x92dp.png" style="padding:28px 0 14px" width="272" id="hplogo"> </div><form action="/search" name="f"><table cellpadding="0" cellspacing="0"><tr valign="top"><td width="25%"> </td><td align="center" nowrap=""><input name="ie" value="ISO-8859-
2022-08-05 09:58:39 UTC	93	IN	Data Raw: 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 76 61 6e 63 65 64 5f 73 65 61 72 63 68 3f 68 6c 3d 64 65 26 61 6d 70 3b 61 75 74 68 75 73 65 72 3d 30 22 3e 45 72 77 65 69 74 65 72 74 65 20 53 75 63 68 65 3c 2f 61 3e 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 61 62 6c 65 3e 3c 69 6e 70 75 74 20 69 64 3d 22 67 62 76 22 20 6e 61 6d 65 3d 22 67 62 76 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 76 61 6c 75 65 3d 22 31 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 36 48 58 4e 59 6d 71 4a 4f 67 6f 47 6c 31 75 59 50 45 51 58 48 67 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 61 2c 62 3d 22 31 22 3b 69 66 28 64 6f 6 3 75 6d 65 6e 74 26 26 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c Data Ascii: eft" nowrap="" width="25%">Erweiterte Suche</td></tr></table><input id="gbv" name="gbv" type="hidden" value="1"><script nonce="6HXNYmqJOGogI1uYPEQXHG">(func tion(){var a,b="1";if(document&&document.getEl
2022-08-05 09:58:39 UTC	95	IN	Data Raw: 72 65 66 3d 22 2f 69 6e 74 6c 2f 64 65 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 4e 75 74 7a 75 6e 67 73 62 65 64 69 6e 67 75 6e 67 65 6e 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 36 48 58 4e 59 6d 71 4a 4f 67 6f 47 6c 31 75 59 50 45 51 58 48 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 63 64 6f 3d 7b 68 65 69 67 68 74 3a 37 35 37 2c 77 69 64 74 68 3a 31 34 34 30 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 61 3d 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 57 69 64 74 68 2c 62 3d 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 48 65 69 67 68 74 3b 69 66 28 21 61 7c 7c 21 62 29 7b 76 61 72 20 63 3d 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 Data Ascii: ref="/intl/de/policies/terms/">Nutzungsbedingungen</p></center><script nonce="6HXNYmqJOGogI1uYPEQXHG">(function(){window.google.cdo={height:757,width:1440};(function(){var a=window.innerWidth,b=win dow.innerHeight;if(!a !b){var c=window.docume
2022-08-05 09:58:39 UTC	96	IN	Data Raw: 6e 75 6c 6c 3b 76 61 72 20 6b 3d 64 2e 74 72 75 73 74 65 64 54 79 70 65 73 3b 69 66 28 6b 26 26 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 28 22 67 6f 67 23 68 74 6d 6c 22 2c 7b 63 72 65 61 74 65 48 54 4d 4c 3a 65 2c 63 72 65 61 74 65 53 63 72 69 70 74 3a 65 2c 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 3a 65 7d 29 7d 63 61 74 63 68 28 71 29 7b 64 2e 63 6f 6e 73 6f 6c 65 26 26 64 2e 63 6f 6e 73 6f 6c 65 2e 65 72 72 6f 72 28 71 2e 6d 65 73 73 61 67 65 29 7d 67 3d 62 7d 65 6c 73 65 20 67 3d 62 7d 61 3d 28 6 2 3d 67 29 3f 62 2e 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 28 61 29 3a 61 3b 61 3d 6e 65 77 20 6c 28 61 2c 68 29 3b 63 2e 73 72 63 3d 61 20 69 6e 73 74 61 6e 63 65 6f 66 20 6c 26 Data Ascii: null;var k=d.trustedTypes;if(k&&k.createPolicy){try{b=k.createPolicy("goog#html"),{createHTML:e,createScript: e,createScriptURL:e}})catch(q){d.console&&d.console.error(q.message)}g=b}else g=b;a=(b=g)?b.createScriptURL(a) :a;a=new l(a,h);c.src=a instanceof l&
2022-08-05 09:58:39 UTC	97	IN	Data Raw: 20 49 6e 66 6f 72 6d 61 74 69 6f 6e 65 6e 5c 78 32 32 2c 5c 78 32 32 6f 73 6b 74 5c 78 32 32 3a 5c 78 32 32 45 69 6e 67 61 62 65 74 6f 6f 6c 73 5c 78 32 32 2c 5c 78 32 32 70 73 72 63 5c 78 32 32 3a 5c 78 32 32 44 69 65 73 65 20 53 75 63 68 61 6e 66 72 61 67 65 20 77 75 72 64 65 20 61 75 73 20 64 65 69 6e 65 6d 20 5c 5c 75 30 30 33 43 61 20 68 72 65 66 5c 78 33 64 5c 5c 5c 78 32 32 2f 68 69 73 74 6f 72 79 5c 5c 5c 78 32 32 5c 5c 75 30 30 33 45 57 65 62 70 72 6f 74 6f 6b 6f 6c 6c 5c 5c 75 30 30 33 43 2f 61 5c 5c 75 30 30 33 45 20 65 6e 74 66 65 72 6e 74 2e 5c 78 32 32 2c 5c 78 32 32 70 73 72 6c 5c 78 32 32 3a 5c 78 32 32 45 6e 74 66 65 72 6e 65 6e 5c 78 32 32 2c 5c 78 32 32 73 62 69 74 5c 78 32 32 3a 5c 78 32 32 42 69 6c 64 65 72 73 75 63 68 65 5c 78 32 32 Data Ascii: Informationen\x22,\x22osktx22:\x22Eingabetools\x22,\x22psrcl\x22:\x22Diese Suchanfrage wurde aus deinem \u003Ca href\x3d\u0026#x22history\u0026#x22\u003EWebprotokoll\u003C/a\u0026#x22 entfernt.\x22,\x22psrl\x22:\x2 2Entfernen\x22,\x22sbit\x22:\x22Bildersuche\x22
2022-08-05 09:58:39 UTC	98	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior

4EBE6@3.exe

noise.exe

● InstallUtil.exe
● Acrobat.exe
● conhost.exe



💡 Click to jump to process

System Behavior

Analysis Process: 4EBE6@3.exe PID: 400, Parent PID: 4472

General

Target ID:	1
Start time:	11:58:17
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\4EBE6@3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4EBE6@3.exe"
Imagebase:	0x320000
File size:	641536 bytes
MD5 hash:	ADE71491B076CA7A43EFAF0214DD030
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.342705097.00000000049B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.342705097.00000000049B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.342705097.00000000049B5000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.343598917.0000000004ABC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.343598917.0000000004ABC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.343598917.0000000004ABC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CDFCF06	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	6CDFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsof\CLR_v4.0_32\UsageLogs\4EBE6@3.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D10C78D	CreateFileW

File Moved							
Old File Path	New File Path			Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4EBE6@3.exe	C:\Users\user\AppData\Local\Temp\noise.exe			success or wait	1	DCA9D87	MoveFileExW

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0_32\UsageLogs\4EBE6@3.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 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 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,"Microsoft.VisualStudio.BasicalBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",02,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.	success or wait	1	6D10C907	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	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorliba152fe02a317a7ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	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: noise.exe PID: 1600, Parent PID: 400

General

Target ID:	13
Start time:	11:58:34
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\noise.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\noise.exe"
Imagebase:	0x320000
File size:	641536 bytes
MD5 hash:	ADE71491B076CA7A43EFAF0214DD030
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: 0000000D.00000002.532021277.0000000003E1A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.532021277.0000000003E1A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000D.00000002.532021277.0000000003E1A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.533246648.0000000003E75000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.533246648.0000000003E75000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000D.00000002.533246648.0000000003E75000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.540720727.0000000003F7B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.540720727.0000000003F7B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000D.00000002.540720727.0000000003F7B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\noise.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D10C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\noise.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 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 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,"Win RT","N otApp",12,"Microsoft.Visu alBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f 7f11d50a3a",02,"System. Windows.Forms, Version=4.0.0.0, Cultu re=neutral, PublicKeyToken=b77 a5c561934e089",03,"Sys tem, Version=4.	success or wait	1	6D10C907	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	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefaf3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	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: 6036, Parent PID: 1600	
General	
Target ID:	18
Start time:	11:59:25
Start date:	05/08/2022
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:	0x9b0000
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: 00000012.00000000.442229675.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.442229675.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000012.00000000.442229675.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.574138944.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.574138944.0000000002F11000.00000004.00000800.00020000.00000000.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	6CDFCF06	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	6CDFCF06	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	6BC4BEFF	CreateDirectoryW	
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	6BC4DD66	CopyFileW	

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\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 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 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	6BC4DD66	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	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\la152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6CDDCA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6CDD5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6BC41B4F	ReadFile	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC41B4F	ReadFile	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC41B4F	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	6BC4646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Acrobat	binary	02 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BC4DE2E	RegSetValueExW

Analysis Process: Acrobat.exe

PID: 4876, Parent PID: 3968

General

Target ID:

28

Start time:

12:00:18

Start date:

05/08/2022

Path:

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

Wow64 process (32bit):

true

Commandline:

"C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe"

Imagebase:

0x850000

File size:

41064 bytes

MD5 hash:

EFEC8C379D165E3F33B536739AEE26A3

Has elevated privileges:

false

Has administrator privileges:

false

Programmed in:

.Net C# or VB.NET

Antivirus matches:

- Detection: 0%, Metadefender, [Browse](#)
- Detection: 0%, ReversingLabs

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	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Acrobat.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D10C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BC41B4F	WriteFile
\Device\ConDrv	132	132	55 73 61 67 65 3a 20 49 6e 73 74 61 6c 6c 55 74 69 6c 20 5b 2f 75 20 7c 20 2f 75 6e 69 6e 73 74 61 6c 6c 5d 20 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 20 5b 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 5d 20 5b 2e 2e 2e 5d 5d 0d 0a 0d 0a 49 6e 73 74 61 6c 6c 55 74 69 6c 20 65 78 65 63 75 74 65 73 20 74 68 65 20 69 6e 73 74 61 6c 6c 65 72 73	Usage: InstallUtil [/u /uninstall] [option [...] assembly [[option [...]] assembly] [...]InstallUtil executes the installers	success or wait	1	6BC41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	388	256	74 68 65 6d 2e 20 55 6e 6c 69 6b 65 20 6f 74 68 65 72 0d 0a 6f 70 74 69 6f 6e 73 2c 20 2f 75 20 61 70 70 6c 69 65 73 20 74 6f 20 61 6c 6c 20 61 73 73 65 6d 62 6c 69 65 73 2c 20 72 65 6f 61 72 64 6c 65 73 73 20 6f 66 20 77 68 65 72 65 20 69 74 0d 0a 61 70 70 65 61 72 73 20 6f 6e 20 74 68 65 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 2e 0d 0a 0d 0a 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 69 73 20 64 6f 6e 65 20 69 6e 20 61 20 74 72 61 6e 73 61 63 74 69 6f 6e 65 64 20 77 61 79 3a 20 49 66 20 6f 6e 65 20 6f 66 20 74 68 65 0d 0a 61 73 73 65 6d 62 6c 69 65 73 20 66 61 69 6c 73 20 74 6f 20 69 6e 73 74 61 6c 6c 2c 20 74 68 65 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 73 20 6f 66 20 61 6c 6c 20 6f 74 68 65 72 0d 0a 61 73 73 65 6d 62 6c 69 65 73 20 61 72 65 20 72 6f 6c 6c	them. Unlike other options, /u applies to all assemblies, regardless of where it appears on the command line. Installation is done in a transactioned way: If one of the assemblies fails to install, the installations of all other assemblies are rolled back.	success or wait	7	6BC41B4F	WriteFile
\\Device\\ConDrv	2017	93	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BC41B4F	WriteFile
C:\\Users\\user\\AppData\\Local\\Microsoft\\CLR_v4.0_32\\UsageLogs\\Acrobat.exe.log	0	950	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 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 49 6e 73 74 61 6c 6c 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65	1, "fusion", "GAC", 01, "Win RT", "N otApp", 12, "System.Confi guration.Install, Version=4.0.0.0, Cu lture=neutral, PublicKeyToken= b03f5f7f11d50a3a", 03, "S ystem, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56193 4e089", "C:\\Windows\\ass embly\\NativeImage	success or wait	1	6D10C907	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	6CDD5705	unknown		
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown		
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\mscorlib.b152fe02a317a77ae36903305e8ba6\\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile		
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile		
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\System.4f0a7eefa3cd3e0ba98b5ebddbbc72e6\\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile		
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\System.Configuration\\8d67d92724ba494b6c7fd089d6f25b48\\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile		
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\System.Core\\1d8480152e0da9a60ad49c6d16a3b6d\\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile		
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\System.Xml\\b219d4630d26b88041b59c21e8e2b95c\\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile		

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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile

Analysis Process: conhost.exe PID: 1112, Parent PID: 4876

General	
Target ID:	29
Start time:	12:00:19
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

 No disassembly