ID: 672480
Sample Name: B35@6B.exe
Cookbook: default.jbs
Time: 17:53:07
Date: 24/07/2022
Version: 35.0.0 Citrine

Table of Contents

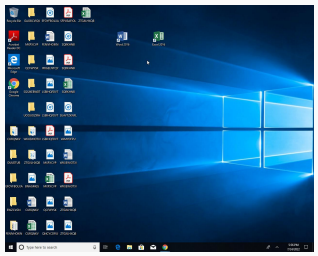
Windows Analysis Report

B35@6B.exe

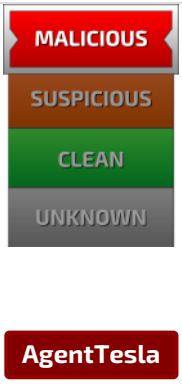
Overview

General Information

Sample Name:	B35@6B.exe
Analysis ID:	672480
MD5:	6753a24ed2a75d.
SHA1:	70c061619c4ebb..
SHA256:	a9b46ddb3ed98e.
Tags:	agenttesla exe
Infos:	



Detection



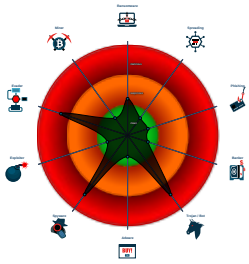
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Drops executable to a common third…
- Machine Learning detection for sam…
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Moves itself to temp directory
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- B35@6B.exe (PID: 1724 cmdline: "C:\Users\user\Desktop\B35@6B.exe" MD5: 6753A24ED2A75DBD488C0A1783F03D05)
  - pot.exe (PID: 3224 cmdline: "C:\Users\user\AppData\Local\Temp\pot.exe" MD5: 6753A24ED2A75DBD488C0A1783F03D05)
    - InstallUtil.exe (PID: 1448 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- Acrobat.exe (PID: 5284 cmdline: "C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe" MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 4940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Acrobat.exe (PID: 5680 cmdline: "C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe" MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 6128 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
0000000A.00000000.420464455.0000000000632000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000000.420464455.0000000000632000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.303282970.0000000004AE1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.303282970.0000000004AE1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000A.00000000.420090127.0000000000632000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.B35@6B.exe.4b4aa42.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.B35@6B.exe.4b4aa42.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.B35@6B.exe.4b4aa42.4.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
0.2.B35@6B.exe.4be84c2.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.B35@6B.exe.4be84c2.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 73 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.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)

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

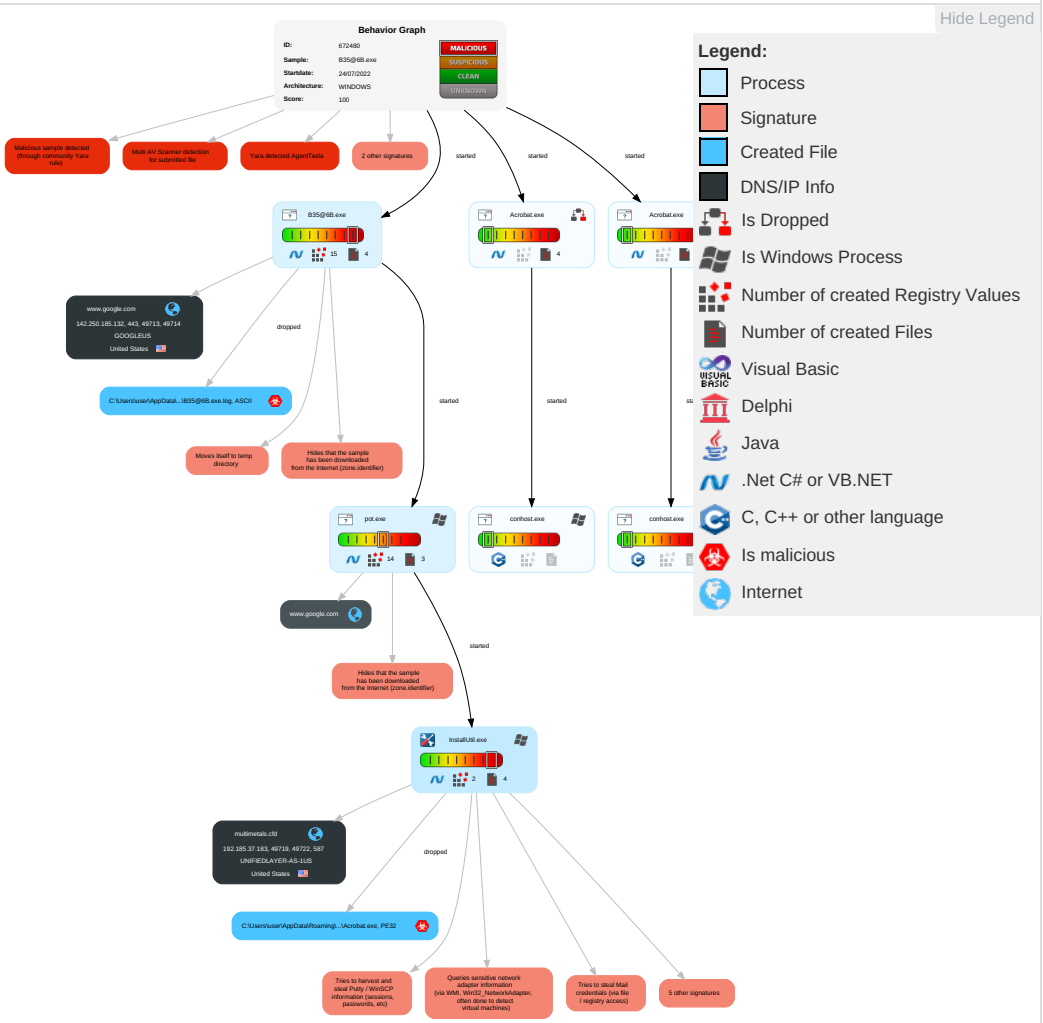
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Masquerading	LSA Secrets	1 4 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window 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 1 Process Injection	DCSync	1 Remote System 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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
B35@6B.exe	46%	Virustotal		Browse
B35@6B.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
B35@6B.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
10.0.InstallUtil.exe.630000.2.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.InstallUtil.exe.630000.1.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.InstallUtil.exe.630000.4.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.InstallUtil.exe.630000.3.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.2.InstallUtil.exe.630000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.InstallUtil.exe.630000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.carterandcone.comZ	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://OKJTye.com	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.carterandcone.com4	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	URL Reputation	safe	
http://www.carterandcone.comB	0%	URL Reputation	safe	
http://www.rcsc.lt/repository0	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://www.google.comT	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.correo.com.uy/correocert/cps.pdf0	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://7lPQxKUhrmku.org	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crt08	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://ns.ado/1yP	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.oaticerts.com/repository.	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.carterandcone.comic-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
multimetals.cfd	192.185.37.183	true	false		unknown
www.google.com	142.250.185.132	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	InstallUtil.exe, 0000000A.00000003.494116501.00000000005BFF000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496829199.0000000005C0A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	InstallUtil.exe, 0000000A.00000003.496161057.000000000637C000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496626164.000000000637E000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html/	B35@6B.exe, 00000000.00000003.246719543.000000000C5A9000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.246455927.000000000C5A6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.dhimyotis.com/certignarootca.crl0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	InstallUtil.exe, 0000000A.00000003.496161057.000000000637C000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	InstallUtil.exe, 0000000A.00000003.495723205.000000000636F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.494909642.0000000006360000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	InstallUtil.exe, 0000000A.00000003.495665837.000000006355000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495356932.0000000005BCE000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.517974136.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	B35@6B.exe, 00000000.00000003.245908483.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.246675183.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.245973902.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.246009181.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.245546404.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.246108229.000000000C5C6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	InstallUtil.exe, 0000000A.00000003.495487980.000000005BC8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	B35@6B.exe, 00000000.00000002.290388561.00000000031B1000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000002.432584864.0000000002B31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	B35@6B.exe, 00000000.00000003.243338541.000000000C593000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243479887.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243541779.000000000C595000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	InstallUtil.exe, 0000000A.00000002.506967470.000000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://pki.registradores.org/normativa/index.htm0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://policy.camerfirma.com0	InstallUtil.exe, 0000000A.00000003.495228110.000000005BD9000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.494909642.0000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	InstallUtil.exe, 0000000A.00000003.495356932.000000005BCE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	InstallUtil.exe, 0000000A.00000003.496083673.000000006381000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	InstallUtil.exe, 0000000A.00000003.494909642.000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	InstallUtil.exe, 0000000A.00000002.517031388.000000005C2F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.516809161.0000000005BFF000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.516089255.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.511725863.0000000002926000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.512386843.0000000002972000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comZ	B35@6B.exe, 00000000.00000003.243479887.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243541779.000000000C595000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	InstallUtil.exe, 0000000A.00000003.494788620.000000005BDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	InstallUtil.exe, 0000000A.00000003.496083673.000000006381000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	InstallUtil.exe, 0000000A.00000003.494909642.000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	InstallUtil.exe, 0000000A.00000003.494409848.000000005C2F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496795773.0000000005C38000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	InstallUtil.exe, 0000000A.00000003.495228110.000000005BD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	InstallUtil.exe, 0000000A.00000002.506967470.000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	InstallUtil.exe, 0000000A.00000003.496083673.000000006381000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	InstallUtil.exe, 0000000A.00000002.516089255.000000005B40000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496284015.0000000005B94000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	InstallUtil.exe, 0000000A.00000003.495665837.000000006355000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.oces.trust2408.com/oces.crl0	InstallUtil.exe, 0000000A.00000003.495356932.000000005BCE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	InstallUtil.exe, 0000000A.00000003.494909642.000000006360000.00000004.00000800.00020000.00000000.sdmp	false		high
http://certs.oaticerts.com/repository/OATICA2.crl	InstallUtil.exe, 0000000A.00000003.496726197.000000005BD6000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.516627598.0000000005BD6000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495356932.0000000005BCE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	InstallUtil.exe, 0000000A.00000003.495228110.000000005BD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	InstallUtil.exe, 0000000A.00000003.495665837.000000006355000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	InstallUtil.exe, 0000000A.00000003.495771329.000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://OKJTye.com	InstallUtil.exe, 0000000A.00000002.506967470.000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	InstallUtil.exe, 0000000A.00000003.494909642.000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	InstallUtil.exe, 0000000A.00000003.495665837.000000006355000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495356932.0000000005BCE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	InstallUtil.exe, 0000000A.00000003.494909642.000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	InstallUtil.exe, 0000000A.00000003.496004090.000000006387000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.com4	B35@6B.exe, 00000000.00000003.243338541.000000000C593000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.securetrust.com/SGCA.crl0	InstallUtil.exe, 0000000A.00000002.516089255.000000005B40000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

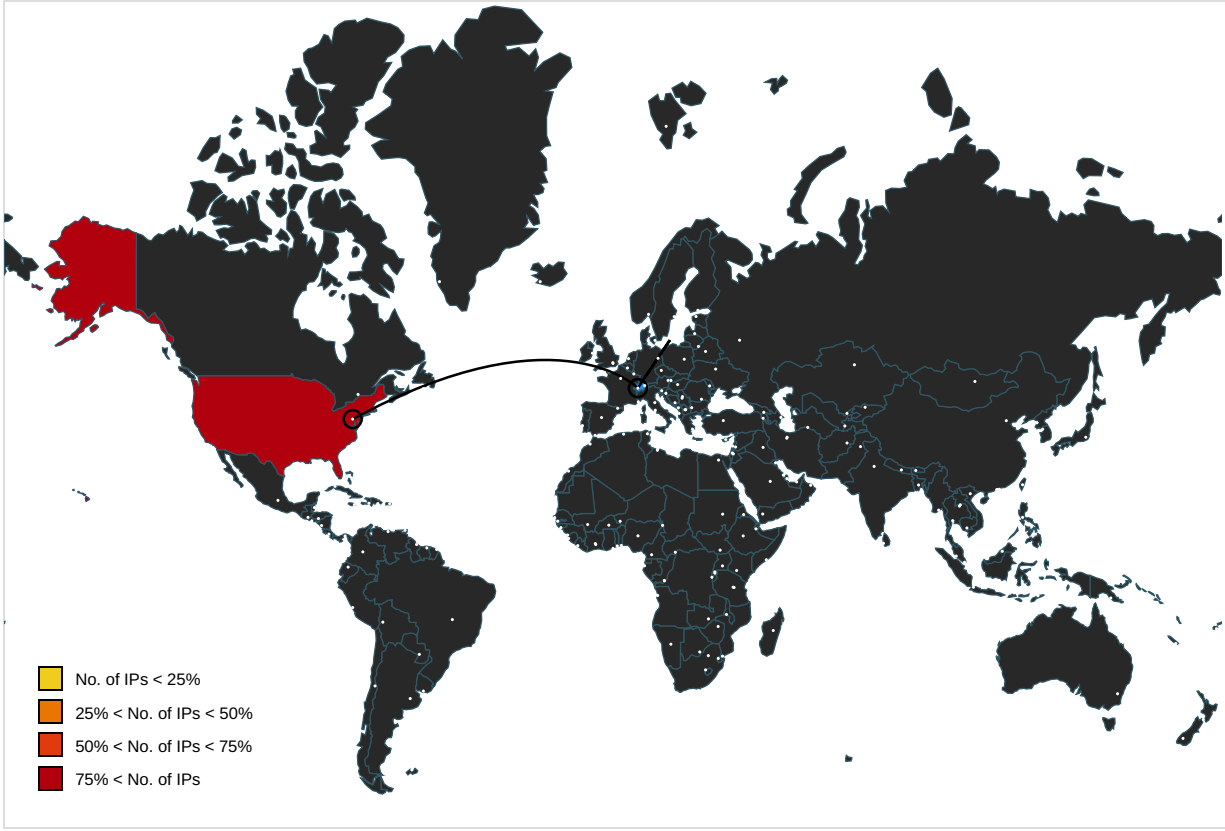
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.agesic.gub.uy/acrn/acrn.crl0)	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comB	B35@6B.exe, 00000000.00000003.243479887.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243541779.000000000C595000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	InstallUtil.exe, 0000000A.00000003.495665837.00000000006355000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	InstallUtil.exe, 0000000A.00000003.495356932.0000000005BCE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.comT	B35@6B.exe, 00000000.00000002.290388561.00000000031B1000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000002.432584864.0000000002B31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadisglobal.com/cps0	InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	InstallUtil.exe, 0000000A.00000002.516089255.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.511725863.0000000002926000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.517974136.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.512386843.0000000002972000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	InstallUtil.exe, 0000000A.00000002.516089255.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.511725863.0000000002926000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.517974136.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.512386843.0000000002972000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.correo.com.uy/correocert/cps.pdf0	InstallUtil.exe, 0000000A.00000003.494116501.0000000005BFF000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496829199.0000000005C0A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	InstallUtil.exe, 0000000A.00000002.506967470.000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://7lPQxKUhrmku.org	InstallUtil.exe, 0000000A.00000002.512055045.0000000002948000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.511374769.00000000028E8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	InstallUtil.exe, 0000000A.00000003.495228110.0000000005BD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.ado/1yP	pot.exe, 00000001.00000003.311383323.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.411228926.000000000BEA8000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.413434243.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.307834538.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.314434884.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.309793041.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.310985083.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.317213060.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.308761023.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.314204431.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.319967920.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.310639752.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.312141601.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.313899652.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.312675654.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.314567273.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.314769045.000000000BECB000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.308319804.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.311461105.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.309511461.000000000BECA000.00000004.00000800.00020000.00000000.sdmp, pot.exe, 00000001.00000003.411816052.000000000BEC0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.anf.es/AC/RC/ocsp0c	InstallUtil.exe, 0000000A.00000003.496083673.000000006381000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comexc	B35@6B.exe, 00000000.00000003.243479887.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243541779.000000000C595000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.oaticerts.com/repository.	InstallUtil.exe, 0000000A.00000003.495228110.000000005BD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	InstallUtil.exe, 0000000A.00000003.493994696.000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	InstallUtil.exe, 0000000A.00000002.506967470.000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://ocsp.accv.es0	InstallUtil.exe, 0000000A.00000003.495665837.000000006355000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.echoworx.com/ca/root2/cps.pdf0	InstallUtil.exe, 0000000A.00000003.496083673.000000006381000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rca.e-szigno.hu/ocsp0-	InstallUtil.exe, 0000000A.00000003.493994696.00000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	InstallUtil.exe, 0000000A.00000003.495487980.00000000005BC8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-std0	InstallUtil.exe, 0000000A.00000003.496004090.00000000006387000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	B35@6B.exe, 00000000.00000003.242654377.000000000C5BE000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000002.308900248.000000000D822000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.242690897.000000000C5BF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	InstallUtil.exe, 0000000A.00000003.493994696.00000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	B35@6B.exe, 00000000.00000003.246772634.000000000C5A6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel05	InstallUtil.exe, 0000000A.00000003.493994696.00000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	InstallUtil.exe, 0000000A.00000003.495665837.00000000006355000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.gva.es/cps0%	InstallUtil.exe, 0000000A.00000003.495665837.00000000006355000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.cert.fnmt.es/dpcs/0	InstallUtil.exe, 0000000A.00000003.494409848.00000000005C2F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496795773.0000000005C38000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496004090.0000000006387000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-bt0	InstallUtil.exe, 0000000A.00000003.494788620.00000000005BDE000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.516662324.0000000005BE1000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495309733.0000000005BE1000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.493994696.0000000005BE7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.comsign.co.il/cps0	InstallUtil.exe, 0000000A.00000003.494909642.00000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.ado/1	pot.exe, 00000001.00000003.427221317.000000000BED0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 0000000A.00000002.506967470.00000000025C1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.e-me.lv/repository0	InstallUtil.exe, 0000000A.00000003.494550099.00000000063F4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	InstallUtil.exe, 0000000A.00000003.496161057.00000000637C000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.496128218.0000000006375000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495771329.0000000006373000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.494909642.0000000006360000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.495013297.0000000006373000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	InstallUtil.exe, 0000000A.00000003.495723205.00000000636F000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.494909642.0000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comic-	B35@6B.exe, 00000000.00000003.243686727.000000000C593000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.244376914.000000000C59D000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.244356588.000000000C5A6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243874994.000000000C598000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243338541.000000000C593000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243479887.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243834321.000000000C5A0000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.245244855.000000000C5A6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.244623217.000000000C59F000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243541779.000000000C595000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.244576344.000000000C59F000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.243711214.000000000C5A6000.00000004.00000800.00020000.00000000.sdmp, B35@6B.exe, 00000000.00000003.244119845.000000000C59B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.37.183	multimetals.cfd	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.185.132	www.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	672480
Start date and time: 24/07/202217:53:07	2022-07-24 17:53:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	B35@6B.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:	18
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@9/8@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%

HCA Information:	• Successful, ratio: 90% • 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, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.238.189.126, 8.248.143.254, 67.26.83.254, 8.248.145.254, 8.241.126.249
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:54:34	API Interceptor	1x Sleep call for process: B35@6B.exe modified
17:55:00	API Interceptor	210x Sleep call for process: pot.exe modified
17:55:44	API Interceptor	165x Sleep call for process: InstallUtil.exe modified
17:55:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Acrobat C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
17:55:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Acrobat C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<......3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`..u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.I.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....I6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.117486686032403
Encrypted:	false
SSDEEP:	6:kKjF+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:rFNkPlE99SNxAhUeE1
MD5:	73CB15AC02F056D28244E698853528B5
SHA1:	DA327ED34396A489D99AE142804DBD1B555E2C80
SHA-256:	502B90D353CEE81025E252ECF95C09DF708EF89661CB2B37ED30A2F2F0B0178F
SHA-512:	7964520645C46CF53D4A123702C02F04000245AE2CDAFC0CA8628EC62034DA84A8791B2176F56C71A4FB1E3424CCD8853E5F2147F0198B2249D6980FC43007AD
Malicious:	false
Reputation:	low
Preview:	p..... .....(|...(..... .....L.....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

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

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:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEF93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AEA77
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B35@6B.exe.log

Process:	C:\Users\user\Desktop\B35@6B.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MIHKov2HKXwYHKhQnoPtHoxHhAHKzvr3
MD5:	90DA70F21E67A8A3197C9F454FA9CB57
SHA1:	FC0B4A2B0F54E399477E168EEAFE962E6589DF91
SHA-256:	FEA95A3982BE3C224FDDFCE307C75459525FDFE66B5A7E6D83625FF51542F54E
SHA-512:	8563365117151AC0F90DFF6352D766F9A06E7AFCE2A2D949EC2A59DFA7078615BBCE59E6B081F351D45F8BB50793129509810EAF97F8D42ECD4F3B21AB3938C
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

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

Process:	C:\Users\user\AppData\Local\Temp\pot.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4Ko84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4KE4VE4j:MIHKov2HKXwYHKhQnoPtHoxHhAHKzvr3
MD5:	90DA70F21E67A8A3197C9F454FA9CB57
SHA1:	FC0B4A2B0F54E399477E168EEAFE962E6589DF91
SHA-256:	FEA95A3982BE3C224FDDFCE307C75459525FDFE66B5A7E6D83625FF51542F54E
SHA-512:	8563365117151AC0F90DFF6352D766F9A06E7AFCE2A2D949EC2A59DFA7078615BBCE59E6B081F351D45F8BB50793129509810EAF97F8D42ECD4F3B21AB3938C
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b880

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

\Device\ConDrv

Process:	C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404DB3
Malicious:	false
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs 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. Uninstall is not transactioned.....Options take the form /switch=[value]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.8232068623635715
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	B35@6B.exe
File size:	600576
MD5:	6753a24ed2a75dbd488c0a1783f03d05
SHA1:	70c061619c4ebbbb111923257e76cd3cef5b3618
SHA256:	a9b46ddb3ed98e2ca5e71253a69f686e1f618f724821eb98b52b812844117f33
SHA512:	f7ffb706831a980a4fb1a631de7a7e594de3b95f490b869291439c828ed77afce69f168ac5e23b105fca5709d6f07b662a080cdce49dd81fd3db0b938465d588
SSDEEP:	12288:+HND4jk8+eBJ3VhdcZelUbQ/y9vwItbzdEaBy61I38b:+HND4jk8+eBJ3VYZelv5bpEF61I
TLSH:	E6D4E03A3F91A41CC13D07B1047A6AC1A372918A3755CB1EA4C7E3EADF5172BBF22059
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....8].....<... ...@....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x493cde
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5D380A89 [Wed Jul 24 07:36:41 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x93c84	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0x602	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x96000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x91ce4	0x91e00	False	0.6697645538774636	data	6.8368028789554005	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x602	0x800	False	0.3466796875	data	3.6045008467063555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

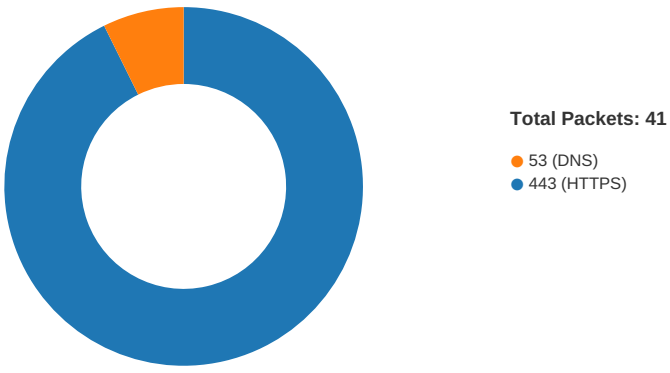
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x940a0	0x378	data		
RT_MANIFEST	0x94418	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 24, 2022 17:54:10.792373896 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:10.792428970 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:10.792521000 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:10.821880102 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:10.821922064 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:10.885759115 CEST	443	49713	142.250.185.132	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 24, 2022 17:54:10.885905027 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:10.891100883 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:10.891132116 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:10.891422033 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:10.941837072 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.212323904 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.252496004 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.281989098 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.282044888 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.282099962 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.282139063 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.282298088 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.282332897 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.282744884 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.283169031 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.283185005 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.283938885 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.284045935 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.284060001 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.285134077 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.285332918 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.285353899 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.286458969 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.286546946 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.286560059 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.301203966 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.301325083 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.301342010 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.301662922 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.301738977 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.301750898 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.303106070 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.303184986 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.303198099 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.304275990 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.304352045 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.304364920 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.305352926 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.305433989 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.305448055 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.306571007 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.306663036 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.306675911 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.307769060 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.307847977 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.307862997 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.308959007 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.309036970 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.309050083 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.310189962 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.310261965 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.310275078 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.311444044 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.311512947 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.311526060 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.312607050 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.312688112 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.312700033 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.314085960 CEST	443	49713	142.250.185.132	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 24, 2022 17:54:11.314157009 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.314173937 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.315335989 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.315409899 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.315423012 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.315548897 CEST	443	49713	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:11.315604925 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:11.318387985 CEST	49713	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.329665899 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.329739094 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:33.329819918 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.404717922 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.404779911 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:33.459418058 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:33.459551096 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.464680910 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.464715004 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:33.465203047 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:33.506261110 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.955151081 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:33.996494055 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038065910 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038162947 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038243055 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038311958 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038331032 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:34.038389921 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.038414955 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:34.038973093 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.039124012 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:34.039141893 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.040553093 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.040607929 CEST	443	49714	142.250.185.132	192.168.2.4
Jul 24, 2022 17:54:34.040648937 CEST	49714	443	192.168.2.4	142.250.185.132
Jul 24, 2022 17:54:34.040672064 CEST	443	49714	142.250.185.132	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 24, 2022 17:54:10.740134954 CEST	53775	53	192.168.2.4	8.8.8.8
Jul 24, 2022 17:54:10.762516975 CEST	53	53775	8.8.8.8	192.168.2.4
Jul 24, 2022 17:54:33.290987968 CEST	54800	53	192.168.2.4	8.8.8.8
Jul 24, 2022 17:54:33.309811115 CEST	53	54800	8.8.8.8	192.168.2.4
Jul 24, 2022 17:56:05.546564102 CEST	60506	53	192.168.2.4	8.8.8.8
Jul 24, 2022 17:56:05.718669891 CEST	53	60506	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 24, 2022 17:54:10.740134954 CEST	192.168.2.4	8.8.8.8	0xaedc	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 24, 2022 17:54:33.290987968 CEST	192.168.2.4	8.8.8.8	0x979b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 24, 2022 17:56:05.546564102 CEST	192.168.2.4	8.8.8.8	0xebf9	Standard query (0)	multimetals.cfd	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 24, 2022 17:54:10.762516975 CEST	8.8.8.8	192.168.2.4	0xaedc	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 24, 2022 17:54:33.309811115 CEST	8.8.8.8	192.168.2.4	0x979b	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)
Jul 24, 2022 17:56:05.718669891 CEST	8.8.8.8	192.168.2.4	0xebf9	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	192.168.2.4	49713	142.250.185.132	443	C:\Users\user\Desktop\B35@6B.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:11 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-07-24 15:54:11 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 24 Jul 2022 15:54:11 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: AEC=AakniGMek99NlxaowW24W4xNN_U526psYorP_WCPyGsImtSoN_tuEFPvtA; expires=Fri, 20-Jan-2023 15:54:11 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=6.SE=lteViqBfFG3rP25uCPTAaJ6QTqimm-nQyRZxXX_2wjWEVpJZxCQ7CMvIZID wP9gjSMwCGD9hAYHc8Uc9bZ_e2LuSkNVTYT0l4NyfAC0QifQkrt_bwmr3KeDJVpB7BYkOWSp8Fw2-HSxgOaSSjFVSM 0FmB30Jw9s5L0mFXhnpwbk; expires=Thu, 24-Aug-2023 08:12:29 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+864; expires=Tue, 23-Jul-2024 15:54:11 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-24 15:54:11 UTC	1	IN	Data Raw: 35 36 33 35 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 Data Ascii: 5635<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-GB"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta cont
2022-07-24 15:54:11 UTC	1	IN	Data Raw: 65 6e 74 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 4d 67 44 4b 30 2d 49 37 4d 36 79 4b 68 59 64 6c 4e 42 47 32 7a 41 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 3d 7b 6b 45 49 3a 27 49 32 76 64 59 75 37 4d 44 59 6d 58 39 75 38 50 30 76 47 62 34 41 51 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 36 30 35 38 2c 32 30 37 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 36 2c 35 2c 31 33 Data Ascii: ent="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google< /title><script nonce="MgDK0-I7M6yKhYdlNBG2zA">(function(){window.google={kEI:'I2vdYu7MDYmX9u8P0vGb4A Q',kEXPI:'0,1302536,56873,6058,207,4804,2316,383,246,5,13
2022-07-24 15:54:11 UTC	2	IN	Data Raw: 39 2c 31 33 38 30 35 39 32 2c 31 32 38 36 35 27 2c 6b 42 4c 3a 27 5a 7a 62 4d 27 7d 3b 67 6f 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 65 6e 2d 47 42 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c 68 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 6e 75 6c 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 Data Ascii: 9,1380592,12865',kBL:'ZzbM'};google.sn='webhp';google.kHL='en-GB';})();(function(){var f=this||self;var h,k= [];function l(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||h}function m(a){for(var b=null;a&&(!a.getAtt

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:11 UTC	3	IN	Data Raw: 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 Data Ascii: .loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.lx=function(){};}).call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfalse");a="1"===c
2022-07-24 15:54:11 UTC	5	IN	Data Raw: 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c Data Ascii: idth:100%}.gbtcb{position:absolute;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility:hidden;text-al
2022-07-24 15:54:11 UTC	6	IN	Data Raw: 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 Data Ascii: argin:0;padding:0}.gbmc{background:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgb
2022-07-24 15:54:11 UTC	7	IN	Data Raw: 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 73 2c 23 67 62 69 34 73 31 7b 66 6f 6e 74 2d Data Ascii: 4c4c4c;background-image:none;_background-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-
2022-07-24 15:54:11 UTC	8	IN	Data Raw: 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c Data Ascii: bnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{display:bl
2022-07-24 15:54:11 UTC	10	IN	Data Raw: 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b Data Ascii: x 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{
2022-07-24 15:54:11 UTC	11	IN	Data Raw: 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 62 6d 70 61 6c 61 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 7d 23 67 62 6d 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a Data Ascii: te-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;padding-right:
2022-07-24 15:54:11 UTC	12	IN	Data Raw: 62 2d 6e 6f 2d 66 6f 63 75 73 3a 66 6f 63 75 73 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c Data Ascii: b-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>14</td><td>IN</td><td>Data Raw: 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77
Data Ascii: ge:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:active{background-color:inherit;-w</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>15</td><td>IN</td><td>Data Raw: 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 62 29
Data Ascii: -image:linear-gradient(top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#fff),to(#fbfbfb)</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>16</td><td>IN</td><td>Data Raw: 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 61 3a 61 63 74 69 76 65 2c 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70
Data Ascii: .1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}#gbmpas{max-height:220p</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>17</td><td>IN</td><td>Data Raw: 67 62 73 62 62 7b 2d 77 65 62 6b 69 74 2d 6d 61 73 6b 2d 62 6f 78 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 2e 35 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 38 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 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
Data Ascii: gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0))</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>19</td><td>IN</td><td>Data Raw: 31 35 35 38 64 36 7d 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 34 62 31 31 61 38 7d 2e 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61
Data Ascii: 1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block}#WqQANb a{displa</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>20</td><td>IN</td><td>Data Raw: 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 65 5d 2c 62 2b 3d 22 26 63 61 64 3d 22 2b 63 28 65 3f 65 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 66 6f 72 28 76 61 72 20 74 20 69 6e 20 64 29 62 2b 3d 22 26 22 2c 62 2b 3d 63 28 74 29 2c 62 2b 3d 22 3d 22 2c 62 2b 3d 63 28 64 5b 74 5d 29 3b 62 3d 62 2b 22 26 65 6d 73 67 3d 22 2b 63 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b 62 3d 62 2b 22 26 6a 73 73 74 3d 22 2b 63 28 61 2e 73 74 61 63 6b 7c 7c 22 4e 2f 41 22 29 3b 31 32 32 38 38 3c 3d 62 2e 6c 65 6e 67 74 68 26 26 28 62 3d 62 2e 73 75 62 73 74 72 28 30 2c 31 32 32 38 38 29 29 3b
Data Ascii: t.documentElement.outerHTML.split("\n")[e],b+="&cad="+c(e?e.substring(0,300):"No script found."));for(var t in d)b+="&",b+=c(t),b+="=",b+=c(d[t]);b=b+"&emsg="+c(a.name+": "+a.message);b=b+"&jsst="+c(a.stack||"N/A");12288<=b.length&&(b=b.substr(0,12288));</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>21</td><td>IN</td><td>Data Raw: 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 3d 66 75 6e
Data Ascii: is,arguments),m=c.apply(this,arguments);return void 0==k?m:void 0==m?k:m&&k}}}var da=function(a){return function(){return g.bv.m==a}},ea=da(1),fa=da(2);p("sb",ea);p("kn",fa);h.a=_tvv;h.b=_tvf;h.c=_tvn;h.i=aa;var r=window.gbar.i.i;var t=function(){},ha=fun</td></tr>
<tr><td>2022-07-24 15:54:11 UTC</td><td>22</td><td>IN</td><td>Data Raw: 65 37 0d 0a 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 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 0d 0a
Data Ascii: e7&&c[0]!=a;++b);!c||c[1].l||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].url,a),c[1].libs&&C&&C(c[1].libs))},ta=function(a){A("gc",a)},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];</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:11 UTC	22	IN	Data Raw: 36 38 39 64 0d 0a 74 72 79 7b 75 61 28 61 29 7d 63 61 74 63 68 28 66 29 7b 7d 7d 7d 3b 70 28 22 6d 64 63 22 2c 76 29 3b 70 28 22 6d 64 69 22 2c 6c 61 29 3b 70 28 22 62 6e 63 22 2c 77 29 3b 70 28 22 71 47 43 22 2c 74 61 29 3b 70 28 22 71 6d 22 2c 42 29 3b 70 28 22 71 64 22 2c 78 29 3b 70 28 22 6c 62 22 2c 44 29 3b 70 28 22 6d 63 66 22 2c 70 61 29 3b 70 28 22 62 63 66 22 2c 6f 61 29 3b 70 28 22 61 71 22 2c 41 29 3b 70 28 22 6d 64 64 22 2c 22 22 29 3b 0a 70 28 22 68 61 73 22 2c 71 61 29 3b 70 28 22 74 72 68 22 2c 76 61 29 3b 70 28 22 74 65 76 22 2c 73 61 29 3b 69 66 28 68 2e 61 28 22 6d 3b 2f 5f 2f 73 63 73 2f 61 62 63 2d 73 74 61 74 69 63 2f 5f 2f 6a 73 2f 6b 3d 67 61 70 69 2e 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 Data Ascii: 689dtry{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("mc f",pa);p("bcf",oa);p("aq",A);p("mdd","");p("has",qa);p("trh",va);p("tev",sa);if(h.a("m;/_/scs/abc-static/_/js/k=gapi.gap i.en.t9z7VPsEMFg.O/d=1/r
2022-07-24 15:54:11 UTC	24	IN	Data Raw: 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 2c 22 26 6a 65 78 70 69 64 3d 22 2c 64 28 22 32 38 38 33 34 22 29 2c 22 26 73 72 63 70 67 3d 22 2c 64 28 22 70 72 6f 70 3d 31 22 29 2c 22 26 6a 73 72 3d 22 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 46 61 29 2c 22 26 6f 67 65 76 3d 22 2c 64 28 22 49 32 76 64 59 76 44 74 44 71 47 68 37 5f 55 50 30 34 65 39 57 41 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 31 35 31 31 30 38 39 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 Data Ascii: www.google.com/gen_204?atyp=i&zx=",(new Date).getTime(),"&jexpid=",d("28834"),"&srcpg=",d("prop=1"),"&jsr=",Math.round(1/Fa),"&ogev=",d("I2vdYvDtDqGh7_UP04e9WA"),"&ogf=",g.bv.f,"&ogrp=",d(""),"&ogv=",d("46151 1089.0"),"&oggv="+d("es_plusone_gc_20220706.0_p
2022-07-24 15:54:11 UTC	25	IN	Data Raw: 41 2e 4f 22 2c 22 2f 72 74 3d 6a 2f 6d 3d 22 2c 61 2c 22 2f 72 73 3d 22 2c 22 41 41 32 59 72 54 76 32 59 6d 4e 78 6b 6f 64 75 52 48 6c 4d 6f 79 4a 7a 6a 6e 75 58 48 68 78 5a 6f 41 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 6c 46 6e 78 6e 77 6b 54 79 4a 55 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 Data Ascii: A.O","/rt=j/m=",a,"/rs=","AA2YrTv2YmNxkoduRHlMoyJzjnuXHhxZoA"];Ka&&a.push("?host=www.gstatic.com&b ust=og.og2.en_US.IFnxnwkTyJU.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;funct
2022-07-24 15:54:11 UTC	26	IN	Data Raw: 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 22 67 62 74 6f 22 29 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 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 6c 6f 73 65 28 61 29 7d 29 7d 2c 65 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 42 28 66 75 6e 63 74 69 6f 6e Data Ascii: owner");if(n.length){var l=document.getElementById(n);l&&l.parentNode&&K(l.parentNode,"gbto")}}}$a (f)&&ab(f);O=d;J(k,"gbto")}}}}B(function(){g.tg(a,b,!0)});bb(a)}catch(q){r(q,"sb","tg")}},db=function(a){B(function(){g. close(a)})},eb=function(a){B(function
2022-07-24 15:54:11 UTC	28	IN	Data Raw: 65 72 26 26 67 2e 61 64 64 48 6f 76 65 72 28 61 29 7d 65 6c 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 7d 63 61 74 63 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 66 6f 72 28 76 61 72 20 63 3d 62 2e 6c 65 6e 67 74 68 2c 0a 64 3d 30 3b 64 3c 63 3b 64 2b 2b 29 69 66 28 48 28 61 2c 62 5b 64 5d 29 29 72 65 74 75 72 6e 21 30 3b 72 65 74 75 72 6e 21 31 7d 2c 68 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 62 28 61 2c 62 2c 63 29 7d 2c 69 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 62 28 61 2c 62 2c 63 2e 70 63 6d 28 29 7d 29 Data Ascii: er&&g.addHover(a)}else k.appendChild(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=function(a,b){gb(a,"gbe",b)},jb=function(){B(f unction(){g.pcm&&g.pcm()})}
2022-07-24 15:54:11 UTC	29	IN	Data Raw: 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 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 65 72 22 2b 61 3b 61 3d 22 6f 66 66 73 65 74 22 2b 61 3b 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 5b 62 5d 3f 77 69 6e 64 6f 77 5b 62 5d 3a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 26 26 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3f 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 5b 61 5d 3a 30 7d Data Ascii: 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]?window[b]:document.documentElement&&document.do cumentElement[a]?document.documentElement[a]:0}
2022-07-24 15:54:11 UTC	30	IN	Data Raw: 6c 47 43 22 2c 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 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 28 29 7b 41 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 Data Ascii: lGC",Cb);h.a("1")&&p("lPWF",Cb)};window.__PVT="";if(h.a("1")&&h.a("1")){var Db=function(a){Cb(function() {A("pw",a);D("pw")})};p("lPW",Db);w.push(["pw",{url:"//ssl.gstatic.com/gb/js/abc/pwm_45f73e4df07a0e388b0fa1f3d30e7 280.js"}]);var Fb=[],Gb=function(a){F
2022-07-24 15:54:11 UTC	31	IN	Data Raw: 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 67 73 72 3d 22 2c 63 2c 22 26 6f 67 76 3d 22 2c 45 2c 55 2c 22 26 6f 67 64 3d 22 2c 49 2c 22 26 6f 67 6c 3d 22 2c 56 2c 22 26 6f 67 63 3d 22 2c 57 2c 22 26 6f 67 75 73 3d 22 2c 79 5d 3b 69 66 28 62 29 7b 22 6f 67 77 22 69 6e 20 62 26 26 28 61 2e 70 75 73 68 28 22 26 6f 67 77 Data Ascii: r 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,"&ogsr=",c,"&ogv=",E,U,"&ogd=",I,"&ogl=",V,"&ogc =",W,"&ogus=",y];if(b){"ogw"in b&&(a.push("&ogw

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:11 UTC	33	IN	Data Raw: 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 28 22 31 22 29 2c 6d 67 3a 22 25 31 24 73 20 28 64 65 6c 65 67 61 74 65 64 29 22 2c 6d 64 3a 22 25 31 24 73 20 28 64 65 66 61 75 6c 74 29 22 2c 6d 68 3a 22 32 32 30 22 2c 73 3a 22 31 22 2c 70 70 3a 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 70 61 67 65 22 7d 3b 76 2e 70 72 66 3d 61 63 7d 3b 76 61 72 20 53 2c 62 63 2c 54 2c 63 63 2c 58 3d 30 2c 64 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 2e 69 6e 64 65 78 4f 66 29 72 65 74 75 72 6e 20 61 2e 69 6e 64 65 78 4f 66 28 62 2c 63 29 3b 69 66 28 41 72 72 61 79 2e 69 6e 64 65 78 4f 66 28 62 2c 63 29 3b 69 66 28 41 72 72 61 79 2e 69 6e 64 65 78 4f Data Ascii: tent.com/ogw/default-user=s96",cp:"1",xp:h.a("1"),mg:"%1$s (delegated)",md:"%1$s (default)",mh:"220",s:"1",pp:Zb,ppl:h.a(""),ppa:h.a(""),ppm:"Google+ page"};v.prf=ac};var S,bc,T,cc,X=0,dc=function(a,b,c){if(a.indexOf)return a.indexOf(b,c);if(Array.indexO
2022-07-24 15:54:11 UTC	34	IN	Data Raw: 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 69 62 75 74 65 28 62 2c 63 29 2c 61 2e 73 61 76 65 28 61 2e 69 64 29 29 29 7d 63 61 74 63 68 28 66 29 7b 66 2e 63 6f 64 65 21 3d 44 4f 4d 45 78 63 65 70 74 69 6f 6e 2e 51 55 4f 54 41 5f 45 58 43 45 45 44 45 44 5f 45 52 52 26 26 72 28 66 2c 22 75 70 22 2c 22 73 70 64 22 29 7d 7d 2c 6e 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 74 72 79 Data Ascii: r&&"undefined"!=typeof a.load},mc=function(a,b,c,d){try{jc(document)||(d||(b="og-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&&r(f,"up","spd")}},nc=function(a,b,c){try
2022-07-24 15:54:11 UTC	35	IN	Data Raw: 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 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,"ml","or")}d?p("ldb",a):c?ca(window,"load",b):b()}p("rdl",rc) Data Ascii: l[1].url,l[0]),l[1].libs&&C&&C(l[1].libs));m<k.length&&setTimeout(a,0)}function b(){0<f--?setTimeout(b,0):a()}var c=h.a("1"),d=h.a(""),f=3,k=w,m=0,n=window.gbarOnReady;if(n)try{n()}catch(l){r(l,"ml","or")}d?p("ldb",a):c?ca(window,"load",b):b()}p("rdl",rc)
2022-07-24 15:54:11 UTC	36	IN	Data Raw: 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 67 29 2c 63 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 5f 22 2b 61 29 3b 62 26 26 66 2e 6c 28 62 2c 68 2e 74 65 73 74 28 62 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 3b 63 26 26 66 2e 6b 28 63 2c 68 2e 74 65 73 74 28 63 2e 63 6c 61 73 73 4e 61 6d 65 29 3f 22 67 62 6d 30 6c 22 3a 22 67 62 7a 30 6c 22 29 7d 63 61 74 63 68 28 6c 29 7b 64 28 6c 2c 22 73 6a 22 2c 22 73 73 70 22 29 7d 67 3d 61 7d 2c 6d 3d 65 2e 71 73 2c 6e 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 61 2e 68 72 65 66 3b 76 61 72 20 63 3d 77 Data Ascii: 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.className)?"gbm0l":"gbz0l")}catch(l){d(l,"sj","ssp")}g=a},m=e.qs,n=function(a){var b=a.href;var c=w
2022-07-24 15:54:11 UTC	38	IN	Data Raw: 79 70 65 5b 6c 5d 3f 6b 5b 6c 5d 3a 6b 5b 6c 5d 3d 7b 7d 3a 6b 5b 6c 5d 3d 67 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 77 69 6e 64 6f 77 2e 67 62 61 72 2e 72 64 6c 28 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f Data Ascii: ype[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 Authors. SPDX-License-Identifier: Apache-2.0*/window.gbar.rdl();}catch(e){window.gbar&&gbar.lo
2022-07-24 15:54:11 UTC	39	IN	Data Raw: 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 65 6e 26 74 61 62 3d 77 38 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 50 6c 61 79 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 74 73 3e 7a 74 20 69 64 3d 67 62 5f 33 36 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 3f 67 6c 3d 47 42 26 74 61 62 3d 77 31 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 59 6f 75 54 75 62 65 3c 2f 73 70 Data Ascii: bzt id=gb_78 href="https://play.google.com/?hl=en&tab=w8">Play <li class=gbt>YouTube</sp
2022-07-24 15:54:11 UTC	40	IN	Data Raw: 43 61 6c 65 6e 64 61 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 63 6f 2e 75 6b 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 54 22 3e 54 72 61 6e 73 6c 61 74 65 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 31 30 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6b 73 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 70 22 3e 42 6f 6f 6b 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d Data Ascii: Calendar <li class=gbmtc>Translate <li class=gbmtc>Books <li class=gbmtc><a class=gbm
2022-07-24 15:54:11 UTC	42	IN	Data Raw: 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 65 6e 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 26 65 63 3d 47 41 5a 41 41 51 22 20 6f 6e 63 6c 69 63 6b 3d 22 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 39 2c 7b 6c 3a 27 69 27 7d 29 22 20 69 64 3d 67 62 5f 37 30 20 63 6c 61 73 73 3d 67 62 67 74 3e 3c 73 70 61 6e 20 63 Data Ascii: Options</h2><ol class=gbtc><li class=gbt><a target=_top href="https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/&ec=GAZAAQ" onclick="gbar.logger.il(9,{l:'i'})" id=gb_70 class=gbgt><span c

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:11 UTC	43	IN	Data Raw: 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 6f 2f 31 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 77 68 69 74 65 5f 62 61 63 6b 67 72 6f 75 6e 64 5f 63 6f 6c 6f 72 5f 32 37 32 78 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 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 Data Ascii: id="lga"><img alt="Google" height="92" src="/images/branding/googlelogo/1x/googlelogo_white_backgr ound_color_272x92dp.png" style="padding:28px 0 14px" width="272" id="hplogo"> <form action="/search" name="f"><table cellpadding="0" cellspacing
2022-07-24 15:54:11 UTC	44	IN	Data Raw: 69 4b 30 65 38 41 41 41 41 41 59 74 31 35 4d 77 52 71 54 56 57 59 51 4c 5a 36 37 34 73 63 4b 33 6e 2d 39 37 59 73 7a 4b 69 58 22 20 6e 61 6d 65 3d 22 69 66 6c 73 69 67 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 74 64 3e 3c 74 64 20 63 6c 61 73 73 3d 22 66 6c 20 73 62 6c 63 22 20 61 6c 69 67 6e 3d 22 6c 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 76 61 6e 63 65 64 5f 73 65 61 72 63 68 3f 68 6c 3d 65 6e 2d 47 42 26 61 6d 70 3b 61 75 74 68 75 73 65 72 3d 30 22 3e 41 64 76 61 6e 63 65 64 20 73 65 61 72 63 68 3c 2f 61 3e 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 61 62 6c 65 3e 3c 69 6e 70 75 74 20 69 64 3d 22 67 62 76 22 20 6e 61 6d 65 3d Data Ascii: iK0e8AAAAAYt15MwRqTVWYQLZ674scK3n-97YszKiX" name="iflsig" type="hidden"></td><td class="fl sblc" align="left" nowrap="" width="25%">Advanced se arch</td></tr></table><input id="gbv" name=
2022-07-24 15:54:11 UTC	45	IN	Data Raw: 64 69 76 3e 3c 2f 64 69 76 3e 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 70 74 3b 63 6f 6c 6f 72 3a 23 37 30 37 35 37 61 22 3e 26 63 6f 70 79 3b 20 32 30 32 32 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 70 6f 6c 69 63 69 65 73 2f 70 72 69 76 61 63 79 2f 22 3e 50 72 69 76 61 63 79 3c 2f 61 3e 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 54 65 72 6d 73 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 4d 67 44 4b 30 2d 49 37 4d 36 79 4b 68 59 64 6c 4e 42 47 32 7a 41 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 2e 63 64 6f 3d 7b 68 65 69 67 68 74 3a Data Ascii: div> © 2022 - Privacy - Terms <script nonce="MgDK0-I7M6yKhYdlNBG2zA">(function(){window.google.cdo={height:
2022-07-24 15:54:11 UTC	47	IN	Data Raw: 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 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 Data Ascii: IPT";"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",{createHTML:e,createScript:e,crea teScriptURL:e})}catch(q){d.console&&d
2022-07-24 15:54:11 UTC	48	IN	Data Raw: 68 5c 78 32 32 2c 5c 78 32 32 64 79 6d 5c 78 32 32 3a 5c 78 32 32 44 69 64 20 79 6f 75 20 6d 65 61 6e 3a 5c 78 32 32 2c 5c 78 32 32 6c 63 6b 79 5c 78 32 32 3a 5c 78 32 32 49 5c 5c 75 30 30 32 36 23 33 39 3b 6d 20 46 65 65 6c 69 6e 67 20 4c 75 63 6b 79 5c 78 32 32 2c 5c 78 32 32 6c 6d 6c 5c 78 32 32 3a 5c 78 32 32 4c 65 61 72 6e 20 6d 6f 72 65 5c 78 32 32 2c 5c 78 32 32 6f 73 6b 74 5c 78 32 32 3a 5c 78 32 32 49 6e 70 75 74 20 74 6f 6f 6c 73 5c 78 32 32 2c 5c 78 32 32 70 73 72 63 5c 78 32 32 3a 5c 78 32 32 54 68 69 73 20 73 65 61 72 63 68 20 77 61 73 20 72 65 6d 6f 76 65 64 20 66 72 6f 6d 20 79 6f 75 72 20 5c 5c 75 30 30 33 43 61 20 68 72 65 66 5c 78 33 64 5c 5c 5c 78 32 32 2f 68 69 73 74 6f 72 79 5c 5c 5c 78 32 32 5c 5c 75 30 30 33 45 57 65 62 20 48 69 73 Data Ascii: h\x22,\x22dym\x22:\x22Did you mean:\x22,\x22lcky\x22:\x22I\\u0026#39;m Feeling Lucky\x22,\x22lml\x 22:\x22Learn more\x22,\x22oskt\x22:\x22Input tools\x22,\x22psrc\x22:\x22This search was removed from your \\u003Ca href\x3d\\\x22/history\\\x22\\u003EWeb His
2022-07-24 15:54:11 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	192.168.2.4	49714	142.250.185.132	443	C:\Users\user\Desktop\B35@6B.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:33 UTC	49	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	49	IN	HTTP/1.1 200 OK Date: Sun, 24 Jul 2022 15:54:33 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=AakniGPy_B-J3ibkif6wYtRKD7j355ubJj89mlpY_Dtl1IsLpphUKyNPmrw; expires=Fri, 20-Jan-2023 15:54:34 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=6.SE=R9j0hhYDGTeqtLlByfY3tFkmRp-xSrS59qyeJEQ6oQcyllEYn1fPBsapAXsxRUVt4l8U0naUeTP1r9GQuniN2gxUSiMjOawiwXb-V_H4J5EgM2P0RpBGhBrDXHYRlWE_1GtHS807cJqjSxrM97AOiKJzzh25bqx7wVCB_Al34SY; expires=Thu, 24-Aug-2023 08:12:51 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+372; expires=Tue, 23-Jul-2024 15:54:33 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-24 15:54:34 UTC	50	IN	Data Raw: 35 35 39 64 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e Data Ascii: 559d<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-GB"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta con
2022-07-24 15:54:34 UTC	50	IN	Data Raw: 74 65 6e 74 3d 22 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 67 2f 31 78 2f 67 6f 67 6c 65 67 5f 73 74 61 6e 64 61 72 64 5f 63 6f 6c 6f 72 5f 31 32 38 64 70 2e 70 6e 67 22 20 69 74 65 6d 70 72 6f 70 3d 22 69 6d 61 67 65 22 3e 3c 74 69 74 6c 65 3e 47 6f 6f 67 6c 65 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 5f 38 57 44 4d 36 76 77 44 74 33 56 5a 31 34 73 48 31 58 48 4c 51 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 4f 57 76 64 59 73 79 67 4f 37 36 38 78 63 38 50 67 76 32 58 30 41 51 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 36 38 37 33 2c 31 37 31 30 2c 34 33 34 38 2c 32 30 37 2c 34 38 30 34 2c 32 33 31 36 2c 33 38 33 2c 32 34 Data Ascii: tent="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="_8WDM6vwDt3VZ14sH1XHLQ">(function(){window.google={kEI:'OWvdYsygO768xc8Pgv2X0AQ',kEXPI:'0,1302536,56873,1710,4348,207,4804,2316,383,24
2022-07-24 15:54:34 UTC	51	IN	Data Raw: 32 2c 31 39 36 34 2c 32 39 33 35 2c 31 35 39 2c 31 33 35 38 2c 31 32 32 32 30 2c 33 34 30 36 2c 35 34 34 34 2c 31 34 38 33 2c 32 34 35 2c 31 33 38 30 35 39 33 2c 31 32 38 36 35 27 2c 6b 42 4c 3a 27 5a 7a 62 4d 27 7d 3b 67 6f 6f 67 6c 65 2e 73 6e 3d 27 77 65 62 68 70 27 3b 67 6f 6f 67 6c 65 2e 6b 48 4c 3d 27 65 6e 2d 47 42 27 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 76 61 72 20 66 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 68 2c 6b 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 6c 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 65 69 64 22 29 29 29 3b 29 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 72 65 74 75 72 6e 20 62 7c 7c Data Ascii: 2,1964,2935,159,1358,12220,3406,5444,1483,245,1380593,12865',kBL:'ZzbM'};google.sn='webhp';google.kHL='en-GB';})();(function(){var f=this||self;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||
2022-07-24 15:54:34 UTC	53	IN	Data Raw: 69 6f 6e 28 61 2c 62 2c 63 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 5b 61 5d 2c 62 2c 63 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d Data Ascii: ion(a,b,c){google.lq.push([[a],b,c])};google.loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.lx=function(){};}).call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=
2022-07-24 15:54:34 UTC	54	IN	Data Raw: 76 65 7d 23 67 62 62 77 7b 6c 65 66 74 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 33 30 70 78 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e Data Ascii: ve}#gbbw{left:0;position:absolute;top:30px;width:100%}.gbtcb{position:absolute;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-in
2022-07-24 15:54:34 UTC	55	IN	Data Raw: 2e 67 62 6d 63 2c 2e 67 62 6d 63 63 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 Data Ascii: .gbmc,.gbmcc{display:block;list-style:none;margin:0;padding:0}.gbmc{background:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*d

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	56	IN	Data Raw: 63 75 73 2c 2e 67 62 67 74 2d 68 76 72 2c 2e 67 62 67 74 3a 66 6f 63 75 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d Data Ascii: cus,.gbgt-hvr,.gbgt:focus{background-color:#4c4c4c;background-image:none;_background-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-
2022-07-24 15:54:34 UTC	58	IN	Data Raw: 3a 2d 36 70 78 20 2d 32 32 70 78 7d 2e 67 62 6e 20 2e 67 62 6d 74 2c 2e 67 62 6e 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f Data Ascii: :-6px -22px}.gbn .gbmt,.gbn .gbmt:visited,.gbnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:no
2022-07-24 15:54:34 UTC	59	IN	Data Raw: 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 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 Data Ascii: ow:0 2px 4px rgba(0,0,0,.12);box-shadow:0 2px 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolu
2022-07-24 15:54:34 UTC	60	IN	Data Raw: 72 69 66 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 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 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 Data Ascii: rif;line-height:27px;padding:10px 20px 0;white-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}
2022-07-24 15:54:34 UTC	61	IN	Data Raw: 20 30 20 30 20 31 70 78 20 23 66 66 66 2c 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 2d 6e 6f 2d 66 6f 63 75 73 3a 66 6f 63 75 73 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 37 39 65 64 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 Data Ascii: 0 0 1px #fff,0 1px 1px rgba(0,0,0,.1)}.gbqfb-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgb
2022-07-24 15:54:34 UTC	63	IN	Data Raw: 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 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 Data Ascii: gradient(top,#4d90fe,#357ae8);background-image:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae
2022-07-24 15:54:34 UTC	64	IN	Data Raw: 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 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 Data Ascii: ear-gradient(top,#f8f8f8,#f1f1f1);background-image:linear-gradient(top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear
2022-07-24 15:54:34 UTC	65	IN	Data Raw: 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 63 6f 6c 6f 72 3a 23 32 32 32 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 71 66 62 62 3a 61 63 74 69 76 65 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 Data Ascii: ,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	67	IN	Data Raw: 65 62 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 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 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 Data Ascii: eb;border-color:rgba(0,0,0,.3);top:0}.gbsb .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,lef
2022-07-24 15:54:34 UTC	68	IN	Data Raw: 74 69 76 65 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 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 Data Ascii: tive{text-decoration:underline}.fl a{color:#1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;heig
2022-07-24 15:54:34 UTC	69	IN	Data Raw: 63 28 6c 29 2c 65 26 26 6c 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 65 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 65 5d 2c 62 2b 3d 22 26 63 61 64 3d 22 2b 63 28 65 3f 65 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 33 30 30 29 3a 22 4e 6f 20 73 63 72 69 70 74 20 66 6f 75 6e 64 2e 22 29 29 3b 66 6f 72 28 76 61 72 20 74 20 69 6e 20 64 29 62 2b 3d 22 26 22 2c 62 2b 3d 63 28 74 29 2c 62 2b 3d 22 3d 22 2c 62 2b 3d 63 28 64 5b 74 5d 29 3b 62 3d 62 2b 22 26 65 6d 73 67 3d 22 2b 63 28 61 2e 6e 61 6d 65 2b 22 3a 20 22 2b 61 2e 6d 65 73 73 61 67 65 29 3b 62 3d 62 2b 22 26 6a 73 73 74 3d 22 2b 63 28 61 2e 73 74 61 63 6b 7c 7c 22 4e Data Ascii: c(l),e&&l===window.location.href&&(e=document.documentElement.outerHTML.split("\n")[e],b+="&cad="+c(e?e.substring(0,300):"No script found.")));for(var t in d)b+="&",b+=c(t),b+="=",b+=c(d[t]);b=b+"&emsg="+c(a.name+": "+a.message);b=b+"&jsst="+c(a.stack||"N
2022-07-24 15:54:34 UTC	70	IN	Data Raw: 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 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 Data Ascii: {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("sb",ea);p("kn",fa);h.a=_tvv;h.b=_tvf;h.c=_tvn;h.i=aa;var
2022-07-24 15:54:34 UTC	71	IN	Data Raw: 64 39 0d 0a 62 7c 7c 22 55 4e 4b 22 29 2b 22 20 75 72 6c 3d 22 2b 61 29 29 7d 29 3b 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 78 6a 73 63 22 29 7c 7c 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 7c 7c 0a 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 63 29 7d 2c 44 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 28 63 3d 77 5b 62 5d 29 26 26 63 5b 30 5d 21 3d 61 3b 2b 2b 62 29 3b 21 63 7c 7c 63 5b 31 0d 0a Data Ascii: d9b||"UNK")+" url="+a)})};(document.getElementById("xjsc")||document.getElementsByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(c)},D=function(a){for(var b=0,c;(c=w[b])&&c[0]!=a;++b);!c||c[1
2022-07-24 15:54:34 UTC	71	IN	Data Raw: 36 39 37 31 0d 0a 5d 2e 6c 7c 7c 63 5b 31 5d 2e 73 7c 7c 28 63 5b 31 5d 2e 73 3d 21 30 2c 73 61 28 32 2c 61 29 2c 63 5b 31 5d 2e 75 72 6c 26 26 72 61 28 63 5b 31 5d 2e 75 72 6c 2c 61 29 2c 63 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 63 5b 31 5d 2e 6c 69 62 73 29 29 7d 2c 74 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 67 63 22 2c 61 29 7d 2c 75 61 3d 6e 75 6c 6c 2c 76 61 3d 66 75 6e 63 74 69 6f 6e 28 61 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 Data Ascii: 6971].l||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].url,a),c[1].libs&&C&&C(c[1].libs))},ta=function(a){A("gc",a)},ua=null,va=function(a){ua=a},sa=function(a,b,c){if(ua){a={t:a,b:b};if(c)for(var d in c)a[d]=c[d];try{ua(a)}catch(f){}}};p("mdc",v);p("mdi
2022-07-24 15:54:34 UTC	73	IN	Data Raw: 6c 3a 22 65 6e 22 7d 3b 76 2e 67 6c 3d 45 61 3b 77 61 3f 41 61 2e 6c 6f 61 64 7c 7c 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3a 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3b 70 28 22 64 67 6c 22 2c 42 61 29 3b 70 28 22 61 67 6c 22 2c 44 61 29 3b 68 2e 6f 3d 78 61 7d 3b 76 61 72 20 46 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 30 30 31 29 2c 47 61 3d 30 3b 0a 66 75 6e 63 74 69 6f 6e 20 5f 6d 6c 54 6f 6b 65 6e 28 61 2c 62 29 7b 74 72 79 7b 69 66 28 31 3e 47 61 29 7b 47 61 2b 2b 3b 76 61 72 20 63 3d 61 3b 62 3d 62 7c 7c 7b 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 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 65 29 2e Data Ascii: l:"en"};v.gl=Ea;wa?Aa.load||p("load",Ba,Aa):p("load",Ba,Aa);p("dgl",Ba);p("agl",Da);h.o=xa};var Fa=h.b("0.1",.001),Ga=0;function _mlToken(a,b){try{if(1>Ga){Ga++;var c=a;b=b||{};var d=encodeURIComponent,f=["//www.google.com/gen_204?atyp=i&zx=",(new Date).
2022-07-24 15:54:34 UTC	74	IN	Data Raw: 28 61 2c 62 29 7b 48 28 61 2c 62 29 3f 4b 28 61 2c 62 29 3a 4a 28 61 2c 62 29 7d 2c 4e 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 2c 4f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3f 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 22 2c 22 2f 6f 67 2f 5f 2f 6a 73 2f 64 3d 31 2f 6b 3d 22 2c 22 6f 67 2e 6f 67 32 2e 65 6e 5f 55 53 2e 68 79 6a 56 6d 61 75 61 37 79 41 2e 4f 22 2c 22 2f 72 74 3d 6a 2f 6d 3d 22 2c 61 2c 22 2f 72 73 3d 22 2c 22 41 41 32 59 72 54 76 32 59 6d 4e 78 6b 6f 64 75 52 48 6c Data Ascii: (a,b){H(a,b)?K(a,b):J(a,b)},Na=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})},Oa=function(a){a=[La?"":"https://www.gstatic.com","/og/_/js/d=1/k=","og.og2.en_US.hyjVmaua7yA.O","/rt=j/m=",a,"/rs=","AA2YrTv2YmNxkoduRHl

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	75	IN	Data Raw: 74 65 28 22 61 72 69 61 2d 6f 77 6e 73 22 29 3b 69 66 28 64 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 66 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 64 29 3b 69 66 28 66 29 7b 76 61 72 20 6b 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 69 66 28 4f 3d 3d 64 29 4f 3d 76 6f 69 64 20 30 2c 0a 4b 28 6b 2c 22 67 62 74 6f 22 29 3b 65 6c 73 65 7b 69 66 28 4f 29 7b 76 61 72 20 6d 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 4f 29 3b 69 66 28 6d 26 26 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 29 7b 76 61 72 20 6e 3d 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 6f 77 6e 65 72 22 29 3b 69 66 28 6e 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 6c 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e Data Ascii: te("aria-owns");if(d.length){var f=document.getElementById(d);if(f){var k=b.parentNode;if(O==d)O=void 0,K(k,"gbto");else{if(O){var m=document.getElementById(O);if(m&&m.getAttribute){var n=m.getAttribute("aria-owner");if(n.length){var l=document.getElemen
2022-07-24 15:54:34 UTC	77	IN	Data Raw: 29 7c 7c 28 6c 3d 64 29 7d 62 72 65 61 6b 7d 30 3c 64 26 26 64 2b 31 3c 6e 26 26 64 2b 2b 7d 69 66 28 30 3c 3d 6c 29 7b 76 61 72 20 79 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 79 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 63 22 3b 7a 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 20 67 62 6d 68 22 3b 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 7a 29 3b 6b 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 79 2c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 6c 5d 29 7d 67 2e 61 64 64 48 6f 76 65 72 26 26 67 2e 61 64 64 48 6f 76 65 72 28 61 29 7d 65 6c 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 63 61 74 63 Data Ascii:)||(l=d)}break}0<d&&d+1<n&&d++}if(0<=l){var y=document.createElement("li"),z=document.createElement("div");y.className="gbmtc";z.className="gbmt gbmh";y.appendChild(z);k.insertBefore(y,k.childNodes[l])}g.addHover&&g.addHover(a)}else k.appendChild(m)}}catc
2022-07-24 15:54:34 UTC	78	IN	Data Raw: 3b 63 3d 30 3b 66 6f 72 28 76 61 72 20 66 3b 66 3d 62 5b 63 5d 3b 63 2b 2b 29 7b 76 61 72 20 6b 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 0a 6b 2e 69 6e 6e 65 72 48 54 4d 4c 3d 66 3b 64 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6b 29 7d 7d 65 6c 73 65 20 64 2e 69 6e 6e 65 72 48 54 4d 4c 3d 62 3b 51 28 61 2c 21 30 29 7d 7d 7d 2c 51 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 28 62 3d 76 6f 69 64 20 30 21 3d 3d 62 3f 62 3a 21 30 29 3f 4a 28 61 2c 22 67 62 6d 73 67 6f 22 29 3a 4b 28 61 2c 22 67 62 6d 73 67 6f 22 29 7d 2c 24 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 76 61 72 20 62 3d 30 2c 63 3b 63 3d 61 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 62 5d 3b 62 2b 2b 29 69 66 28 48 28 63 2c 22 67 62 6d 73 67 Data Ascii: ;c=0;for(var f;f=b[c];c++){var k=document.createElement("div");k.innerHTML=f;d.appendChild(k)}}else d.innerHTML=b;Q(a,!0)}}},Q=function(a,b){(b=void 0!==b?b:!0)?J(a,"gbmsgo"):K(a,"gbmsgo")},$a=function(a){for(var b=0,c;c=a.childNodes[b];b++)if(H(c,"gbmsg
2022-07-24 15:54:34 UTC	79	IN	Data Raw: 6c 69 62 73 3a 22 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6c 69 65 6e 74 3a 67 61 70 69 2e 69 66 72 61 6d 65 73 22 7d 5d 29 3b 76 61 72 20 42 62 3d 7b 76 65 72 73 69 6f 6e 3a 22 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 69 6e 64 65 78 3a 22 22 2c 6c 61 6e 67 3a 22 65 6e 22 7d 3b 76 2e 67 63 3d 42 62 3b 76 61 72 20 43 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 77 69 6e 64 6f 77 2e 67 6f 6f 67 6c 65 61 70 69 73 26 26 77 69 6e 64 6f 77 2e 69 66 72 61 6d 65 73 3f 61 26 26 61 28 29 3a 28 61 26 26 74 61 28 61 29 2c 44 28 22 67 63 22 29 29 7d 3b 70 28 22 6c 47 43 22 2c 43 62 29 3b 68 2e 61 28 22 31 22 29 26 26 70 28 22 6c 50 57 46 22 2c 43 62 29 7d 3b 77 69 6e 64 6f 77 2e 5f 5f 50 56 54 Data Ascii: libs:"googleapis.client:gapi.iframes"}]);var Bb={version:"gci_91f30755d6a6b787dcc2a4062e6e9824.js",index:"",lang:"en"};v.gc=Bb;var Cb=function(a){window.googleapis&&window.iframes?a&&a():(a&&ta(a),D("gc"))};p("lGC",Cb);h.a("1")&&p("lPWF",Cb)};window.__PVT
2022-07-24 15:54:34 UTC	80	IN	Data Raw: 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 6b 3d 64 28 22 32 38 38 33 34 22 29 3b 6d 3d 64 28 22 4f 57 76 64 59 71 62 4c 50 4a 69 52 78 63 38 50 77 72 61 75 69 41 73 22 29 3b 76 61 72 20 6c 3d 67 2e 62 76 2e 66 2c 71 3d 64 28 22 31 22 29 3b 6e 3d 64 28 6e 29 3b 63 3d 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 63 29 3b 76 61 72 20 45 3d 64 28 22 34 36 31 35 31 31 30 38 39 2e 30 22 29 2c 55 3d 22 26 6f 67 76 3d 22 2b 64 28 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 32 30 36 30 37 2e 31 5f 70 30 22 29 2c 49 3d 64 28 22 63 6f 6d 22 29 2c 56 3d 64 28 22 65 6e 22 29 2c 57 3d 0a 64 28 22 47 42 52 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 Data Ascii: w Date).getTime();k=d("28834");m=d("OWvdYqbLPJiRxc8PwrauiAs");var l=g.bv.f,q=d("1");n=d(n);c=Math.round(1/c);var E=d("461511089.0"),U="&oggv="+d("es_plusone_gc_20220607.1_p0"),I=d("com"),V=d("en"),W=d("GBR");var y=0;h.a("")&&(y|=1);h.a("")&&(y|=2);h.a(""
2022-07-24 15:54:34 UTC	82	IN	Data Raw: 65 72 3d 73 32 34 22 7d 2c 0a 24 62 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 64 28 29 7d 29 7d 3b 70 28 22 73 70 6e 22 2c 56 62 29 3b 70 28 22 73 70 70 22 2c 58 62 29 3b 70 28 22 73 70 73 22 2c 57 62 29 3b 70 28 22 73 70 64 22 2c 24 62 29 3b 70 28 22 70 61 61 22 2c 54 62 29 3b 70 28 22 70 72 6d 22 2c 55 62 29 3b 6d 62 28 22 67 62 64 34 22 2c 55 62 29 3b 0a 69 66 28 68 2e 61 28 22 22 29 29 7b 76 61 72 20 61 63 3d 7b 64 3a 68 2e 61 28 22 22 29 2c 65 3a 22 22 2c 73 61 6e 77 3a 68 2e 61 28 22 22 29 2c 70 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 Data Ascii: er=s24"},$b=function(){B(function(){g.spd()})};p("spn",Vb);p("spp",Xb);p("sps",Wb);p("spd",$b);p("paa",Tb);p("prm",Ub);mb("gbd4",Ub);if(h.a(""")){var ac={d:h.a(""),e:"",sanw:h.a(""),p:"https://lh3.googleusercontent.com/ogw/default-user=s96",cp:"1",xp:h.a
2022-07-24 15:54:34 UTC	83	IN	Data Raw: 76 61 72 20 62 3d 21 31 3b 74 72 79 7b 62 3d 61 2e 63 6f 6f 6b 69 65 26 26 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 22 50 52 45 46 22 29 7d 63 61 74 63 68 28 63 29 7b 7d 72 65 74 75 72 6e 21 62 7d 2c 6b 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 72 65 74 75 72 6e 21 21 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 7d 63 61 74 63 68 28 61 29 7b 72 65 74 75 72 6e 21 31 7d 7d 2c 6c 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 26 26 61 2e 73 74 79 6c 65 26 26 61 2e 73 74 79 6c 65 2e 62 65 68 61 76 69 6f 72 26 26 22 75 6e 64 65 66 69 6e 65 64 22 21 3d 74 79 70 65 6f 66 20 61 2e 6c 6f 61 64 7d 2c 6d 63 3d 66 75 6e 63 74 69 6f 6e 28 61 Data Ascii: var b=!1;try{b=a.cookie&&a.cookie.match("PREF")}catch(c){}return!b},kc=function(){try{return!!e.localStorage&&"object"==typeof e.localStorage}catch(a){return!1}},lc=function(a){return a&&a.style&&a.style.behavior&&"undefined"!=typeof a.load},mc=function(a
2022-07-24 15:54:34 UTC	84	IN	Data Raw: 22 29 3b 5a 28 67 2e 75 70 2c 22 73 69 22 29 3b 5a 28 67 2e 75 70 2c 22 73 70 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 64 70 63 22 29 3b 5a 28 67 2e 75 70 2c 22 69 69 63 22 29 3b 67 2e 6d 63 66 28 22 75 70 22 2c 7b 73 70 3a 68 2e 62 28 22 30 2e 30 31 22 2c 31 29 2c 74 6c 64 3a 22 63 6f 2e 75 6b 22 2c 70 72 69 64 3a 22 31 22 7d 29 3b 66 75 6e 63 74 69 6f 6e 20 72 63 28 29 7b 66 75 6e 63 74 69 6f 6e 20 61 28 29 7b 66 6f 72 28 76 61 72 20 6c 3b 28 6c 3d 6b 5b 6d 2b 2b 5d 29 26 26 22 6d 22 21 3d 6c 5b 30 5d 26 26 21 6c 5b 31 5d 2e 61 75 74 6f 3b 29 3b 6c 26 26 28 73 61 28 32 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 75 72 6c 26 26 72 61 28 6c 5b 31 5d 2e 75 72 6c 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 6c 5b 31 5d 2e 6c 69 62 73 29 29 3b 6d Data Ascii: ");Z(g.up,"si");Z(g.up,"spl");Z(g.up,"dpc");Z(g.up,"iic");g.mcf("up",{sp:h.b("0.01",1),tld:"co.uk",prid:"1"});function rc(){function a(){for(var l;(l=k[m++])&&"m"!=l[0]&&!l[1].auto;);l&&(sa(2,l[0]),l[1].url&&ra(l[1].url,l[0]),l[1].libs&&C&&C(l[1].libs));m

Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	85	IN	Data Raw: 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 64 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 2e 69 3b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 76 61 72 20 66 3d 65 2e 69 3b 76 61 72 20 67 3d 66 2e 63 28 22 31 22 2c 30 29 2c 68 3d 2f 5c 62 67 62 6d 74 5c 62 2f 2c 6b 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 74 72 79 7b 76 61 72 20 62 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 Data Ascii: l(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var d=window.gbar.i.i;var e=window.gbar;var f=e.i;var g=f.c("1",0),h=/\bgbmt\b/,k=function(a){try{var b =document.getElementB
2022-07-24 15:54:34 UTC	87	IN	Data Raw: 22 29 2c 74 6f 3a 65 28 22 33 30 30 30 30 30 22 29 2c 75 3a 65 28 22 22 29 2c 76 66 3a 22 2e 36 36 2e 22 7d 2c 67 3d 66 2c 68 3d 5b 22 62 6e 64 63 66 67 22 5d 2c 6b 3d 61 3b 68 5b 30 5d 69 6e 20 6b 7c 7c 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6b 2e 65 78 65 63 53 63 72 69 70 74 7c 7c 6b 2e 65 78 65 63 53 63 72 69 70 74 28 22 76 61 72 20 22 2b 68 5b 30 5d 29 3b 66 6f 72 28 76 61 72 20 6c 3b 68 2e 6c 65 6e 67 74 68 26 26 28 6c 3d 68 2e 73 68 69 66 74 28 29 29 3b 29 68 2e 6c 65 6e 67 74 68 7c 7c 76 6f 69 64 20 30 3d 3d 3d 67 3f 6b 3d 6b 5b 6c 5d 26 26 6b 5b 6c 5d 21 3d 3d 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 5b 6c 5d 3f 6b 5b 6c 5d 3a 6b 5b 6c 5d 3d 7b 7d 3a 6b 5b 6c 5d 3d 67 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 Data Ascii: ");to:e("300000"),u:e(""),vf:".66."},g=f,h=["bndcfg"],k=a;h[0]in k||"undefined"==typeof k.execScript||k.exec Script("var "+h[0];for(var l;h.length&&(l=h.shift());)h.length||void 0===g?k=k[l]&&k[l]!==Object.prototype[l]?k[l]:k[l]={}:k[l]=g ;}catch(e){window
2022-07-24 15:54:34 UTC	88	IN	Data Raw: 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 49 6d 61 67 65 73 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 70 73 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 6d 61 70 73 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 6c 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 73 3e 4d 61 70 73 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 37 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 6c 61 79 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f Data Ascii: Images <li class=gbt>Maps <li class=gbt><a cla ss=gbzt id=gb_78 href="https://play.google.com/
2022-07-24 15:54:34 UTC	89	IN	Data Raw: 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 6d 20 69 64 3d 67 62 64 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 7a 74 6d 3e 3c 64 69 76 20 69 64 3d 67 62 6d 6d 62 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 20 67 62 73 62 69 73 22 3e 3c 6f 6c 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 69 63 22 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 69 64 3d 67 62 5f 32 34 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 61 6c 65 6e 64 61 72 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 63 61 6c 65 6e 64 61 72 3f 74 61 62 3d 77 63 22 3e 43 61 6c 65 6e 64 61 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 Data Ascii:);</script> <ol id=gbmm class="gbmcc gbsbic"><li class=gbmtc>Calendar <li class=gbmtc><a class=g
2022-07-24 15:54:34 UTC	91	IN	Data Raw: 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e 6c 6f 67 67 65 72 2e 69 6c 28 31 2c 7b 74 3a 36 36 7d 29 3b 3b 20 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 73 62 74 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 67 62 73 62 62 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 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 Data Ascii: ').addEventListener('click', function clickHandler() { gbar.logger.il(1,{t:66});; });</script> <div class=gbs bt> <h2 class=gbxx>Account Options</h2><ol c
2022-07-24 15:54:34 UTC	92	IN	Data Raw: 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 2f 6f 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 33 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 67 62 78 34 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 5f 38 57 44 4d 36 76 77 44 74 33 56 5a 31 34 73 48 31 58 48 4c 51 27 3e 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 65 6c 70 26 26 67 62 61 72 2e 65 6c 70 28 29 3c 2f 73 63 72 69 70 74 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 63 65 6e 74 65 72 3e 3c 62 72 20 63 6c 65 61 72 3d 22 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 Data Ascii: li> <script nonce='_8W DM6vwDt3VZ14sH1XHLQ'>window.gbar&&gbar.elp&&gbar.elp()</script> <br clear="all" id="lgpd"> <img alt="Google" height="92" src=
2022-07-24 15:54:34 UTC	93	IN	Data Raw: 64 31 27 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 69 64 29 2e 6f 6e 63 6c 69 63 6b 20 3d 20 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 20 28 74 68 69 73 2e 66 6f 72 6d 2e 71 2e 76 61 6c 75 65 29 7b 74 68 69 73 2e 63 68 65 63 6b 65 64 20 3d 20 31 3b 69 66 20 28 74 68 69 73 2e 66 6f 72 6d 2e 69 66 6c 73 69 67 29 74 68 69 73 2e 66 6f 72 6d 2e 69 66 6c 73 69 67 2e 64 69 73 61 62 6c 65 64 20 3d 20 66 61 6c 73 65 3b 7d 0a 65 6c 73 65 20 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 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 41 59 74 31 35 53 54 4e 31 6f 76 50 4a 61 52 4a 48 74 69 32 55 73 4a 69 42 65 53 49 42 62 37 6c 6d 22 Data Ascii: d1';document.getElementById(id).onclick = function(){if (this.form.q.value){this.checked = 1;if (this.form.i flsig)this.form.iflsig.disabled = false;}else top.location='/doodles/';};})();</script><input value="AJiK0e8AAAAAYt15STN 1ovPJaRJHti2UsJiBeSlBb7lm"
2022-07-24 15:54:34 UTC	94	IN	Data Raw: 20 53 6f 6c 75 74 69 6f 6e 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 61 62 6f 75 74 2e 68 74 6d 6c 22 3e 41 62 6f 75 74 20 47 6f 6f 67 6c 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 73 65 74 70 72 65 66 64 6f 6d 61 69 6e 3f 70 72 65 66 64 6f 6d 3d 47 42 26 61 6d 70 3b 70 72 65 76 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 26 61 6d 70 3b 73 69 67 3d 4b 5f 44 79 36 66 7a 61 66 61 59 4d 6c 6e 76 70 52 44 5a 50 61 55 70 55 6f 44 46 76 38 25 33 44 22 3e 47 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 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 Data Ascii: SolutionsAbout GoogleGoog le.co.uk <p style="font-size:8pt;color:#70

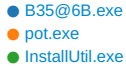
Timestamp	kBytes transferred	Direction	Data
2022-07-24 15:54:34 UTC	96	IN	Data Raw: 7d 3b 66 75 6e 63 74 69 6f 6e 20 6e 28 29 7b 76 61 72 20 61 3d 75 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 70 28 61 29 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 7d 3b 67 6f 6f 67 6c 65 2e 62 78 7c 7c 67 6f 6f 67 6c 65 2e 6c 78 28 29 7d 0a 66 75 6e 63 74 69 6f 6e 20 70 28 61 29 7b 67 6f 6f 67 6c 65 2e 74 69 6d 65 72 73 26 26 67 6f 6f 67 6c 65 2e 74 69 6d 65 72 73 2e 6c 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 Data Ascii: };function n(){var a=u;google.lx=function(){p(a);google.lx=function(){}};google.bx||google.lx()}function p(a){google.timers&&google.timers.load&&google.tick&&google.tick("load","xjsls");var b=document;var c="SCRIPT";"application/xhtml+xml"===b.contentTyp
2022-07-24 15:54:34 UTC	97	IN	Data Raw: 6d 2d 68 70 5c 78 32 32 2c 5c 78 32 32 64 68 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 64 68 71 74 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 64 73 5c 78 32 32 3a 5c 78 32 32 5c 78 32 32 2c 5c 78 32 32 66 66 71 6c 5c 78 32 32 3a 5c 78 32 32 65 6e 5c 78 32 32 2c 5c 78 32 32 66 6c 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 68 6f 73 74 5c 78 32 32 3a 5c 78 32 32 67 6f 6f 67 6c 65 2e 63 6f 6d 5c 78 32 32 2c 5c 78 32 32 69 73 62 68 5c 78 32 32 3a 32 38 2c 5c 78 32 32 6a 73 6f 6e 70 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6d 73 67 73 5c 78 32 32 3a 7b 5c 78 32 32 63 69 62 6c 5c 78 32 32 3a 5c 78 32 32 43 6c 65 61 72 20 53 65 61 72 63 68 5c 78 32 32 2c 5c 78 32 32 64 79 6d 5c 78 32 32 3a 5c 78 32 32 44 69 64 20 79 6f 75 20 6d 65 61 6e 3a 5c 78 32 32 2c 5c 78 32 Data Ascii: m-hp\x22,\x22dh\x22:true,\x22dhqt\x22:true,\x22ds\x22:\x22\x22,\x22ffql\x22:\x22en\x22,\x22fl\x22:true,\x22host\x22:\x22google.com\x22,\x22isbh\x22:28,\x22jsonp\x22:true,\x22msgs\x22:{\x22cibl\x22:\x22Clear Search\x22,\x22dym\x22:\x22Did you mean:\x22,\x2
2022-07-24 15:54:34 UTC	98	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

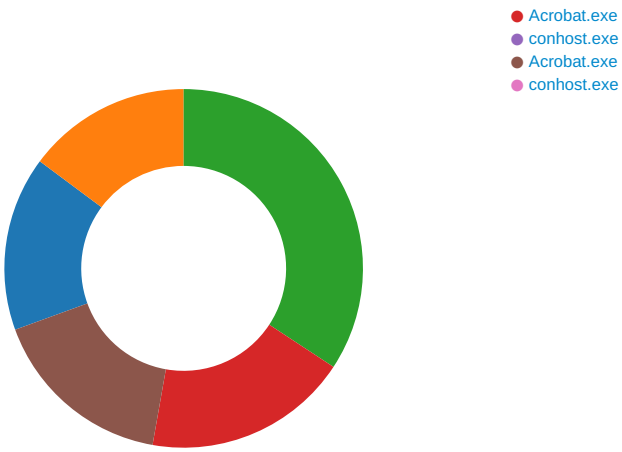
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 24, 2022 17:56:06.231204033 CEST	587	49719	192.185.37.183	192.168.2.4	220-gator4044.hostgator.com ESMTP Exim 4.95 #2 Sun, 24 Jul 2022 10:56:06 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jul 24, 2022 17:56:06.231595993 CEST	49719	587	192.168.2.4	192.185.37.183	EHLO 878411
Jul 24, 2022 17:56:06.400350094 CEST	587	49719	192.185.37.183	192.168.2.4	250-gator4044.hostgator.com Hello 878411 [84.17.52.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jul 24, 2022 17:56:06.400914907 CEST	49719	587	192.168.2.4	192.185.37.183	STARTTLS
Jul 24, 2022 17:56:06.569955111 CEST	587	49719	192.185.37.183	192.168.2.4	220 TLS go ahead
Jul 24, 2022 17:56:15.382637024 CEST	587	49722	192.185.37.183	192.168.2.4	220-gator4044.hostgator.com ESMTP Exim 4.95 #2 Sun, 24 Jul 2022 10:56:15 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jul 24, 2022 17:56:15.382828951 CEST	49722	587	192.168.2.4	192.185.37.183	EHLO 878411
Jul 24, 2022 17:56:15.554317951 CEST	587	49722	192.185.37.183	192.168.2.4	250-gator4044.hostgator.com Hello 878411 [84.17.52.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jul 24, 2022 17:56:15.554552078 CEST	49722	587	192.168.2.4	192.185.37.183	STARTTLS
Jul 24, 2022 17:56:15.724662066 CEST	587	49722	192.185.37.183	192.168.2.4	220 TLS go ahead

Statistics

Behavior





System Behavior

Analysis Process: B35@6B.exe PID: 1724, Parent PID: 1496

General

Target ID:	0
Start time:	17:54:09
Start date:	24/07/2022
Path:	C:\Users\user\Desktop\B35@6B.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\B35@6B.exe"
Imagebase:	0xf10000
File size:	600576 bytes
MD5 hash:	6753A24ED2A75DBD488C0A1783F03D05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.303282970.0000000004AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.303282970.0000000004AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.304264302.0000000004BE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.304264302.0000000004BE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D90CF06	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	6D90CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B35@6B.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC1C78D	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B35@6B.exe	C:\Users\user\AppData\Local\Temp\pot.exe	success or wait	1	C338587	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B35@6B.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",02,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.	success or wait	1	6DC1C907	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	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	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: pot.exe PID: **3224**, Parent PID: **1724**

General

Target ID:	1
Start time:	17:54:31

Start date:	24/07/2022
Path:	C:\Users\user\AppData\Local\Temp\pot.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\pot.exe"
Imagebase:	0xf10000
File size:	600576 bytes
MD5 hash:	6753A24ED2A75DBD488C0A1783F03D05
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: 00000001.00000002.455643526.0000000004462000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.455643526.0000000004462000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.454626461.00000000043B7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.454626461.00000000043B7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.457363000.0000000004569000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.457363000.0000000004569000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D90CF06	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	6D90CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pot.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC1C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pot.exe.log	0	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",02,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.	success or wait	1	6DC1C907	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	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	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: **1448**, Parent PID: **3224**

General

Target ID:	10
Start time:	17:55:35
Start date:	24/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x260000
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: 0000000A.00000000.420464455.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.420464455.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.420090127.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.420090127.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.500496206.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.500496206.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.420800374.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.420800374.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.419618627.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.419618627.0000000000632000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.506967470.00000000025C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.506967470.00000000025C1000.00000004.00000800.00020000.00000000.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	6D90CF06	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	6D90CF06	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	6C75BEFF	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	6C75DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe	0	41064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 5a fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 fd 72 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELZZ0Tr @ `	success or wait	1	6C75DD66	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	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D8ECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C751B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C751B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C751B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C751B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C751B4F	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	6C75646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Acrobat	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C75DE2E	RegSetValueExW

Analysis Process: Acrobat.exe PID: **5284**, Parent PID: **3616**

General

Target ID:	14
Start time:	17:55:57
Start date:	24/07/2022
Path:	C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe"
Imagebase:	0x7c0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
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	6D90CF06	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	6D90CF06	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	6DC1C78D	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	6C751B4F	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	6C751B4F	WriteFile
\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 67 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 otheroptions, /u applies to all assemblies, regardless of where itappears on the command line.Installation is done in a transactioned way: If one of theassemblies fails to install, the installations of all otherassemblies are roll	success or wait	7	6C751B4F	WriteFile
\Device\ConDrv	2017	93	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C751B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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,"WinRT","NotApp",12,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImage	success or wait	1	6DC1C907	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	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	ReadFile

Analysis Process: conhost.exe PID: **4940**, Parent PID: **5284**

General

Target ID:	15
Start time:	17:55:57
Start date:	24/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: Acrobat.exe PID: **5680**, Parent PID: **3616**

General

Target ID:	16
Start time:	17:56:05
Start date:	24/07/2022
Path:	C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Acrobat\Acrobat.exe"
Imagebase:	0xd00000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D90CF06	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	6D90CF06	unknown

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	6C751B4F	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	6C751B4F	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 67 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 otheroptions, /u applies to all assemblies, reg ardless of where itappears on the command line.Installation is done in a transactioned way: If one of theassemblies fails to install, the installations of all otherassemblies are r oll	success or wait	7	6C751B4F	WriteFile
\Device\ConDrv	2017	93	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C751B4F	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	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C751B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C751B4F	ReadFile

Analysis Process: conhost.exe PID: **6128**, Parent PID: **5680**

General

Target ID:	17
Start time:	17:56:05
Start date:	24/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly