ID: 652396
Sample Name: atpRyiZGTE.exe
Cookbook: default.jbs
Time: 09:46:56
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

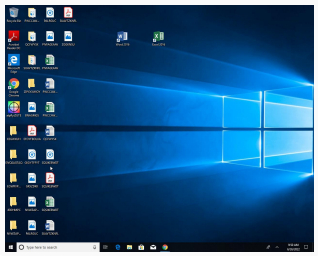
Windows Analysis Report

atpRyiZGTE.exe

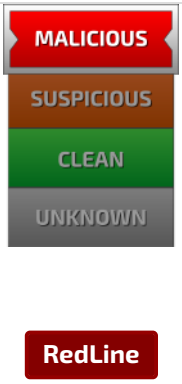
Overview

General Information

Sample Name:	atpRyiZGTE.exe
Analysis ID:	652396
MD5:	0515b4d32d6d65.
SHA1:	3cb9acc775da69..
SHA256:	9027302b65c696..
Tags:	Arechclient2 exe
Infos:	



Detection



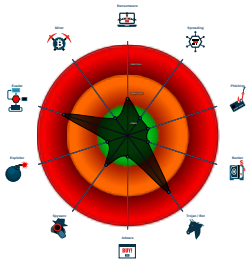
RedLine

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Machine Learning detection for sam…
- Uses ping.exe to check the status o…
- Uses ping.exe to sleep
- Creates an undocumented autostart…
- Machine Learning detection for drop…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- atpRyiZGTE.exe (PID: 3452 cmdline: "C:\Users\user\Desktop\atpRyiZGTE.exe" MD5: 0515B4D32D6D65D19832858957F0847F)
  - cmd.exe (PID: 6720 cmdline: cmd" /c ping 127.0.0.1 -n 38 > nul && REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /f /v "Shell" /t REG_SZ /d "explorer.exe,C:\Users\user\AppData\Roaming\LightKeeperService.exe, MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 6792 cmdline: ping 127.0.0.1 -n 38 MD5: 70C24A306F768936563ABDADB9CA9108)
    - reg.exe (PID: 3796 cmdline: REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /f /v "Shell" /t REG_SZ /d "explorer.exe,C:\Users\user\AppData\Roaming\LightKeeperService.exe," MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - cmd.exe (PID: 6248 cmdline: cmd" /c ping 127.0.0.1 -n 45 > nul && copy "C:\Users\user\Desktop\atpRyiZGTE.exe" "C:\Users\user\AppData\Roaming\LightKeeperService.exe" && ping 127.0.0.1 -n 45 > nul && "C:\Users\user\AppData\Roaming\LightKeeperService.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 6200 cmdline: ping 127.0.0.1 -n 45 MD5: 70C24A306F768936563ABDADB9CA9108)
    - PING.EXE (PID: 6864 cmdline: ping 127.0.0.1 -n 45 MD5: 70C24A306F768936563ABDADB9CA9108)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.450115307.0000000004BE2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.450115307.0000000004BE2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.448862255.00000000048DB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.448862255.00000000048DB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: atpRyiZGTE.exe PID: 3452	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.atpRyiZGTE.exe.49762aa.1.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x451b1:$s1: +773yll • 0x45342:$s1: \xED\xF1\xF1\xF5\xBF\xAA\xAA • 0x475df:$s1: \xE5\xF9\xF9\xFD\xB7\xA2\xA2 • 0x47783:$s1: PLLH\x02\x17\x17 • 0x48628:$s1: \x13\x0F\x0F\x0BATT • 0x82d05:$s1: \xCA\xD6\xD6\xD2\x98\x8D\x8D • 0x451be:$s2: +7730yll • 0x4534f:$s2: \xED\xF1\xF1\xF5\xF6\xBF\xAA\xAA • 0x475ec:$s2: \xE5\xF9\xF9\xFD\xFE\xB7\xA2\xA2 • 0x47790:$s2: PLLHK\x02\x17\x17 • 0x4c19a:$s2: \xF5\xE9\xE9\xED\xEE\xA7\xB2\xB2 • 0x4c5f7:$s2: \x08\x14\x14\x10\x13ZOO • 0x73a84:$s2: osswt=((• 0x73b9b:$s2: \xCB\xD7\xD7\xD3\xD0\x99\x8C\x8C • 0x83582:$s2: \x0E\x12\x12\x16\x15\II
0.2.atpRyiZGTE.exe.49762aa.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.atpRyiZGTE.exe.49762aa.1.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.atpRyiZGTE.exe.49762aa.1.unpack	MALWARE_Win_Arechclient2	Detects Arechclient2 RAT	ditekSHen	• 0x92f6d:$s14: keybd_event • 0x97c10:$v1_1: grabber@ • 0x90796:$v1_2: <BrowserProfile>k__ • 0x9185a:$v1_3: <SystemHardwares>k__ • 0x91919:$v1_5: <ScannedWallets>k__ • 0x919a9:$v1_6: <DicrFiles>k__ • 0x91985:$v1_7: <MessageClientFiles>k__ • 0x91d4f:$v1_8: <ScanBrowsers>k__BackingField • 0x91da1:$v1_8: <ScanWallets>k__BackingField • 0x91dbe:$v1_8: <ScanScreen>k__BackingField • 0x91df8:$v1_8: <ScanVPN>k__BackingField • 0x84e76:$v1_9: displayName[AString-ZaString-z\d]{2String4}\.[String\w-]{String6}\.[\wString-]{2String7}Local Extension Settingshost • 0x84682:$v1_10: \sitemanager.xml MB or SELECT * FROM Cookiesconfig
0.2.atpRyiZGTE.exe.4c7d2e8.5.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x451b1:$s1: +773yll • 0x45342:$s1: \xED\xF1\xF1\xF5\xBF\xAA\xAA • 0x475df:$s1: \xE5\xF9\xF9\xFD\xB7\xA2\xA2 • 0x47783:$s1: PLLH\x02\x17\x17 • 0x48628:$s1: \x13\x0F\x0F\x0BATT • 0x82d05:$s1: \xCA\xD6\xD6\xD2\x98\x8D\x8D • 0x451be:$s2: +7730yll • 0x4534f:$s2: \xED\xF1\xF1\xF5\xF6\xBF\xAA\xAA • 0x475ec:$s2: \xE5\xF9\xF9\xFD\xFE\xB7\xA2\xA2 • 0x47790:$s2: PLLHK\x02\x17\x17 • 0x4c19a:$s2: \xF5\xE9\xE9\xED\xEE\xA7\xB2\xB2 • 0x4c5f7:$s2: \x08\x14\x14\x10\x13ZOO • 0x73a84:$s2: osswt=((• 0x73b9b:$s2: \xCB\xD7\xD7\xD3\xD0\x99\x8C\x8C • 0x83582:$s2: \x0E\x12\x12\x16\x15\II
Click to see the 35 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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses ping.exe to check the status of other devices and networks

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Uses ping.exe to sleep

Stealing of Sensitive Information

Yara detected RedLine Stealer

Remote Access Functionality

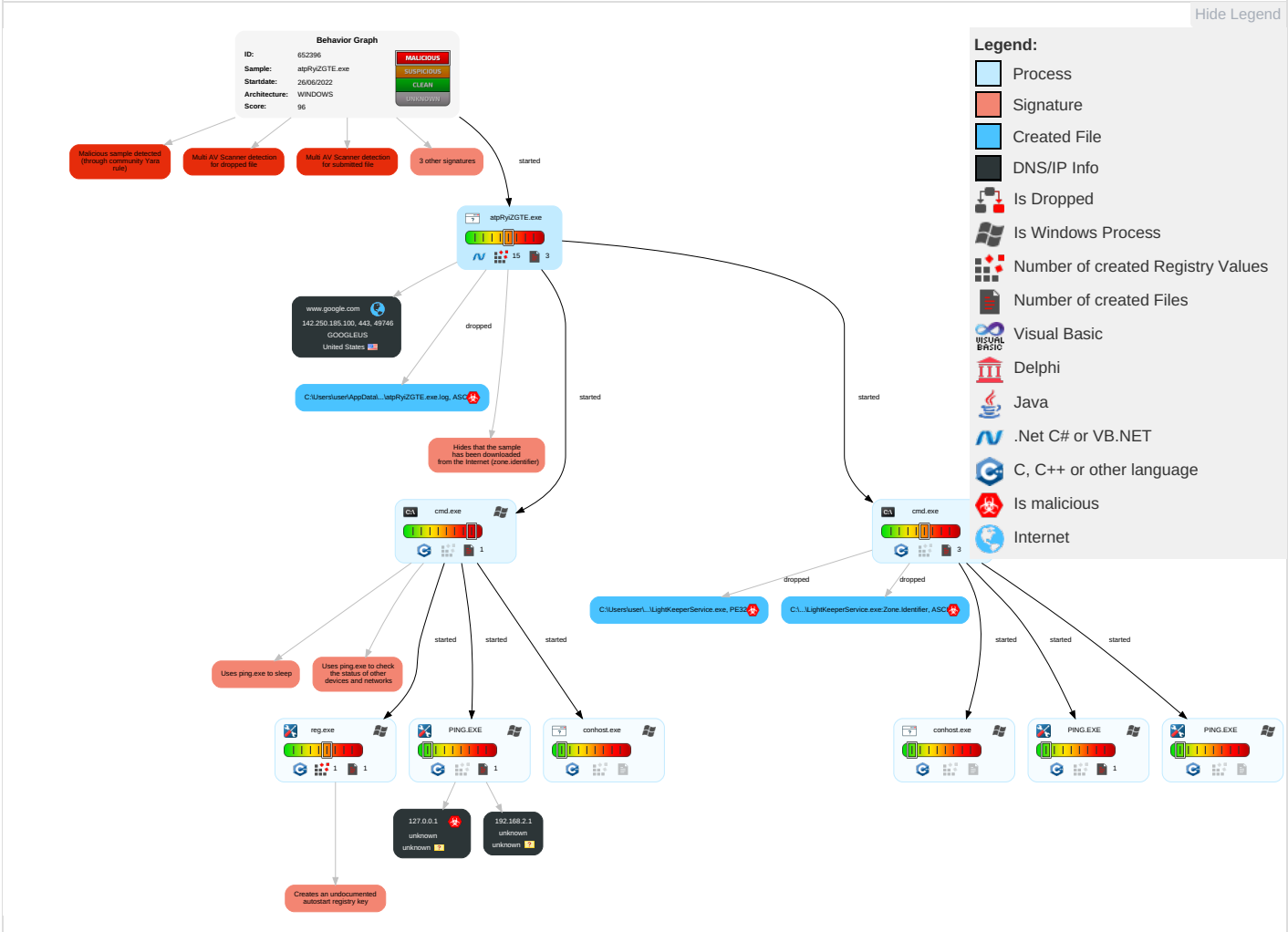
Yara detected RedLine Stealer

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	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Modify Registry	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 System Network Configuration 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 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
atpRyiZGTE.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
atpRyiZGTE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LightKeeperService.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LightKeeperService.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlG	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sakkal.comr	0%	URL Reputation	safe	
http://https://www.google.comT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://ns.adp/1.0/	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://https://www.google.com%BorderColorFocused	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deEv	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://ns.microsoto/1.2	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.185.100	true	false		high

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

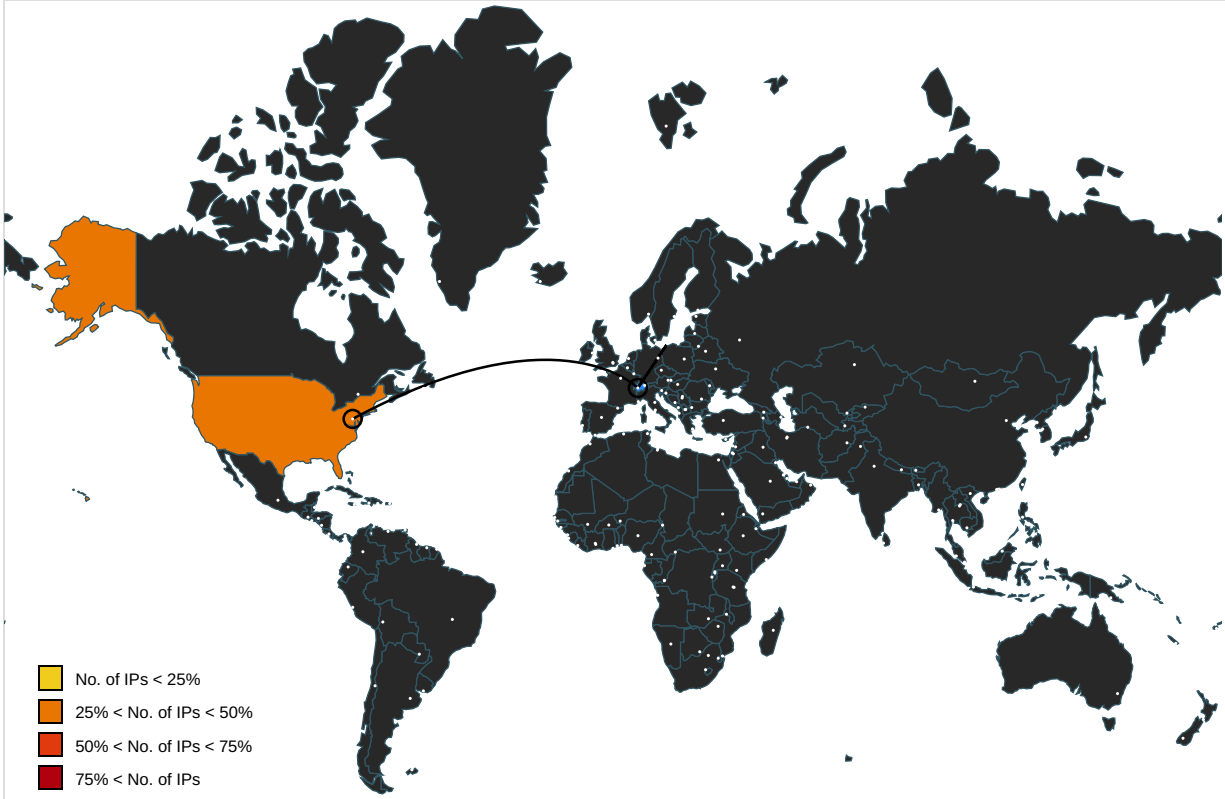
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.295467627.0000000006850000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.295597676.0000000006845000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.295438765.0000000006845000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.htmlG	atpRyiZGTE.exe, 00000000.00000003.298764281.0000000006846000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	atpRyiZGTE.exe, 00000000.00000002.452188664.0000000006800000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com	atpRyiZGTE.exe, atpRyiZGTE.exe, 00000000.00000002.445054854.0000000002EA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/i	atpRyiZGTE.exe, 00000000.00000003.295735340.0000000006846000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.295655832.0000000006846000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.295687027.0000000006846000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.312675141.0000000006814000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.comr	atpRyiZGTE.exe, 00000000.00000003.299475642.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300737819.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300455988.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300935758.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300039387.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.301161307.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300667068.0000000006814000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.comT	atpRyiZGTE.exe, 00000000.00000002.445054854.0000000002EA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	atpRyiZGTE.exe, 00000000.00000003.314251572.0000000006846000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adp/1.0/	atpRyiZGTE.exe, 00000000.00000003.348966637.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.337172932.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.334588359.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.335558240.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.440305727.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.341919239.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.348472153.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.341573864.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.345775535.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.340929865.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.438770547.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.343342627.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.342714698.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.344471615.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.353915669.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.351717491.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.347097585.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.336546347.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.354548458.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.352972101.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.335252277.0000000006887000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.como	atpRyiZGTE.exe, 00000000.00000002.452188664.0000000006800000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com%BorderColorFocused	atpRyiZGTE.exe, LightKeeperService.exe.19.dr	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/DPlease	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deEv	atpRyiZGTE.exe, 00000000.00000003.315674707.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.315753789.0000000006814000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	atpRyiZGTE.exe, 00000000.00000003.299802336.0000000006859000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.299334032.0000000006859000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.298764281.0000000006846000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.300440687.0000000006859000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html8	atpRyiZGTE.exe, 00000000.00000003.312783150.0000000006855000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.312649918.0000000006855000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.microsoto/1.2	atpRyiZGTE.exe, 00000000.00000003.348966637.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.337172932.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.334588359.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.335558240.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.440305727.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.341919239.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.348472153.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.341573864.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.345775535.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.340929865.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.438770547.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.343342627.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.342714698.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.344471615.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.353915669.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.351717491.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.347097585.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.336546347.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.354548458.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.352972101.0000000006887000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.335252277.0000000006887000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	atpRyiZGTE.exe, 00000000.00000003.309958195.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.309784943.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.315674707.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.310013124.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.315753789.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.310158459.0000000006814000.00000004.00000800.00020000.00000000.sdmp, atpRyiZGTE.exe, 00000000.00000003.309902011.0000000006814000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	atpRyiZGTE.exe, 00000000.00000002.445054854.0000000002EA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	atpRyiZGTE.exe, 00000000.00000002.454472741.000000000A742000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652396
Start date and time: 26/06/202209:46:56	2022-06-26 09:46:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	atpRyiZGTE.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:	31
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:	mal96.troj.evad.winEXE@15/5@1/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 84.5% • Quality standard deviation: 1.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: atpRyiZGTE.exe

Simulations

Behavior and APIs

Time	Type	Description
09:49:02	API Interceptor	184x Sleep call for process: atpRyiZGTE.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\atpRyiZGTE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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=b77a

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

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1598976
Entropy (8bit):	6.542587858621466
Encrypted:	false
SSDEEP:	24576:hfFQnGpTDv52xFCsS4M61DPcnc4VsBKm6cCEtfG4RTRTHTM:hfFQnkV2TCo1DPcnc4VsKm6c9NxDXM
MD5:	0515B4D32D6D65D19832858957F0847F
SHA1:	3CB9ACC775DA6908C56890F0827398B817467E0E
SHA-256:	9027302B65C696C2E079F70C18F55ABC1FD10C497B4CAD63BDBFBD8AC110B916

<table>
<tr><td>SHA-512:</td><td>9E145260E75D7359772FAB436372CCFA249054F4CDA7E9FAFD2A67B7CC7B8166CBD1F38C73CD89737E3EA6F6D670684400250ADB26CD777080D4A203E4FD40 E</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Antivirus:</td><td>• Antivirus: Joe Sandbox ML, Detection: 100%
• Antivirus: ReversingLabs, Detection: 42%</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......2................................ ....@.. ....`...................................S.................................................................................. ............... ..H...........text........ ...................... ..`.rsrc...............................@..@.reloc........ ....d.............@..B......................H.......0...x.......y... {...j.?f...k.........i....12..w..1=...L.Q..(.~>.lE+.R.|../.4z.F....a.....).#.}..LB.Q~..!...@s....p..E. ....^....@N...n..i.O.6.q.L.Z...C]..e......!.xf0.#.w.;..EN9Mr0..'M.\.".|.B..`l..{H.~&...<S ......p.*..&......J6.S.*x?.0E. ..Y.Y....l..!.i+.....G._.oT.........9.J.G......K.^Z... %..R.O.......z^..r. @.6.%.........POW.fj...u.mLC...Ts...8...=....\."U.dF.5..F.o...(@C...z.....S.a...}v.0.,9.</td></tr>
</table>

C:\Users\user\AppData\Roaming\LightKeeperService.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

\Device\Null

Process:	C:\Windows\SysWOW64\PING.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2440
Entropy (8bit):	4.725663483598328
Encrypted:	false
SSDEEP:	12:PKMRJpTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTeTd:/elAokItULVDv
MD5:	CE2B4D3E2C6F89A5578B7B2574D9316A
SHA1:	0B97F330E453CBCD78F3FE1C41675DF80D8BC81A
SHA-256:	23F40B2D6379451ACD948C88723D09339D6386D08C068D70A9DC67EB56D3FB95
SHA-512:	1AE47563977707328E8381BF37E1628B57886A9B570314D36225A628130B7F83058D5C4889C7BDF48F0719181B302985F3913264089854029098385B3D5C7E8F
Malicious:	false
Preview:	..Pinging 127.0.0.1 with 32 bytes of data:..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 ..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127 .0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: byt

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.542587858621466
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:	atpRyiZGTE.exe
File size:	1598976
MD5:	0515b4d32d6d65d19832858957f0847f
SHA1:	3cb9acc775da6908c56890f0827398b817467e0e

SHA256:	9027302b65c696c2e079f70c18f55abc1fd10c497b4cad63bdbfbd8ac110b916
SHA512:	9e145260e75d7359772fab436372ccfa249054f4cda7e9fafd2a67b7cc7b8166cbd1f38c73cd89737e3ea6f6d670684400250adb26cd777080d4a203e4fd409e
SSDEEP:	24576:hfFQnGpTDv52xFCsS4M61DPcnc4VsBKm6cCEtfG4RTRTHTM:hfFQnkV2TCo1DPcnc4VsKm6c9NxDXM
TLSH:	4575BEA22B857E03C03CA63E8234F54093F6FDCAA349C79D7DD5B5C666A23413BA2754
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......2................................. ....@.. ....`................................

File Icon

Icon Hash:	8e2b6d6c6c69abcc

Static PE Info

General

Entrypoint:	0x56a3fe
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:	0x32E593FC [Wed Jan 22 04:13:48 1997 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16a3a8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16c000	0x1db00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x168404	0x168600	False	0.6130488802896289	data	6.475046719062856	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x16c000	0x1db00	0x1dc00	False	0.7296316964285714	data	6.869642401970742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x18a000	0xc	0x200	False	0.041015625	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x16c628	0x1c57	PNG image data, 128 x 128, 8-bit colormap, non-interlaced		
RT_ICON	0x16e280	0x1628	data		
RT_ICON	0x16f8a8	0xea8	data		
RT_ICON	0x170750	0x8a8	data		
RT_ICON	0x170ff8	0x6c8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1716c0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x171c28	0x8683	PNG image data, 256 x 256, 8-bit/color RGB, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17a2ac	0x3d5c	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x17e008	0x4228	data		
RT_ICON	0x182230	0x25a8	data		
RT_ICON	0x1847d8	0x10a8	data		
RT_ICON	0x185880	0x988	data		
RT_ICON	0x186208	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x186670	0x2e8	data		
RT_ICON	0x186958	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x186a80	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x186ba8	0x2e8	data		
RT_ICON	0x186e90	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294967295, next used block 4286019583		
RT_ICON	0x187178	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1872a0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x187b48	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1880b0	0xca8	dBase IV DBT of @.DBF, block length 3072, next free block index 40, next free block 4143380214, next used block 4143380214		
RT_ICON	0x188d58	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1890c0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x189528	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x189650	0xbc	data		
RT_GROUP_ICON	0x18970c	0x22	data		
RT_GROUP_ICON	0x189730	0x22	data		
RT_GROUP_ICON	0x189754	0x5a	data		
RT_GROUP_ICON	0x1897b0	0x22	data		
RT_VERSION	0x1897d4	0x32c	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

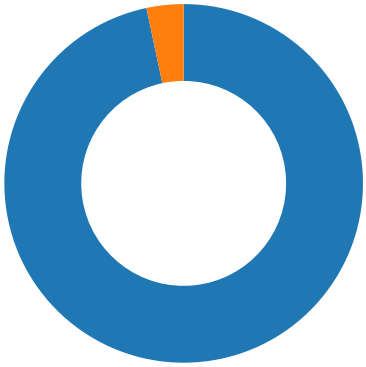
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 30

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:48:20.692310095 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:20.692351103 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:20.692446947 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:20.764801979 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:20.764837980 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:20.817599058 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:20.817701101 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:20.821000099 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:20.821022034 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:20.821403027 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.009613037 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.224230051 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.264503002 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.283855915 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.283974886 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.284046888 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.284091949 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.284181118 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.284250975 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.284262896 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.284284115 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.284348965 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.284708977 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.285936117 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.286016941 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.286029100 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.286052942 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.286099911 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.287271976 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.288619995 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.288696051 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.288716078 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.288743973 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.288794994 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.300412893 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.300869942 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.300940037 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.300992966 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.301035881 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.301119089 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.302185059 CEST	443	49746	142.250.185.100	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:48:21.303555012 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.303637981 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.303685904 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.303713083 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.303775072 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.304765940 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.306030989 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.306128025 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.306149006 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.307329893 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.307384968 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.307414055 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.307430983 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.307475090 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.308541059 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.309636116 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.309689999 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.309756994 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.309781075 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.309827089 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.310713053 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.311939001 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.312007904 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.312042952 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.312062025 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.312105894 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.312947989 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.314049959 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.314114094 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.314165115 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.314188957 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.314249039 CEST	443	49746	142.250.185.100	192.168.2.4
Jun 26, 2022 09:48:21.314279079 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.314316034 CEST	49746	443	192.168.2.4	142.250.185.100
Jun 26, 2022 09:48:21.326067924 CEST	49746	443	192.168.2.4	142.250.185.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:48:20.636743069 CEST	60506	53	192.168.2.4	8.8.8.8
Jun 26, 2022 09:48:20.662038088 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
Jun 26, 2022 09:48:20.636743069 CEST	192.168.2.4	8.8.8.8	0xc6da	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:48:20.662038088 CEST	8.8.8.8	192.168.2.4	0xc6da	No error (0)	www.google.com		142.250.185.100	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	49746	142.250.185.100	443	C:\Users\user\Desktop\atpRyiZGTE.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2022-06-26 07:48:21 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 26 Jun 2022 07:48:21 GMT Expires: -1 Cache-Control: private, max-age=0 Content-Type: text/html; charset=ISO-8859-1 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: AEC=AakniGPWn24ct2sLJwkW8tir5SqQA7-iC8qNpsQ5GdxWywSGbxpJrJNDqg; expires=Fri, 23-Dec-2022 07:48:21 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: __Secure-ENID=5.SE=X8yGHJuvgnzc55XoNk8_Mza3nrf_VAoZchfNhOXPFcbqcmgj1aewySqRYSn GFa0ilk8eMV4EXP5nkNk3gV51yHqvAH8wD5DgmNpHFFfLVYb-7qDKKviaOiPYs4cwftZ1orAh6t7MMg7MqKj8TIZ_A CF7qCnLvdxGp80kbDkVtx8; expires=Thu, 27-Jul-2023 00:06:39 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+312; expires=Tue, 25-Jun-2024 07:48:21 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-26 07:48:21 UTC	1	IN	Data Raw: 35 36 37 38 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 22 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 57 65 62 50 61 67 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 Data Ascii: 5678<!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
2022-06-26 07:48:21 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 6d 63 55 74 69 34 46 30 6e 31 4c 53 35 44 72 76 4a 70 76 4d 42 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 52 51 2d 34 59 73 53 66 44 72 4b 41 69 2d 67 50 31 66 43 73 6f 41 59 27 2c 6b 45 58 50 49 3a 27 30 2c 31 33 30 32 35 33 36 2c 35 34 32 34 34 2c 32 36 32 39 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 Data Ascii: ent="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="mcUti4F0n1LS5DrvJpvMBQ">(function(){window.google={kEI:'RQ-4YsSfDrKAi-gP1fCsoAY',kEXPI:'0,1302536,54244,2629,6058,207,4804,2316,383,246
2022-06-26 07:48:21 UTC	2	IN	Data Raw: 30 2c 32 31 33 30 2c 34 32 37 2c 38 34 39 2c 37 31 39 2c 33 36 35 38 2c 39 33 32 35 31 39 27 2c 6b 42 4c 3a 27 30 4d 75 38 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 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 Data Ascii: 0,2130,427,849,719,3658,932519',kBL:'0Mu8'};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=nul
2022-06-26 07:48:21 UTC	3	IN	Data Raw: 5d 2c 62 2c 63 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 6c 6f 61 64 41 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 67 6f 6f 67 6c 65 2e 6c 71 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 3b 67 6f 6f 67 6c 65 2e 62 78 3d 21 31 3b 67 6f 6f 67 6c 65 2e 6c 78 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 Data Ascii:],b,c])};google.loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.lx=function(){};}).call(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submitfa
2022-06-26 07:48:21 UTC	5	IN	Data Raw: 6c 75 74 65 3b 74 6f 70 3a 33 30 70 78 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 67 62 74 63 62 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 23 67 62 7a 20 2e 67 62 74 63 62 7b 72 69 67 68 74 3a 30 7d 23 67 62 67 20 2e 67 62 74 63 62 7b 6c 65 66 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 Data Ascii: lute;top:30px;width:100%}.gbtcb{position:absolute;visibility:hidden}#gbz .gbtcb{right:0}#gbg .gbtcb{left:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{position:absolute;z-index:999;top:-999px;visibility

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	6	IN	Data Raw: 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 67 62 6d 63 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 3b 7a 6f 6f 6d 3a 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f Data Ascii: st-style:none;margin:0;padding:0}.gbmc{background:#fff;padding:10px 0;position:relative;z-index:2;zoom:1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-align:top}.gbt{*display:inline}.gbto{box-shado
2022-06-26 07:48:21 UTC	7	IN	Data Raw: 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 63 34 63 34 63 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 5f 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 30 20 2d 31 30 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 Data Ascii: kground-color:#4c4c4c;background-image:none;_background-image:none;background-position:0 -102px;background-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gbtb2{border-top-color:#dd4b39!important}#gbi4
2022-06-26 07:48:21 UTC	8	IN	Data Raw: 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 2c 2e 67 62 6e 64 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 64 64 38 65 32 37 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 66 20 2e 67 62 6d 74 2c 2e 67 62 66 20 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 Data Ascii: gbmt:visited,.gbnd .gbmt,.gbnd .gbmt:visited{color:#dd8e27 !important}.gbf .gbmt,.gbf .gbmt:visited{color:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:vis
2022-06-26 07:48:21 UTC	10	IN	Data Raw: 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 29 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 31 7d 23 67 62 64 34 20 2e 67 62 6d 68 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 62 6d 74 63 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 Data Ascii: box-shadow:0 2px 4px rgba(0,0,0,.12);position:relative;z-index:1}#gbd4 .gbmh{margin:0}.gbmtc{padding:0;margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc
2022-06-26 07:48:21 UTC	11	IN	Data Raw: 31 30 70 78 20 32 30 70 78 20 30 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 62 6d 70 61 6c 61 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 67 62 6d 70 61 6c 62 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 7d 23 67 62 6d 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b Data Ascii: 10px 20px 0;white-space:nowrap}.gbmpala{padding-left:0;text-align:left}.gbmpalb{padding-right:0;text-align:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gbiba{margin:8px 20px 10px}.gbmpiaw{display:inline-block
2022-06-26 07:48:21 UTC	12	IN	Data Raw: 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 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 Data Ascii: 0,0,0,.1)}.gbqfb-no-focus:focus{border:1px solid #3079ed;-moz-box-shadow:none;-webkit-box-shadow:none;box-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px
2022-06-26 07:48:21 UTC	14	IN	Data Raw: 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 Data Ascii: ;background-image:-moz-linear-gradient(top,#4d90fe,#357ae8);background-image:-ms-linear-gradient(top,#4d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:active{background-c
2022-06-26 07:48:21 UTC	15	IN	Data Raw: 31 66 31 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 38 66 38 66 38 2c 23 66 31 66 31 66 31 29 3b 66 69 6c 74 65 72 3a 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 67 72 61 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 Data Ascii: 1f1);background-image:linear-gradient(top,#f8f8f8,#f1f1f1);filter:progid:DXImageTransform.Microsoft.gradient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#f

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	16	IN	Data Raw: 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 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 Data Ascii: 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1);color:#222 !important}.gbqfba:active,.gbqfbb:active{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}#gbmpas{
2022-06-26 07:48:21 UTC	17	IN	Data Raw: 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 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 Data Ascii:);top:0}.gbsb .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right top,color-stop(0,rgba(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to
2022-06-26 07:48:21 UTC	19	IN	Data Raw: 65 7d 2e 66 6c 20 61 7b 63 6f 6c 6f 72 3a 23 31 35 35 38 64 36 7d 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 34 62 31 31 61 38 7d 2e 73 62 6c 63 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 70 78 7d 2e 73 62 6c 63 20 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 32 70 78 20 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 Data Ascii: e}.fl a{color:#1558d6}a:visited{color:#4b11a8}.sblc{padding-top:5px}.sblc a{display:block;margin:2px 0;margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block}#
2022-06-26 07:48:21 UTC	20	IN	Data Raw: 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 2f 41 22 29 3b 31 32 32 38 38 3c 3d 62 2e 6c 65 6e 67 74 68 26 28 62 3d 62 2e 73 75 Data Ascii: ref&&(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/A");12288<=b.length&&(b=b.su
2022-06-26 07:48:21 UTC	21	IN	Data Raw: 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 63 74 69 6f 6e 28 29 7b 7d 2c 6b 61 3d 66 75 6e 63 74 69 6f 6e 28 Data Ascii: y(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=function(){},ka=function(
2022-06-26 07:48:21 UTC	22	IN	Data Raw: 36 38 66 31 0d 0a 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 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 Data Ascii: 68f1&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",la);p("bnc",w);p("qGC",ta);p("qm",B);p("qd",x);p("lb",D);p("mcf",
2022-06-26 07:48:21 UTC	24	IN	Data Raw: 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 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 Data Ascii: ,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).getTime(),"&jexpid=",d("28834"),"&srcpg=",d("prop=1"),"&jsr=",Math.
2022-06-26 07:48:21 UTC	25	IN	Data Raw: 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 7d 2c 4f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 0a 5b 4c 61 3f 22 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 22 2c 22 2f 6f 67 2f 5f 2f 6a 73 2f 64 3d 31 2f 6b 3d 22 2c 22 6f 67 2e 6f 67 32 2e 65 6e 5f 55 53 2e 51 51 49 52 4e 4f 6c 4c 54 37 38 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 49 67 38 4f 7a 4d 4e 63 67 79 68 74 44 54 50 49 6d 4b 7a 31 37 78 4c 4e 35 75 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 Data Ascii: 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.QQIRNOILT78.O","/rt=j/m=",a,"/rs=","AA2YrTvIg8OzMNcgyhtDTPImKz17xLN5uA"];Ka&&a.push("?host=www.gstatic.com&bust=og.og2.en_U

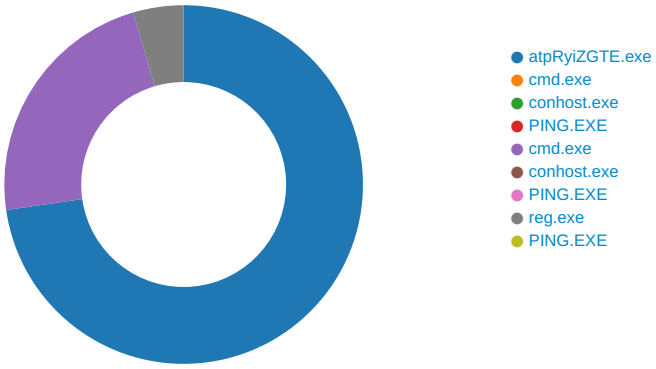
Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	26	IN	Data Raw: 76 61 72 20 6b 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 69 66 28 4f 3d 3d 64 29 4f 3d 76 6f 69 64 20 30 2c 0a 4b 28 6b 2c 22 67 62 74 6f 22 29 3b 65 6c 73 65 7b 69 66 28 4f 29 7b 76 61 72 20 6d 3d 64 6f 63 75 6d 65 6e 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 74 42 79 49 64 28 6e 29 3b 6c 26 26 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 4b 28 6c 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 22 67 62 74 6f 22 29 7d 7d 7d 24 61 28 66 29 26 26 61 62 28 66 29 3b 4f 3d 64 3b Data Ascii: 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.getElementById(n);l&&l.parentNo de&&K(l.parentNode,"gbto")}}}$a(f)&&ab(f);O=d;
2022-06-26 07:48:21 UTC	27	IN	Data Raw: 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 79 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 63 22 3b 7a 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 20 67 62 6d 68 22 3b 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 7a 29 3b 6b 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 79 2c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 6c 5d 29 7d 67 2e 61 64 64 48 6f 76 65 72 26 26 67 2e 61 64 64 48 6f 76 65 72 28 61 29 7d 65 6c 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 7d 63 61 74 63 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 Data Ascii: ("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)}}catch(Eb){r(Eb,"sb","al")}},fb=func tion(a,b){for(var c=b.length,d=0;d<c
2022-06-26 07:48:21 UTC	29	IN	Data Raw: 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 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 Data Ascii: nerHTML=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"))return c},P=function() {qb&&window.clearTimeout(qb)},ub=function(a
2022-06-26 07:48:21 UTC	30	IN	Data Raw: 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 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 2c 61 Data Ascii: 55d6a6b787dcc2a4062e6e9824.js",index:"",lang:"en"};v.gc=Bb;var Cb=function(a){window.googleapis&&w indow.iframes?a&&a():(a&&ta(a),D("gc"))};p("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
2022-06-26 07:48:21 UTC	31	IN	Data Raw: 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 35 35 39 37 32 34 33 31 2e 30 22 29 2c 55 3d 22 26 6f 67 67 76 3d 22 2b 64 28 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 32 30 36 30 37 2e 31 5f 70 30 22 29 2c 49 3d 64 28 22 63 6f 6d 22 29 2c 56 3d 64 28 22 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 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 Data Ascii: .bv.f,q=d("1");n=d(n);c=Math.round(1/c);var E=d("455972431.0"),U="&oggv="+d("es_plusone_gc_2022060 7.1_p0"),l=d("com"),V=d("en"),W=d("GBR");var y=0;h.a("")&&(y|=1);h.a("")&&(y|=2);h.a("")&&(y|=4);a=["//www.goo gle.com/gen_204?atyp=i&zx=",f,"&oge=",a,"&ogex
2022-06-26 07:48:21 UTC	32	IN	Data Raw: 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 7 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 Data Ascii: b);p("sps",Wb);p("spd",$b);p("paa",Tb);p("prm",Ub);mb("gbd4",Ub);if(h.a(""))){var ac={d:h.a(""),e:"",sanw:h.a (""),p:"https://lh3.googleusercontent.com/ogw/default-user=s96",cp:"1",xp:h.a("1"),mg:"%1$s (delegated)",md:"%1$s (default)",mh:"220",s:"1",pp:Zb,
2022-06-26 07:48:21 UTC	34	IN	Data Raw: 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 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 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 3d 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 Data Ascii: c=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,b,c,d){try{jc(document)||(d||(b="og-up-"+ b),kc()?e.localStorage.setI
2022-06-26 07:48:21 UTC	35	IN	Data Raw: 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 30 5d 26 26 21 6c 5b 31 5d 2e 61 75 74 6f 3b 29 3b 6c 26 26 28 73 61 28 32 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 75 72 6c 26 26 72 61 28 6c 5b 31 5d 2e 75 72 6c 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 6c 5b 31 5d 2e 6c 69 62 73 29 29 3b 6d 3c 6b 2e 6c 65 6e 67 74 68 26 26 73 65 74 54 69 6d 65 6f 75 74 28 61 2c 30 29 7d 66 75 6e 63 74 69 6f 6e 20 62 28 29 7b 30 3c 66 2d 2d 3f 73 65 74 54 69 6d 65 6f 75 74 28 62 2c 30 29 3a 61 28 29 7d 76 61 72 Data Ascii: {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<k.length&&setTimeout(a,0)}function b(){0<f--?setTim eout(b,0):a()}var

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	36	IN	Data Raw: 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 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 Data Ascii: sure 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.getElementById("gb_"+g),c=document.getElementB yId("gb_"+a);b&&f.l(b,h.test(b.cla
2022-06-26 07:48:21 UTC	38	IN	Data Raw: 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 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 Data Ascii: ndefined"==typeof k.execScript||k.execScript("var "+h[0]);for(var l;h.length&&(l=h.shift());)h.length||void 0===g? k=k[l]&&k[l]!==Object.prototype[l]?k[l]:k[l]={}:k[l]=g;}catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init "});}})();(funct
2022-06-26 07:48:21 UTC	39	IN	Data Raw: 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 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 Data Ascii: gb_8 href="https://maps.google.co.uk/maps?hl=en&tab=wl"> Maps <li class=gbt><a class=gbzt id=gb_78 href="https://play.google.com/?hl=en&tab=w8"><span cl ass=gbtb2>Play</
2022-06-26 07:48:21 UTC	40	IN	Data Raw: 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 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 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 Data Ascii: "gbmc gbsb gbsbis"><ol id=gbmm class="gbmcc gbsbic"><li class=gbmtc>Calendar <li class=gbmtc><a class=gbmt id=gb_51 href="http s://translate.google.co.uk/?hl=en&tab=wT">Trans
2022-06-26 07:48:21 UTC	41	IN	Data Raw: 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 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 Data Ascii: 1,{t:66});; });</script> <h2 class=gbxx>Account Options</h2><ol class=gbtc><li class=gbt><a target =_top href="https://accounts.google.c
2022-06-26 07:48:21 UTC	43	IN	Data Raw: 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 6d 63 55 74 69 34 46 30 6e 31 4c 53 35 44 72 76 4a 70 76 4d 42 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 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 Data Ascii: bx4> <script nonce='mcUti4F0n1LS5DrvJpvMBQ'>window.gbar&&gbar.elp&&gbar.elp()</script> < /div> <br clear="all" id="lgpd"> <img alt="Google" height="92" src="/images/branding/googl elogo/1x/googlelogo_white_background_color_272x
2022-06-26 07:48:21 UTC	44	IN	Data Raw: 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 72 67 64 56 54 38 65 36 56 58 30 66 63 76 6c 4d 46 4a 71 44 6a 4c 5f 71 2d 42 49 45 4d 72 4f 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 Data Ascii: alue){this.checked = 1;if (this.form.iflsig)this.form.iflsig.disabled = false;}else top.location='/doodles/';};})();</ script><input value="AJiK0e8AAAAAYrgdVT8e6VX0fcvlMFJqDjL_q-BIEMrO" name="iflsig" type="hidden"> </td><td class="fl sblc" al
2022-06-26 07:48:21 UTC	45	IN	Data Raw: 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 66 55 46 49 4c 5f 43 76 43 6b 75 45 76 57 44 57 72 30 55 57 39 47 7a 34 35 74 49 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 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 Data Ascii: ttps://www.google.com/setprefdomain?prefdom=GB&prev=https://www.google.co.uk/&sig=K_fUFIL_ CvCkuEvWDWr0UW9Gz45tI%3D">Google.co.uk <p style="font-size:8pt;color:#70757a">© 2022 - Privacy -

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:48:21 UTC	46	IN	Data Raw: 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 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 Data Ascii: ogle.timers.load&&google.tick&&google.tick("load","xjsls");var b=document;var c="SCRIPT";"applicat ion/xhtml+xml"===b.contentType&&(c=c.toLowerCase());c=b.createElement(c);if(void 0===g){b=null;var k=d.trusted Types;if(k&&k.createPolicy){try{b=k.createPolic
2022-06-26 07:48:21 UTC	48	IN	Data Raw: 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 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 Data Ascii: om\x22,\x22isbh\x22:28,\x22jsonp\x22:true,\x22msgs\x22:{\x22cibl\x22:\x22Clear Search\x22,\x22dym\ x22:\x22Did you mean:\x22,\x22lcky\x22:\x22I\u0026#39;m Feeling Lucky\x22,\x22lml\x22:\x22Learn more\x22,\x22 oskt\x22:\x22Input tools\x22,\x22psrc\x22:\x22T
2022-06-26 07:48:21 UTC	49	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: atpRyiZGTE.exe PID: **3452**, Parent PID: **404**

General

Target ID:	0
Start time:	09:48:15
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\atpRyiZGTE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\atpRyiZGTE.exe"
Imagebase:	0x10a0000
File size:	1598976 bytes
MD5 hash:	0515B4D32D6D65D19832858957F0847F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.450115307.0000000004BE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.450115307.0000000004BE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.448862255.00000000048DB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.448862255.00000000048DB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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: cmd.exe PID: **6720**, Parent PID: **3452**

General

Target ID:	13
Start time:	09:49:00
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c ping 127.0.0.1 -n 38 > nul && REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /f /v "Shell" /t REG_SZ /d "explorer.exe,C:\Users\user\AppData\Roaming\LightKeeperService.exe,
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6740**, Parent PID: **6720**

General

Target ID:	14
Start time:	09:49:01
Start date:	26/06/2022
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: PING.EXE PID: **6792**, Parent PID: **6720**

General

Target ID:	15
Start time:	09:49:02
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 38
Imagebase:	0xa50000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6248**, Parent PID: **3452**

General

Target ID:	19
Start time:	09:49:32
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c ping 127.0.0.1 -n 45 > nul && copy "C:\Users\user\Desktop\atpRyiZGTE.exe" "C:\Users\user\AppData\Roaming\LightKeeperService.exe" && ping 127.0.0.1 -n 45 > nul && "C:\Users\user\AppData\Roaming\LightKeeperService.exe
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LightKeeperService.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	1194E97	CopyFileExW
C:\Users\user\AppData\Roaming\LightKeeperService.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	1194E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LightKeeperService.exe	0	262144	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 fd fd fd 32 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 16 00 00 fd 01 00 00 00 00 00 fd fd 16 00 00 20 00 00 00 fd 16 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 18 00 00 02 00 00 00 00 00 00 02 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.$PEL2 @ `	success or wait	7	1194E97	CopyFileExW
C:\Users\user\AppData\Roaming\LightKeeperService.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	1194E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\atpRyiZGTE.exe	unknown	512	success or wait	1	1195742	ReadFile

Analysis Process: conhost.exe PID: **4148**, Parent PID: **6248**

General

Target ID:	20
Start time:	09:49:33
Start date:	26/06/2022
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: PING.EXE PID: **6200**, Parent PID: **6248**

General

Target ID:	21
Start time:	09:49:34
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 45

Imagebase:	0xa50000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: **3796**, Parent PID: **6720**

General

Target ID:	23
Start time:	09:49:42
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /f /v "Shell" /t REG_SZ /d "explorer.exe,C:\Users\user\AppData\Roaming\LightKeeperService.exe,"
Imagebase:	0x7ff7338d0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	explorer.exe,C:\Users\user\AppData\Roaming\LightKeeperService.exe,	success or wait	1	F35A1D	RegSetValueExW

Analysis Process: PING.EXE PID: **6864**, Parent PID: **6248**

General

Target ID:	30
Start time:	09:50:22
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	
Commandline:	ping 127.0.0.1 -n 45
Imagebase:	
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly