ID: 505624
Sample Name: 987421.exe
Cookbook: default.jbs
Time: 16:28:28
Date: 19/10/2021
Version: 33.0.0 White Diamond

Table of Contents

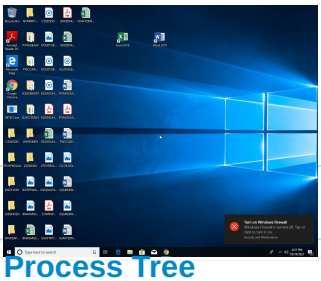
Windows Analysis Report 987421.exe

Overview

General Information

Sample Name:	987421.exe
Analysis ID:	505624
MD5:	75e71ba1842dc3..
SHA1:	3dac2a6f86bf211..
SHA256:	72946d33bc1e39..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

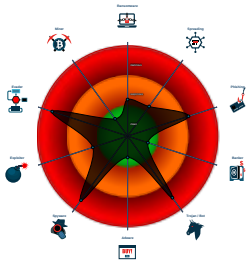
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected HawkEye Rat
- Tries to steal Mail credentials (via fil…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- 987421.exe (PID: 4344 cmdline: 'C:\Users\user\Desktop\987421.exe' MD5: 75E71BA1842DC3F63198386ADB92716F)
  - InstallUtil.exe (PID: 6920 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - vbc.exe (PID: 7160 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6412 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.557838555.000000000762000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	0x7b6c8:$key: HawkEyeKeylogger 0x7d8ba:$salt: 099u787978786 0x7bcd5:$string1: HawkEye_Keylogger 0x7cb28:$string1: HawkEye_Keylogger 0x7d81a:$string1: HawkEye_Keylogger 0x7c0be:$string2: holdermail.txt 0x7c0de:$string2: holdermail.txt 0x7c000:$string3: wallet.dat 0x7c018:$string3: wallet.dat 0x7c02e:$string3: wallet.dat 0x7d3fc:$string4: Keylog Records 0x7d714:$string4: Keylog Records 0x7d912:$string5: do not script --> 0x7b6b0:$string6: \pidloc.txt 0x7b70a:$string7: BSPLIT 0x7b71a:$string7: BSPLIT

Source	Rule	Description	Author	Strings
0000000A.00000002.557838555.000000000762000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0000000A.00000002.557838555.000000000762000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000000A.00000002.557838555.000000000762000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
0000000A.00000002.557838555.000000000762000.00000040.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bd2d:$hawkstr1: HawkEye Keylogger • 0x7cb6e:$hawkstr1: HawkEye Keylogger • 0x7ce9d:$hawkstr1: HawkEye Keylogger • 0x7cff8:$hawkstr1: HawkEye Keylogger • 0x7d15b:$hawkstr1: HawkEye Keylogger • 0x7d3d4:$hawkstr1: HawkEye Keylogger • 0x7b8bb:$hawkstr2: Dear HawkEye Customers! • 0x7cef0:$hawkstr2: Dear HawkEye Customers! • 0x7d047:$hawkstr2: Dear HawkEye Customers! • 0x7d1ae:$hawkstr2: Dear HawkEye Customers! • 0x7b9dc:$hawkstr3: HawkEye Logger Details:
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.InstallUtil.exe.74d0000.9.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
10.2.InstallUtil.exe.7b80000.10.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
10.2.InstallUtil.exe.7bfa72.3.raw.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x1dc56:$key: HawkEyeKeylogger • 0x1fe48:$salt: 099u787978786 • 0x1e263:$string1: HawkEye_Keylogger • 0x1f0b6:$string1: HawkEye_Keylogger • 0x1fda8:$string1: HawkEye_Keylogger • 0x1e64c:$string2: holdermail.txt • 0x1e66c:$string2: holdermail.txt • 0x1e58e:$string3: wallet.dat • 0x1e5a6:$string3: wallet.dat • 0x1e5bc:$string3: wallet.dat • 0x1f98a:$string4: Keylog Records • 0x1fca2:$string4: Keylog Records • 0x1fea0:$string5: do not script --> • 0x1dc3e:$string6: \pidloc.txt • 0x1dc98:$string7: BSPLIT • 0x1dca8:$string7: BSPLIT
10.2.InstallUtil.exe.7bfa72.3.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
10.2.InstallUtil.exe.7bfa72.3.raw.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 78 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Changes the view of files in windows explorer (hidden files and folders)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Tries to steal Mail credentials (via file registry)

Tries to steal Mail credentials (via file access)

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

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality:

Yara detected HawkEye Keylogger

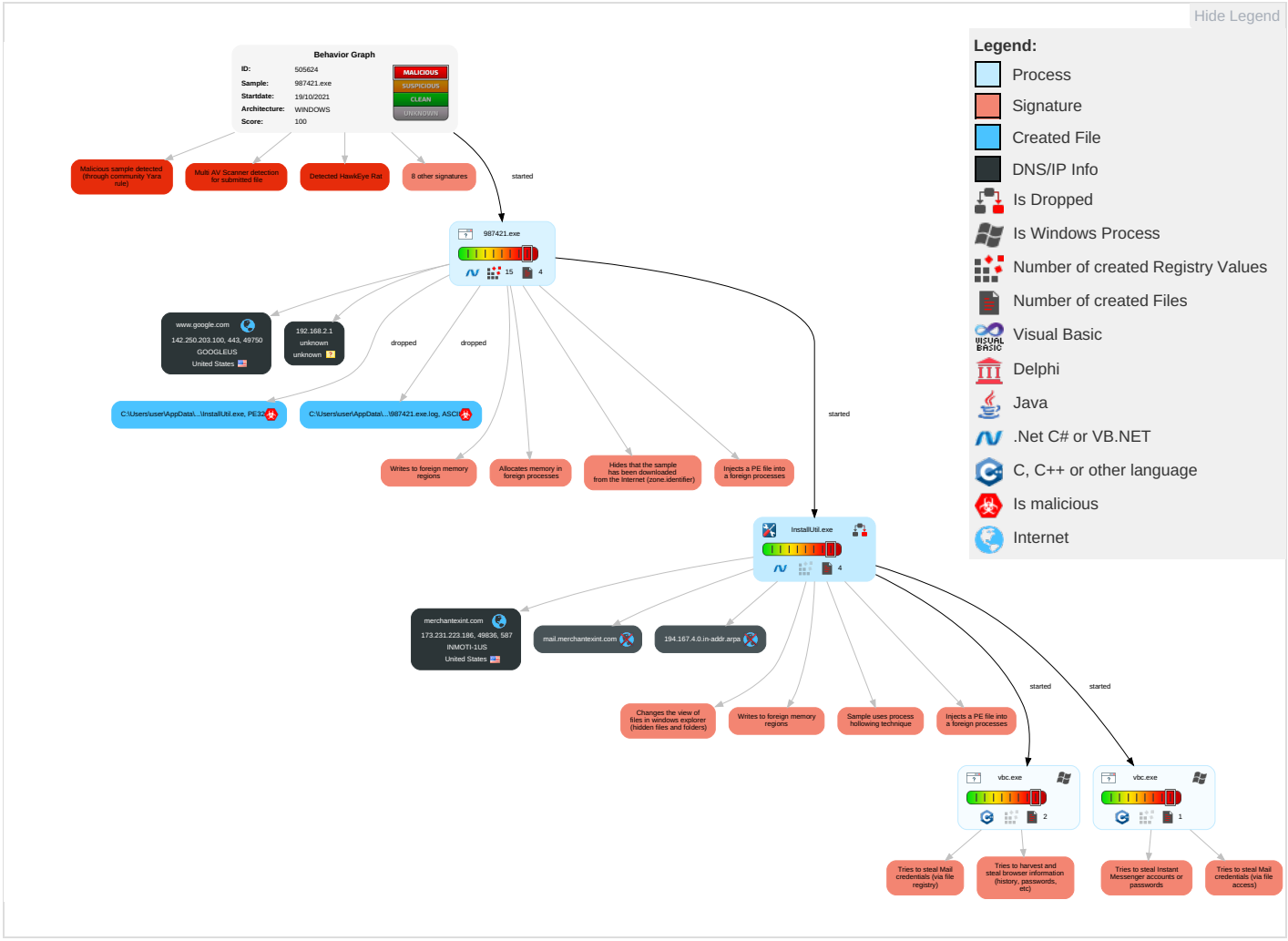
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ir T

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	E C
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	N P
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	R A S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	System Information Discovery 1 9	SSH	Clipboard Data 1	Data Transfer Size Limits	N A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	A L P
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 2	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F P
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

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
987421.exe	39%	ReversingLabs	Win32.Trojan.AgentTesla	
987421.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.987421.exe.446dc1a.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
10.2.InstallUtil.exe.760000.1.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
10.2.InstallUtil.exe.760000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
merchantexint.com	0%	Virustotal		Browse
194.167.4.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.kr-c	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessedw	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sandoll.co.kr?	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFK	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.sandoll.co.krim	0%	URL Reputation	safe	
http://www.carterandcone.comncy	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://www.fontbureau.comalsoe	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.fontbureau.comow	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.urwpp.deld	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	URL Reputation	safe	
http://www.carterandcone.comroa	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comF6	0%	Avira URL Cloud	safe	
http://www.monotype.q	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/w	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.fontbureau.comasno	0%	Avira URL Cloud	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.fontbureau.comdw	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivd	0%	Avira URL Cloud	safe	
http://en.wikip_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://www.galapagosdesign.com//	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/OldConvergedLogin_PCore_xqcDwEKeDux9oCNjuqEZ-A2.js	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://mail.merchantexint.com	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.203.100	true	false		high
merchantexint.com	173.231.223.186	true	false	• 0%, Virustotal, Browse	unknown
mail.merchantexint.com	unknown	unknown	false		unknown
194.167.4.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.231.223.186	merchantexint.com	United States		54641	INMOTI-1US	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	505624
Start date:	19.10.2021
Start time:	16:28:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	987421.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@7/6@4/3
EGA Information:	Failed

HDC Information:	• Successful, ratio: 5.6% (good quality ratio 4.6%) • Quality average: 66.9% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:29:46	API Interceptor	204x Sleep call for process: 987421.exe modified
16:30:54	API Interceptor	25x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
173.231.223.186	482471.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INMOTI-1US	70654 SSEBACT.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	70654 SSEBACT.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	BANKING INFORMATION.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	Angebot Anfrage Maschinensucher YOM.exe	Get hash	malicious	Browse	• 173.205.124.65
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	SecuriteInfo.com.__vbaHresultCheckObj.9268.exe	Get hash	malicious	Browse	• 104.247.76.214
	TRANSFER REQUEST FORM.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	TRANSFER REQUEST FORM.exe	Get hash	malicious	Browse	• 104.193.14 2.174
	Equiniti.AP Summary.3405.html	Get hash	malicious	Browse	• 173.231.22 0.228
	ugsuHxq7Ey.exe	Get hash	malicious	Browse	• 209.182.206.86
	waff.xls	Get hash	malicious	Browse	• 173.231.245.32
	QOJ48GT1(09-17-2021).vbs	Get hash	malicious	Browse	• 199.250.20 2.192
	QJfoKgzkov.exe	Get hash	malicious	Browse	• 199.250.19 9.190
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93
	Dynamic_OrderDetails&Invoice.js	Get hash	malicious	Browse	• 199.250.194.93
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Halkbank_Ekstre_202110019_095125_132879.exe	Get hash	malicious	Browse	• 142.250.203.100
	hesapshareketi-01.pdf.exe	Get hash	malicious	Browse	• 142.250.203.100
	TDH_011523075202IMG.exe	Get hash	malicious	Browse	• 142.250.203.100
	Purchase Order PDF.exe	Get hash	malicious	Browse	• 142.250.203.100
	TDH_71036210065IMG.xls	Get hash	malicious	Browse	• 142.250.203.100
	eLJyojaW0RFPJhK.exe	Get hash	malicious	Browse	• 142.250.203.100
	TDH_71036210065IMG.exe	Get hash	malicious	Browse	• 142.250.203.100
	banka_ekstresi_10-18-2021.exe	Get hash	malicious	Browse	• 142.250.203.100
	New order WEEK 42.exe	Get hash	malicious	Browse	• 142.250.203.100
	SecuriteInfo.com.Variant.MSILKrypt.4.27251.exe	Get hash	malicious	Browse	• 142.250.203.100
	hesapshareketi-01.exe	Get hash	malicious	Browse	• 142.250.203.100
	_10_2021.exe	Get hash	malicious	Browse	• 142.250.203.100
	DHL AWB.pdf.exe	Get hash	malicious	Browse	• 142.250.203.100
	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	• 142.250.203.100
	hesapshareketi-01.PDF.exe	Get hash	malicious	Browse	• 142.250.203.100
	RFQ-10202114365.vbs	Get hash	malicious	Browse	• 142.250.203.100
	hesapshareketi-01.exe	Get hash	malicious	Browse	• 142.250.203.100
	PO.exe	Get hash	malicious	Browse	• 142.250.203.100
	785963.exe	Get hash	malicious	Browse	• 142.250.203.100
	Ref 0180066743.vbs	Get hash	malicious	Browse	• 142.250.203.100

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	1jFL48LG1f.exe	Get hash	malicious	Browse	
	_10_2021.exe	Get hash	malicious	Browse	
	785963.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Cerbu.117505.10723.exe	Get hash	malicious	Browse	
	201586.exe	Get hash	malicious	Browse	
	UmCQxOLk0D.exe	Get hash	malicious	Browse	
	DO1021.exe	Get hash	malicious	Browse	
	YkvUaJLax2.exe	Get hash	malicious	Browse	
	Bankdetails86507.exe	Get hash	malicious	Browse	
	13MH7svRRs.exe	Get hash	malicious	Browse	
	amJMFKmRB2.exe	Get hash	malicious	Browse	
	75lT7DuXrs.exe	Get hash	malicious	Browse	
	NZi63BWERD.exe	Get hash	malicious	Browse	
	p6fx0L15Ae.exe	Get hash	malicious	Browse	
	Mn21Tzx74m.exe	Get hash	malicious	Browse	
	3NJdgX4P5W.exe	Get hash	malicious	Browse	
	GZ904kda5f.exe	Get hash	malicious	Browse	
	FedExOVO PRA#U0106ENJE-pdf.exe	Get hash	malicious	Browse	
	.07.2021.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\987421.exe.log	
Process:	C:\Users\user\Desktop\987421.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKoesXE8:MIHK5HKXE1qHxvbHK5AHKzvRYHKhQnoe
MD5:	1B32E71ED0326337C6593D13A55E54F4
SHA1:	0452CD9E26B6C35A3D186FD6DDB1B3365AFDB16C
SHA-256:	047E61E1F57F4922CA346203710E828859BB61800D9A72C2E64092EBB218CCA8
SHA-512:	1B5BF6D43F14FFEC6A58366222F606CB9EA1781E9E4A7E6F340E9982DD82F296ACA693EA94105F78705C01D254A7B7897050C7289CC942122C7B83221CC15DA
Malicious:	**true**
Reputation:	moderate, very likely benign file
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..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.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\987421.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 1jFL48LG1f.exe, Detection: malicious, Browse • Filename: _10_2021.exe, Detection: malicious, Browse • Filename: 785963.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Cerbu.117505.10723.exe, Detection: malicious, Browse • Filename: 201586.exe, Detection: malicious, Browse • Filename: UmCQxOLk0D.exe, Detection: malicious, Browse • Filename: DO1021.exe, Detection: malicious, Browse • Filename: YkvUaJLax2.exe, Detection: malicious, Browse • Filename: Bankdetails86507.exe, Detection: malicious, Browse • Filename: 13MH7svRRs.exe, Detection: malicious, Browse • Filename: amJMFKmRB2.exe, Detection: malicious, Browse • Filename: 75lT7DuXrs.exe, Detection: malicious, Browse • Filename: NZi63BWERD.exe, Detection: malicious, Browse • Filename: p6fx0L15Ae.exe, Detection: malicious, Browse • Filename: Mn21Tzx74m.exe, Detection: malicious, Browse • Filename: 3NJdgX4P5W.exe, Detection: malicious, Browse • Filename: GZ904kda5f.exe, Detection: malicious, Browse • Filename: FedExOVO PRA#U0106ENJE-pdf.exe, Detection: malicious, Browse • Filename: .07.2021.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Temp\bhvCA0A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xa8f0ce9c, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688

C:\Users\user\AppData\Local\Temp\bhvCA0A.tmp	
Entropy (8bit):	1.0500074532746373
Encrypted:	false
SSDEEP:	24576:+UlA2TaNxucRfDw/ZD0Xko5QqbMgSFDb7uBi:oRfDDy
MD5:	75C00C30F27079918155B76A8A191FA2
SHA1:	AF42DB18B94CCA7218275D513923866D270C80AD
SHA-256:	7C3545274D802709DFB528F9AFD130075C1A0F20E40C0F544DE8EA565888E148
SHA-512:	BFECFAA9ECA4E0ED79E24E6975211A4010D3AA24902B4DC1B72E3A7292D5E59998CC96398363A8506D87775306A2F39C7BE8A1C3634A374DB507AFDEA0DEBC3D
Malicious:	false
Reputation:	low
Preview:	....F1.....te3....wg.....o.....yG.....y..h.q.....6..43....wl.....Z.....B..... ....y..... .....x.....y.}.....5...1....y..... .....

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:CV:CV
MD5:	659B7B42E9C002CE0075077CD55A1623
SHA1:	7C51F33F354F6755A5C2D63F4FFB0AA5ADBCB825
SHA-256:	28C83F4635D193B3CF29A03DCDA640E46122AF04869854943F7364387164E212
SHA-512:	1DDB6234BB5395C973CDA4CBB5B71E849D341583019CABD294FE9A34CAD349E76B9E3A87B7FDC0A1A07EA169B7DF5C87D314FED610485BE4E22B0283E8CB5AF
Malicious:	false
Preview:	6920

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.361973558701858
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAIOWRxRI0dAn:oNWXp+N23f5RndA
MD5:	8069A620598F6D0795A045BC4C040FCE
SHA1:	BE6C7D1B6E3A49925674F335C601A53E985A2496
SHA-256:	85E54950497C2B5262439CC09BB7E0779225EAFF0C50B75D59DECE689F2B0625
SHA-512:	D9AB55D7A597CB3DB20E069AA4893654C7033E42738AD5CF3AA489C5745E3D85CBAD12530542241CD2133C52E108368AA5DB7255692177745A1EEAAFB339830
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.459765346752096
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:	987421.exe
File size:	1335296
MD5:	75e71ba1842dc3f63198386adb92716f
SHA1:	3dac2a6f86bf211fe4ed33f21dc63bbd1ff04114
SHA256:	72946d33bc1e3945ed628d129fcc9096dc1ff9cedcfe2fe568ade44544519a20
SHA512:	e0c2b6d689d6455e46d97079f28fcf7219a043bb1cb943c0d16ea5220b07f6bcc3267382db6a99783f3c2a0d6ec47e10f67a31491fc8bf9612eb15d3c7cdc834
SSDEEP:	24576:VWkquDJ+ssHgu3bt5KbLmYeKSKLRzFmt5J2NYKF:NqqARQyYV9FmzJ2j
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....1P.....V.....t... .....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5474de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5031DAE8 [Mon Aug 20 06:36:24 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1454e4	0x145600	False	0.593298297637	data	6.4640596927	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x148000	0x57e	0x600	False	0.414713541667	data	4.06709741889	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 19, 2021 16:29:26.837239027 CEST	192.168.2.3	8.8.8.8	0xa6d4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Oct 19, 2021 16:30:49.761821032 CEST	192.168.2.3	8.8.8.8	0xec5	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Oct 19, 2021 16:31:10.206275940 CEST	192.168.2.3	8.8.8.8	0x5907	Standard query (0)	mail.merchantexint.com	A (IP address)	IN (0x0001)
Oct 19, 2021 16:31:10.438400984 CEST	192.168.2.3	8.8.8.8	0x9b98	Standard query (0)	mail.merchantexint.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 19, 2021 16:29:26.858906031 CEST	8.8.8.8	192.168.2.3	0xa6d4	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Oct 19, 2021 16:30:49.786411047 CEST	8.8.8.8	192.168.2.3	0xec5	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Oct 19, 2021 16:31:10.384677887 CEST	8.8.8.8	192.168.2.3	0x5907	No error (0)	mail.merchantexint.com	merchantexint.com		CNAME (Canonical name)	IN (0x0001)
Oct 19, 2021 16:31:10.384677887 CEST	8.8.8.8	192.168.2.3	0x5907	No error (0)	merchantexint.com		173.231.223.186	A (IP address)	IN (0x0001)
Oct 19, 2021 16:31:10.545103073 CEST	8.8.8.8	192.168.2.3	0x9b98	No error (0)	mail.merchantexint.com	merchantexint.com		CNAME (Canonical name)	IN (0x0001)
Oct 19, 2021 16:31:10.545103073 CEST	8.8.8.8	192.168.2.3	0x9b98	No error (0)	merchantexint.com		173.231.223.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	142.250.203.100	443	C:\Users\user\Desktop\987421.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive
2021-10-19 14:29:27 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 19 Oct 2021 14:29:27 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: CONSENT=PENDING+100; expires=Fri, 01-Jan-2038 00:00:00 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=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
2021-10-19 14:29:27 UTC	0	IN	Data Raw: 35 30 33 62 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 74 65 6d 73 63 6f 70 65 3d 22 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 66 72 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 2f 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 Data Ascii: 503b<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="fr"><head><meta c ontent="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/googleg/1x/googleg _standard_color_128dp.png" itemprop="image"><
2021-10-19 14:29:27 UTC	1	IN	Data Raw: 2c 32 30 32 33 2c 31 37 37 37 2c 35 32 30 2c 31 34 36 37 30 2c 33 32 32 37 2c 34 31 39 2c 32 34 32 36 2c 37 2c 34 37 37 33 2c 37 35 38 31 2c 35 30 39 36 2c 31 31 36 32 35 2c 34 31 34 32 2c 35 35 33 2c 39 30 38 2c 32 2c 33 35 35 35 2c 31 33 31 34 32 2c 33 2c 33 34 36 2c 32 33 30 2c 36 34 35 39 2c 31 34 39 2c 31 33 39 37 35 2c 31 2c 31 2c 32 2c 31 35 32 38 2c 32 33 30 34 2c 31 32 33 36 2c 35 38 30 33 2c 34 36 38 34 2c 32 30 31 34 2c 31 31 35 30 31 2c 33 38 32 34 2c 33 30 35 30 2c 32 36 35 38 2c 37 33 35 37 2c 33 30 2c 38 39 34 2c 34 37 32 31 2c 34 39 2c 37 39 36 34 2c 32 33 30 35 2c 36 33 38 2c 31 38 32 38 30 2c 35 38 31 32 2c 32 35 34 35 2c 34 30 39 34 2c 31 37 2c 33 31 32 31 2c 36 2c 39 30 38 2c 33 2c 33 35 34 31 2c 31 2c 31 34 37 31 30 2c 31 38 31 35 2c Data Ascii: ,2023,1777,520,14670,3227,419,2426,7,4773,7581,5096,11625,4142,553,908,2,3555,13142,3,346,230,6459 ,149,13975,1,1,2,1528,2304,1236,5803,4684,2014,11501,3824,3050,2658,7357,30,894,4721,49,7964,2305,638,18280,58 12,2545,4094,17,3121,6,908,3,3541,1,14710,1815,
2021-10-19 14:29:27 UTC	2	IN	Data Raw: 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 6c 3b 61 26 26 28 21 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 7c 7c 21 28 62 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 6c 65 69 64 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 7d 0a 66 75 6e 63 74 69 6f 6e 20 6e 28 61 2c 62 2c 63 2c 64 2c 67 29 7b 76 61 72 Data Ascii: f=this||self;var h,k=[];function l(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;retur n b||h}function m(a){for(var b=null;a&&(!a.getAttribute||!(b=a.getAttribute("leid")));)a=a.parentNode;return b}function n(a,b,c,d,g){var
2021-10-19 14:29:27 UTC	3	IN	Data Raw: 6c 28 74 68 69 73 29 3b 67 6f 6f 67 6c 65 2e 66 3d 7b 7d 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 73 75 62 6d 69 74 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 69 66 28 61 3d 62 2e 74 61 72 67 65 74 29 7b 76 61 72 20 63 3d 61 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 73 75 62 6d 69 74 66 61 6c 73 65 22 29 3b 61 3d 22 31 22 3d 3d 3d 63 7c 7c 22 71 22 3d 3d 3d 63 26 26 21 61 2e 65 6c 65 6d 65 6e 74 73 2e 71 2e 76 61 6c 75 65 3f 21 30 3a 21 31 7d 65 6c 73 65 20 61 3d 21 31 3b 61 26 26 28 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 62 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 Data Ascii: l(this);google.f={};(function(){document.documentElement.addEventListener("submit",function(b){var a;if(a=b. target){var c=a.getAttribute("data-submitfalse");a="1"===c||"q"===c&&!a.elements.q.value?!0:!1}else a=!1;a&&(b .preventDefault(),b.stopPropagation(
2021-10-19 14:29:27 UTC	5	IN	Data Raw: 74 3a 30 7d 2e 67 62 78 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 78 6f 7b 6f 70 61 63 69 74 79 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 30 29 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 3b 74 6f 70 3a 2d 39 39 39 70 78 3b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 2d 31 70 78 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c Data Ascii: t:0}.gbxx{display:none !important}.gbxo{opacity:0 !important;filter:alpha(opacity=0) !important}.gbm{positio n:absolute;z-index:999;top:-999px;visibility:hidden;text-align:left;border:1px solid #bebebe;background:#fff;-moz-box-sh adow:-1px 1px 1px rgba(0,0,
2021-10-19 14:29:27 UTC	6	IN	Data Raw: 31 7d 2e 67 62 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 3b 70 61 64 64 69 6e 67 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 67 62 74 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 74 6f 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 2d 77 65 62 6b 69 74 2d 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 Data Ascii: 1}.gbt{position:relative;display:-moz-inline-box;display:inline-block;line-height:27px;padding:0;vertical-al ign:top}.gbt{*display:inline}.gbto{box-shadow:0 2px 4px rgba(0,0,0,.2);-moz-box-shadow:0 2px 4px rgba(0,0,0,.2);-webkit- box-shadow:0 2px 4px rgba(0

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	7	IN	Data Raw: 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 78 3b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 70 64 6a 73 20 2e 67 62 74 6f 20 2e 67 62 6d 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 39 25 7d 2e 67 62 7a 30 6c 20 2e 67 62 74 62 32 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 63 6f 6c 6f 72 3a 23 64 64 34 62 33 39 21 69 6d 70 6f 72 74 61 6e 74 7d 23 67 62 69 34 73 2c 23 67 62 69 34 73 31 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 23 67 62 67 36 2e 67 62 67 74 2d 68 76 72 2c 23 67 62 67 36 2e 67 62 67 74 3a 66 6f 63 75 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 Data Ascii: und-repeat:repeat-x;outline:none;text-decoration:none !important}.gbpdjs .gbto .gbm{min-width:99%}.gbz0l .gb tb2{border-top-color:#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbgt-hvr,#gbg6.gbgt:focus{background-color:transparent;background-imag
2021-10-19 14:29:27 UTC	8	IN	Data Raw: 6f 72 3a 23 39 30 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 33 36 63 20 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 67 62 6d 74 2c 2e 67 62 6d 74 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 62 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 2c 2e 67 62 6d 6c 62 3a 76 69 73 69 74 65 64 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c Data Ascii: or:#900 !important}.gbmt,.gbml1,.gbmlb,.gbmt:visited,.gbml1:visited,.gbmlb:visited{color:#36c !important;text-decoration:none !important}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{display:inline-block;margin:0 10px}.gbml
2021-10-19 14:29:27 UTC	10	IN	Data Raw: 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 47 42 4d 43 43 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 2c 23 47 42 4d 50 41 4c 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 61 66 74 65 72 7b 63 6f 6e 74 65 6e 74 3a 27 5c 30 41 5c 30 41 27 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 7d 23 67 62 6d 70 73 7b 2a 7a 6f 6f 6d 3a 31 7d 23 67 62 64 34 20 2e 67 62 70 63 2c 23 67 62 6d 70 61 73 20 2e 67 62 6d 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 37 70 78 7d 23 67 62 64 34 20 2e 67 62 70 67 73 20 2e 67 62 6d 74 63 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 23 67 62 64 34 20 2e 67 62 6d 74 63 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c Data Ascii: margin:0;line-height:27px}.GBMCC:last-child:after,#GBMPAL:last-child:after{content:'\0A\0A';white-space:pre;position:absolute}#gbmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpgs .gbmtc{line-height:27px}#gbd4 .gbmtc{border-bottom:1px sol
2021-10-19 14:29:27 UTC	11	IN	Data Raw: 69 67 6e 3a 72 69 67 68 74 7d 23 67 62 6d 70 61 73 62 20 2e 67 62 70 73 7b 63 6f 6c 6f 72 3a 23 30 30 30 7d 23 67 62 6d 70 61 6c 20 2e 67 62 71 66 62 62 7b 6d 61 72 67 69 6e 3a 30 20 32 30 70 78 7d 2e 67 62 70 30 20 2e 67 62 70 73 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 61 2e 67 62 69 62 61 7b 6d 61 72 67 69 6e 3a 38 70 78 20 32 30 70 78 20 31 30 70 78 7d 2e 67 62 6d 70 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 7 0 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 78 76 7b 76 69 73 69 62 69 6c 69 74 79 3a 68 69 64 64 65 6e 7d 2e 67 62 6d 70 69 61 61 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 Data Ascii: ign:right}#gbmpasb .gbps{color:#000}#gbmpal .gbqfbb{margin:0 20px}.gbp0 .gbps{*display:inline}a.gb iba{margin:8px 20px 10px}.gbmpiaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-top:10px}.g bxv{visibility:hidden}.gbmpiaa{display:block;ma
2021-10-19 14:29:27 UTC	12	IN	Data Raw: 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 7d 2e 67 62 71 66 62 2d 68 76 72 2c 2e 67 62 71 66 62 61 2d 68 76 72 2c 2e 67 62 71 66 62 62 2d 68 76 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 67 62 71 66 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 61 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 2c 2e 67 62 71 66 62 62 3a 3a 2d 6d 6f 7a 2d 66 6f 63 75 73 2d 69 6e 6e 65 72 7b 62 6f 72 64 65 72 3a Data Ascii: ox-shadow:none}.gbqfb-hvr,.gbqfba-hvr,.gbqfbb-hvr{-webkit-box-shadow:0 1px 1px rgba(0,0,0,.1);-moz-box-shadow:0 1px 1px rgba(0,0,0,.1);box-shadow:0 1px 1px rgba(0,0,0,.1)}.gbqfb::-moz-focus-inner,.gbqfba::-moz-focus-inner,.gbqfbb::-moz-focus-inner{border:
2021-10-19 14:29:27 UTC	14	IN	Data Raw: 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 34 64 39 30 66 65 2c 23 33 35 37 61 65 38 29 7d 2e 67 62 71 66 62 3a 61 63 74 69 76 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 2d 77 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 20 30 2c 20 30 2c 20 30 2e 33 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 Data Ascii: d90fe,#357ae8);background-image:-o-linear-gradient(top,#4d90fe,#357ae8);background-image:linear-gradient(top,#4d90fe,#357ae8)}.gbqfb:active{background-color:inherit;-webkit-box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3);-moz-box-shadow:inset 0 1px 2px rgba
2021-10-19 14:29:27 UTC	15	IN	Data Raw: 64 69 65 6e 74 28 73 74 61 72 74 43 6f 6c 6f 72 53 74 72 3d 27 23 66 38 66 38 66 38 27 2c 45 6e 64 43 6f 6c 6f 72 53 74 72 3d 27 23 66 31 66 31 66 31 27 29 7d 2e 67 62 71 66 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 29 2c 74 6f 28 23 66 62 66 62 66 62 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 66 2c 23 66 62 66 62 66 62 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 2d 6c 69 6e 65 61 Data Ascii: dient(startColorStr='#f8f8f8',EndColorStr='#f1f1f1')}.gbqfbb{background-color:#fff;background-image:-webkit-gradient(linear,left top,left bottom,from(#fff),to(#fbfbfb));background-image:-webkit-linear-gradient(top,#fff,#fbfbfb);background-image:-moz-linea
2021-10-19 14:29:27 UTC	16	IN	Data Raw: 69 76 65 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 32 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 0a 23 67 62 6d 70 61 73 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 32 30 70 78 7d 23 67 62 6d 6d 7b 6d 61 78 2d 68 65 69 67 68 74 3a 35 33 30 70 78 7d 2e 67 62 73 62 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 Data Ascii: ive{-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}#gbmpas{max-height:220px}#gbmm{max-height:530px}.gbsb{-webkit-box-sizing:border-box;display:block;position:rela

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	17	IN	Data Raw: 61 28 30 2c 30 2c 30 2c 2e 31 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 2e 35 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 38 29 29 2c 63 6f 6c 6f 72 2d 73 74 6f 70 28 31 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 62 6f 74 74 6f 6d 2c 6c 65 66 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 29 2c 74 6f 28 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 62 6f 74 74 6f 6d 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 Data Ascii: a(0,0,0,.1)),color-stop(.5,rgba(0,0,0,.8)),color-stop(1,rgba(0,0,0,.1)));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.2)),to(rgba(0,0,0,0)));background-image:-webkit-linear-gradient(bottom,rgba(0,0,0, .2),rgba(0,0,0,0));backgrou
2021-10-19 14:29:27 UTC	19	IN	Data Raw: 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 33 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 6c 73 62 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 3a 73 6f 6c 69 64 20 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 64 63 65 30 20 23 37 30 37 35 37 61 20 23 37 30 37 35 37 61 20 23 64 61 64 63 65 30 3b 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 6c 73 62 62 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 23 57 71 51 41 4e 62 20 61 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 3a 30 20 31 32 70 78 7d 2e 6c 73 62 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 69 6d 61 67 65 73 2f 6e 61 76 5f 6c 6f 67 6f 32 32 39 2e 70 6e 67 29 20 30 20 2d 32 36 31 70 78 20 72 65 70 65 61 Data Ascii: margin-left:13px;font-size:11px}.lsbb{background:#f8f9fa;border:solid 1px;border-color:#dadce0 #70757a #70757a #dadce0;height:30px}.lsbb{display:block}#WqQANb a{display:inline-block;margin:0 12px}.lsb{background:url(/images/nav_logo229.png) 0 -261px repea
2021-10-19 14:29:27 UTC	20	IN	Data Raw: 7c 7c 67 6f 6f 67 6c 65 2e 6c 6f 67 28 30 2c 22 22 2c 61 29 3b 72 65 74 75 72 6e 20 61 7d 3b 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 65 2c 6d 2c 64 29 7b 70 21 3d 3d 61 26 26 67 6f 6f 67 6c 65 2e 6d 6c 28 64 20 69 6e 73 74 61 6e 63 65 6f 66 20 45 72 72 6f 72 3f 64 3a 45 72 72 6f 72 28 61 29 2c 21 31 2c 76 6f 69 64 20 30 2c 21 31 2c 21 64 7c 7c 64 20 69 6e 73 74 61 6e 63 65 6f 66 20 53 79 6e 74 61 78 45 72 72 6f 72 3f 32 3a 30 29 3b 70 3d 6e 75 6c 6c 3b 6c 26 26 6e 3e 3d 6b 26 26 28 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 29 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 Data Ascii: ||google.log(0,"",a);return a};window.onerror=function(a,b,e,m,d){p!==a&&google.ml(d instanceof Error?d:Error(a),!1,void 0,!1,!d||d instanceof SyntaxError?2:0);p=null;l&&n>=k&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library
2021-10-19 14:29:27 UTC	20	IN	Data Raw: 31 31 36 0d 0a 22 63 66 67 22 2c 62 2c 63 5d 2e 6a 6f 69 6e 28 22 2e 22 29 3b 77 69 6e 64 6f 77 2e 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 61 2c 64 29 7d 3b 76 61 72 20 67 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3d 77 69 6e 64 6f 77 2e 67 62 61 72 7c 7c 7b 7d 2c 68 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 7c 7c 7b 7d 2c 62 61 3b 66 75 6e 63 74 69 6f 6e 20 5f 74 76 6e 28 61 2c 62 29 7b 61 3d 70 61 72 73 65 49 6e 74 28 61 2c 31 30 29 3b 72 65 74 75 72 6e 20 69 73 4e 61 4e 28 61 29 3f 62 3a 61 7d 66 75 6e 63 74 69 6f 6e 20 5f 74 76 6e 28 61 2c 62 29 7b 61 3d 70 61 72 73 65 46 6c 6f 61 74 28 61 29 3b 72 65 74 75 72 6e 20 69 73 4e 61 4e 28 61 29 3f 62 3a 61 7d 66 75 6e 63 74 69 6f 6e 20 5f 74 76 76 28 61 29 7b 72 65 Data Ascii: 116"cfg",b,c].join(".");window.gbar.logger.ml(a,d)};var g=window.gbar=window.gbar||{},h=window.gbar.i=window.gbar.i||{},ba;function _tvn(a,b){a=parseInt(a,10);return isNaN(a)?b:a}function _tvf(a,b){a=parseFloat(a);return isNaN(a)?b:a}function _tvv(a){re
2021-10-19 14:29:27 UTC	21	IN	Data Raw: 36 65 38 31 0d 0a 7c 7c 67 29 5b 61 5d 3d 62 7d 67 2e 62 76 3d 7b 6e 3a 5f 74 76 6e 28 22 32 22 2c 30 29 2c 72 3a 22 22 2c 66 3a 22 2e 36 36 2e 22 2c 65 3a 22 22 2c 6d 3a 5f 74 76 6e 28 22 31 22 2c 31 29 7d 3b 0a 66 75 6e 63 74 69 6f 6e 20 63 61 28 61 2c 62 2c 63 29 7b 76 61 72 20 64 3d 22 6f 6e 22 2b 62 3b 69 66 28 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 29 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 62 2c 63 2c 21 31 29 3b 65 6c 73 65 20 69 66 28 61 2e 61 74 74 61 63 68 45 76 65 6e 74 29 61 2e 61 74 74 61 63 68 45 76 65 6e 74 28 64 2c 63 29 3b 65 6c 73 65 7b 76 61 72 20 66 3d 61 5b 64 5d 3b 61 5b 64 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6b 3d 66 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 2c Data Ascii: 6e81||g)[a]=b}g.bv={n:_tvn("2",0),r:"",f:".66.",e:"",m:_tvn("1",1)};function ca(a,b,c){var d="on"+b;if(a.addEventListener)a.addEventListener(b,c,!1);else if(a.attachEvent)a.attachEvent(d,c);else{var f=a[d];a[d]=function(){var k=f.apply(this,arguments),
2021-10-19 14:29:27 UTC	22	IN	Data Raw: 7c 7c 63 5b 31 5d 2e 73 7c 7c 28 63 5b 31 5d 2e 73 3d 21 30 2c 73 61 28 32 2c 61 29 2c 63 5b 31 5d 2e 75 72 6c 26 26 72 61 28 63 5b 31 5d 2e 75 72 6c 2c 61 29 2c 63 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 63 5b 31 5d 2e 6c 69 62 73 29 29 7d 2c 74 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 67 63 22 2c 61 29 7d 2c 75 61 3d 6e 75 6c 6c 2c 76 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 75 61 3d 61 7d 2c 73 61 3d 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 75 61 29 7b 61 3d 7b 74 3a 61 2c 62 3a 62 7d 3b 69 66 28 63 29 66 6f 72 28 76 61 72 20 64 20 69 6e 20 63 29 61 5b 64 5d 3d 63 5b 64 5d 3b 74 72 79 7b 75 61 28 61 29 7d 63 61 74 63 68 28 66 29 7b 7d 7d 3b 70 28 22 6d 64 63 22 2c 76 29 3b 70 28 22 6d 64 69 22 2c 6c 61 29 3b 70 28 22 Data Ascii: ||c[1].s||(c[1].s=!0,sa(2,a),c[1].url&&ra(c[1].url,a),c[1].libs&&C&&C(c[1].libs))},ta=function(a){A("gc",a)},ua=null,va=function(a){ua=a},sa=function(a,b,c){if(ua){a={t:a,b:b};if(c)for(var d in c)a[d]=c[d];try{ua(a)}catch(f){}}};p("mdc",v);p("mdi",la);p("
2021-10-19 14:29:27 UTC	23	IN	Data Raw: 2e 67 6c 3d 45 61 3b 77 61 3f 41 61 2e 6c 6f 61 64 7c 7c 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3a 70 28 22 6c 6f 61 64 22 2c 42 61 2c 41 61 29 3b 70 28 22 64 67 6c 22 2c 42 61 29 3b 70 28 22 61 67 6c 22 2c 44 61 29 3b 68 2e 6f 3d 78 61 7d 3b 76 61 72 20 46 61 3d 68 2e 62 28 22 30 2e 31 22 2c 2e 30 30 31 29 2c 47 61 3d 30 3b 0a 66 75 6e 63 74 69 6f 6e 20 5f 6d 6c 54 6f 6b 65 6e 28 61 2c 62 29 7b 74 72 79 7b 69 66 28 31 3e 47 61 29 7b 47 61 2b 2b 3b 76 61 72 20 63 3d 61 3b 62 3d 62 7c 7c 7b 7d 3b 76 61 72 20 64 3d 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 2c 66 3d 5b 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 65 6e 5f 32 30 34 3f 61 74 79 70 3d 69 26 7a 78 3d 22 2c 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 Data Ascii: .gl=Ea;wa?Aa.load||p("load",Ba,Aa):p("load",Ba,Aa);p("dgl",Ba);p("agl",Da);h.o=xa};var Fa=h.b("0.1",.001),Ga=0;function _mlToken(a,b){try{if(1>Ga){Ga++;var c=a;b=b||{};var d=encodeURIComponent,f=["//www.google.com/gen_204?atyp=i&zx=",(new Date).getTime()
2021-10-19 14:29:27 UTC	24	IN	Data Raw: 2c 62 29 7d 2c 4d 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62].apply(this,d)})}},Na=function(a){a=["//www.gstatic.com","/og/_/js/d=1/k=","og.og2.en_US.Qe4simkQlto.O","/rt=j/m=",a,"/rs=","AA2YrTt5eiRM_fN3TIDhH2J4__CG7OLQfQ"];Ka&&a.push("?host Data Ascii: ,b)},Ma=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})}},Na=function(a){a=["//www.gstatic.com","/og/_/js/d=1/k=","og.og2.en_US.Qe4simkQlto.O","/rt=j/m=",a,"/rs=","AA2YrTt5eiRM_fN3TIDhH2J4__CG7OLQfQ"];Ka&&a.push("?host

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	26	IN	Data Raw: 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 64 29 3b 69 66 28 66 29 7b 76 61 72 20 6b 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 3b 69 66 28 4f 3d 3d 64 29 4f 3d 76 6f 69 64 20 30 2c 0a 4b 28 6b 2c 22 67 62 74 6f 22 29 3b 65 6c 73 65 7b 69 66 28 4f 29 7b 76 61 72 20 6d 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 4f 29 3b 69 66 28 6d 26 26 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 29 7b 76 61 72 20 6e 3d 6d 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 6f 77 6e 65 72 22 29 3b 69 66 28 6e 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 6c 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 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 Data Ascii: document.getElementById(d);if(f){var k=b.parentNode;if(O==d)O=void 0,K(k,"gbto");else{if(O){var m=document.getElementById(O);if(m&&m.getAttribute){var n=m.getAttribute("aria-owner");if(n.length){var l=documen t.getElementById(n);l&&l.parentNode&&K(l.paren
2021-10-19 14:29:27 UTC	27	IN	Data Raw: 3c 3d 6c 29 7b 76 61 72 20 79 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 22 29 2c 7a 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 79 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 63 22 3b 7a 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 67 62 6d 74 20 67 62 6d 68 22 3b 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 7a 29 3b 6b 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 79 2c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 6c 5d 29 7d 67 2e 61 64 64 48 6f 76 65 72 26 26 67 2e 61 64 64 48 6f 76 65 72 28 61 29 7d 65 6c 73 65 20 6b 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6d 29 7d 7d 63 61 74 63 68 28 44 62 29 7b 72 28 44 62 2c 22 73 62 22 2c 22 61 6c 22 29 7d 7d 2c 65 62 3d 66 75 6e 63 74 69 6f 6e Data Ascii: <=l){var y=document.createElement("li"),z=document.createElement("div");y.className="gbmtc";z.clas sName="gbmt gbmh";y.appendChild(z);k.insertBefore(y,k.childNodes[l])}g.addHover&&g.addHover(a)}else k.appendCh ild(m)}}catch(Db){r(Db,"sb","al")}},eb=function
2021-10-19 14:29:27 UTC	28	IN	Data Raw: 66 3d 62 5b 63 5d 3b 63 2b 2b 29 7b 76 61 72 20 6b 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 0a 6b 2e 69 6e 6e 65 72 48 54 4d 4c 3d 66 3b 64 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6b 29 7d 7d 65 6c 73 65 20 64 2e 69 6e 6e 65 72 48 54 4d 4c 3d 62 3b 51 28 61 2c 21 30 29 7d 7d 7d 2c 51 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 28 62 3d 76 6f 69 64 20 30 21 3d 3d 62 3f 62 3a 21 30 29 3f 4a 28 61 2c 22 67 62 6d 73 67 6f 22 29 3a 4b 28 61 2c 22 67 62 6d 73 67 6f 22 29 7d 2c 5a 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 Data Ascii: f=b[c];c++){var k=document.createElement("div");k.innerHTML=f;d.appendChild(k)}}else d.innerHTML=b ;Q(a,!0)}}},Q=function(a,b){(b=void 0!==b?b:!0)?J(a,"gbmsgo"):K(a,"gbmsgo")},Za=function(a){for(var b=0,c;c=a.childNodes[b];b++)if(H(c,"gbmsg"))return c},P=
2021-10-19 14:29:27 UTC	29	IN	Data Raw: 73 2e 63 6c 69 65 6e 74 3a 67 61 70 69 2e 69 66 72 61 6d 65 73 22 7d 5d 29 3b 76 61 72 20 41 62 3d 7b 76 65 72 73 69 6f 6e 3a 22 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65 36 65 39 38 32 34 2e 6a 73 22 2c 69 6e 64 65 78 3a 22 22 2c 6c 61 6e 67 3a 22 66 72 22 7d 3b 76 2e 67 63 3d 41 62 3b 76 61 72 20 42 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 42 62 29 3b 68 2e 61 28 22 31 22 29 26 26 70 28 22 6c 50 57 46 22 2c 42 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 Data Ascii: s.client:gapi.iframes"}]);var Ab={version:"gci_91f30755d6a6b787dcc2a4062e6e9824.js",index:"",lang:"fr"};v.gc =Ab;var Bb=function(a){window.googleapis&&window.iframes?a&&a():(a&&ta(a),D("gc"))};p("lGC",Bb);h.a("1")&&p("l PWF",Bb)};window.__PVT="";if(h.a("1")
2021-10-19 14:29:27 UTC	31	IN	Data Raw: 28 29 3b 6b 3d 64 28 22 32 38 38 33 34 22 29 3b 6d 3d 64 28 22 52 39 5a 75 59 66 5f 30 4a 49 4f 35 67 77 65 50 69 71 38 6f 22 29 3b 76 61 72 20 6c 3d 67 2e 62 76 2e 66 2c 71 3d 64 28 22 31 22 29 3b 6e 3d 64 28 6e 29 3b 63 3d 4d 61 74 68 2e 72 6f 75 6e 64 28 31 2f 63 29 3b 76 61 72 20 45 3d 64 28 22 34 30 32 31 38 32 32 33 37 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 31 31 30 30 34 2e 30 5f 70 30 22 29 2c 49 3d 64 28 22 63 6f 6d 22 29 2c 56 3d 64 28 22 66 72 22 29 2c 57 3d 0a 64 28 22 46 52 41 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 Data Ascii: ();k=d("28834");m=d("R9ZuYf_0JIO5gwePiq8o");var l=g.bv.f,q=d("1");n=d(n);c=Math.round(1/c);var E=d ("402182237.0"),U="&oggv="+d("es_plusone_gc_20211004.0_p0"),l=d("com"),V=d("fr"),W=d("FRA");var y=0;h.a("")&&(y|=1);h.a("")&&(y|=2);h.a("")&&(y|=4);a=["//ww
2021-10-19 14:29:27 UTC	32	IN	Data Raw: 69 6f 6e 28 29 7b 42 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 2e 73 70 64 28 29 7d 29 7d 3b 70 28 22 73 70 6e 22 2c 55 62 29 3b 70 28 22 73 70 70 22 2c 57 62 29 3b 70 28 22 73 70 73 22 2c 56 62 29 3b 70 28 22 73 70 64 22 2c 5a 62 29 3b 70 28 22 70 61 61 22 2c 53 62 29 3b 70 28 22 70 72 6d 22 2c 54 62 29 3b 6c 62 28 22 67 62 64 34 22 2c 54 62 29 3b 0a 69 66 28 68 2e 61 28 22 22 29 29 7b 76 61 72 20 24 62 3d 7b 64 3a 68 2e 61 28 22 22 29 2c 65 3a 22 22 2c 73 61 6e 77 3a 68 2e 61 28 22 22 29 2c 70 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 39 36 22 2c 63 70 3a 22 31 22 2c 78 70 3a 68 2e 61 28 22 31 22 29 2c 6d 67 3a 22 25 31 24 73 20 28 64 e9 Data Ascii: ion(){B(function(){g.spd()})};p("spn",Ub);p("spp",Wb);p("sps",Vb);p("spd",Zb);p("paa",Sb);p("prm",Tb);lb("gb d4",Tb);if(h.a(""){var $b={d:h.a(""),e:"",sanw:h.a(""),p:"https://lh3.googleusercontent.com/ogw/default-user=s96",cp:"1 ",xp:h.a("1"),mg:"%1$s (d
2021-10-19 14:29:27 UTC	33	IN	Data Raw: 63 6f 6f 6b 69 65 26 26 61 2e 63 6f 6f 6b 69 65 2e 6d 61 74 63 68 28 22 50 52 45 46 22 29 7d 63 61 74 63 68 28 63 29 7b 7d 72 65 74 75 72 6e 21 62 7d 2c 6a 63 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 72 65 74 75 72 6e 21 21 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 7d 63 61 74 63 68 28 61 29 7b 72 65 74 75 72 6e 21 31 7d 7d 2c 6b 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 6c 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 74 72 79 7b 69 63 28 64 6f Data Ascii: cookie&&a.cookie.match("PREF")}catch(c){}return!b},jc=function(){try{return!!e.localStorage&&"object"==typeof e.localStorage}catch(a){return!1}},kc=function(a){return a&&a.style&&a.style.behavior&&"undefined"!=typeof a.load},lc= function(a,b,c,d){try{ic(do
2021-10-19 14:29:27 UTC	35	IN	Data Raw: 28 67 2e 75 70 2c 22 73 70 6c 22 29 3b 5a 28 67 2e 75 70 2c 22 64 70 63 22 29 3b 5a 28 67 2e 75 70 2c 22 69 69 63 22 29 3b 67 2e 6d 63 66 28 22 75 70 22 2c 7b 73 70 3a 68 2e 62 28 22 30 2e 30 31 22 2c 31 29 2c 74 6c 64 3a 22 66 72 22 2c 70 72 69 64 3a 22 31 22 7d 29 3b 66 75 6e 63 74 69 6f 6e 20 71 63 28 29 7b 66 75 6e 63 74 69 6f 6e 20 61 28 29 7b 66 6f 72 28 76 61 72 20 6c 3b 28 6c 3d 6b 5b 6d 2b 2b 5d 29 26 26 22 6d 22 21 3d 6c 5b 30 5d 26 26 21 6c 5b 31 5d 2e 61 75 74 6f 3b 29 3b 6c 26 26 28 73 61 28 32 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 75 72 6c 26 26 72 61 28 6c 5b 31 5d 2e 75 72 6c 2c 6c 5b 30 5d 29 2c 6c 5b 31 5d 2e 6c 69 62 73 26 26 43 26 26 43 28 6c 5b 31 5d 2e 6c 69 62 73 29 29 3b 6d 3c 6b 2e 6c 65 6e 67 74 68 26 26 73 65 74 54 69 6d 65 6f 75 Data Ascii: (g.up,"spl");Z(g.up,"dpc");Z(g.up,"iic");g.mcf("up",{sp:h.b("0.01",1),tld:"fr",prid:"1"});function qc(){function a(){f or(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&&se tTimeou

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	36	IN	Data Raw: 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 64 3d 77 69 6e 64 6f 77 2e 67 62 61 72 2e 69 2e 69 3b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 76 61 72 20 66 3d 65 2e 69 3b 76 61 72 20 67 3d 66 2e 63 28 22 31 22 2c 30 29 2c 68 3d 2f 5c 62 67 62 6d 74 5c 62 2f 2c 6b 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 74 72 79 7b 76 61 72 20 62 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 5f 22 2b 67 29 2c 63 3d 64 6f 63 75 6d Data Ascii: "});})}();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var d=window.gbar.i.i;var e=window.gbar;var f=e.i;var g=f.c("1",0),h=/\bgbmt\b/,k=function(a){try{var b=document.getElementById("gb_"+g),c=docum
2021-10-19 14:29:27 UTC	37	IN	Data Raw: 22 29 2c 76 66 3a 22 2e 36 36 2e 22 7d 2c 67 3d 66 2c 68 3d 5b 22 62 6e 64 63 66 67 22 5d 2c 6b 3d 61 3b 68 5b 30 5d 69 6e 20 6b 7c 7c 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6b 2e 65 78 65 63 53 63 72 69 70 74 7c 7c 6b 2e 65 78 65 63 53 63 72 69 70 74 28 22 76 61 72 20 22 2b 68 5b 30 5d 29 3b 66 6f 72 28 76 61 72 20 6c 3b 68 2e 6c 65 6e 67 74 68 26 26 28 6c 3d 68 2e 73 68 69 66 74 28 29 29 3b 29 68 2e 6c 65 6e 67 74 68 7c 7c 76 6f 69 64 20 30 3d 3d 3d 67 3f 6b 3d 6b 5b 6c 5d 26 26 6b 5b 6c 5d 21 3d 3d 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 5b 6c 5d 3f 6b 5b 6c 5d 3a 6b 5b 6c 5d 3d 7b 7d 3a 6b 5b 6c 5d 3d 67 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 Data Ascii: "),vf:".66."},g=f,h=["bndcfg"],k=a;h[0]in k||"undefined"==typeof k.execScript||k.execScript("var "+h[0]);for(var l;h.length&&(l=h.shift());)h.length||void 0===g?k=k[l]&&k[l]!==Object.prototype[l]?k[l]:k[l]={}:k[l]=g;}catch(e){window.gbar&&gbar.logger&&gba
2021-10-19 14:29:27 UTC	38	IN	Data Raw: 73 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 38 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 70 73 2e 67 6f 6f 67 6c 65 2e 66 72 2f 6d 61 70 73 3f 68 6c 3d 66 72 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 66 72 26 74 61 62 3d 77 38 22 3e 3c 73 70 61 6e 20 63 6c 61 73 Data Ascii: s <li class=gbt>Maps <li class=gbt><a class=gbzt id=gb_78 href="https://play.google.com/?hl=fr&tab=w8"><span clas
2021-10-19 14:29:27 UTC	40	IN	Data Raw: 73 3d 67 62 6d 20 69 64 3d 67 62 64 20 61 72 69 61 2d 6f 77 6e 65 72 3d 67 62 7a 74 6d 3e 3c 64 69 76 20 69 64 3d 67 62 6d 6d 62 20 63 6c 61 73 73 3d 22 67 62 6d 63 20 67 62 73 62 20 67 62 73 62 69 73 22 3e 3c 6f 6c 20 69 64 3d 67 62 6d 6d 20 63 6c 61 73 73 3d 22 67 62 6d 63 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 41 67 65 6e 64 61 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 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 Data Ascii: s=gbm id=gbd aria-owner=gbztm> <ol id=gbmm class="gbmcc gbsbic"><li class=gbmtc>Agenda <li class=gbmtc><a class=gbmt id=gb_51 href="htt
2021-10-19 14:29:27 UTC	41	IN	Data Raw: 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 3e 41 63 63 6f 75 6e 74 20 4f 70 74 69 6f 6e 73 3c 2f 68 32 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 63 62 3e 3c 2f 73 70 61 6e 3e 3c 6f 6c 20 63 6c 61 73 73 3d 67 62 74 63 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 74 61 72 67 65 74 3d 5f 74 6f 70 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 63 63 6f 75 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 53 65 72 76 69 63 65 4c 6f 67 69 6e 3f 68 6c 3d 66 72 26 70 61 73 73 69 76 65 3d 74 72 75 65 26 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c Data Ascii: class=gbsbb> <h2 class=gbxx>Account Options</h2><ol class=gbtc><li class=gbt><a target=_top href="https://accounts.google.com/ServiceLogin?hl=fr&passive=true&continue=https://www.googl
2021-10-19 14:29:27 UTC	42	IN	Data Raw: 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 39 32 64 70 2e 70 6e 67 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 32 38 70 78 20 30 20 31 34 70 78 22 20 77 69 64 74 68 3d 22 32 37 32 22 20 Data Ascii: indow.gbar&&gbar.elp&&gbar.elp()</script> <br clear="all" id="lgpd"> <img alt="Google" height="92" src="/images/branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png" style="padding:28px 0 14px" width="272"
2021-10-19 14:29:27 UTC	43	IN	Data Raw: 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 4c 73 2d 77 41 4d 41 41 41 41 41 41 59 57 37 6b 56 30 5f 4c 53 6b 62 78 73 58 65 4e 68 5a 46 51 43 49 34 4a 4e 6a 63 50 70 32 68 76 22 20 6e 61 6d 65 3d 22 69 66 6c 73 69 67 22 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 74 64 3e 3c 74 64 20 63 6c 61 73 73 3d 22 66 6c 20 73 62 6c 63 22 20 61 6c 69 67 6e 3d 22 6c 65 66 74 22 20 6e 6f 77 72 61 70 3d 22 22 20 77 69 64 74 68 3d 22 32 35 25 22 3e 3c 61 20 68 72 65 66 3d 22 2f 61 64 Data Ascii: his.form.iflsig.disabled = false;}else top.location='/doodles/';});})();</script><input value="ALs-wAMAAAAAYW7kV0_LSkbxsXeNhZFQCI4JNjcPp2hv" name="iflsig" type="hidden"></td><td class="fl sblc" align="left" nowrap="" width="25%"><a href="/ad
2021-10-19 14:29:27 UTC	45	IN	Data Raw: 69 67 3d 4b 5f 34 62 64 36 34 61 52 68 55 34 66 74 4b 6c 68 36 53 54 67 4c 30 4b 73 44 34 67 30 25 33 44 22 3e 47 6f 6f 67 6c 65 2e 66 72 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 31 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 66 72 2f 70 6f 6c 69 63 69 65 73 2f 70 72 69 76 61 63 79 2f 22 3e 43 6f 6e 66 69 64 65 6e 74 69 61 6c 69 74 e9 3c 2f 61 3e 20 2d 20 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 66 72 2f 70 6f 6c 69 63 69 65 73 2f 74 65 72 6d 73 2f 22 3e 43 6f 6e 64 69 74 69 6f 6e 73 3c 2f 61 3e 3c 2f 70 3e 3c 2f 73 70 61 6e 3e 3c 2f 63 65 6e 74 65 72 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 Data Ascii: ig=K_4bd64aRhU4ftKlh6STgL0KsD4g0%3D">Google.fr © 2021 - Confidentialit - Conditions <script nonc

Timestamp	kBytes transferred	Direction	Data
2021-10-19 14:29:27 UTC	46	IN	Data Raw: 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 65 2e 74 72 75 73 74 65 64 54 79 70 65 73 3b 69 66 28 6b 26 26 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 29 7b 74 72 79 7b 62 3d 6b 2e 63 72 65 61 74 65 50 6f 6c 69 63 79 28 22 67 6f 6f 67 23 68 74 6d 6c 22 2c 7b 63 72 65 61 74 65 48 54 4d 4c 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 3a 66 2c 63 72 65 61 74 65 53 63 72 69 70 74 55 52 4c 3a 66 7d 29 7d 63 61 74 63 68 28 70 29 7b 65 2e 63 6f Data Ascii: r c="SCRIPT";"application/xhtml+xml"===b.contentType&&(c=c.toLowerCase());c=b.createElement(c);if(void 0===g){b=null;var k=e.trustedTypes;if(k&&k.createPolicy){try{b=k.createPolicy("goog#html",{createHTML:f,createScript:f,createScriptURL:f})}catch(p){e.co
2021-10-19 14:29:27 UTC	47	IN	Data Raw: 5c 78 32 32 66 6c 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 68 6f 73 74 5c 78 32 32 3a 5c 78 32 32 67 6f 6f 67 6c 65 2e 63 6f 6d 5c 78 32 32 2c 5c 78 32 32 69 73 62 68 5c 78 32 32 3a 32 38 2c 5c 78 32 32 6a 73 6f 6e 70 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6c 6d 5c 78 32 32 3a 74 72 75 65 2c 5c 78 32 32 6d 73 67 73 5c 78 32 32 3a 7b 5c 78 32 32 63 69 62 6c 5c 78 32 32 3a 5c 78 32 32 45 66 66 61 63 65 72 20 6c 61 20 72 65 63 68 65 72 63 68 65 5c 78 32 32 2c 5c 78 32 32 64 79 6d 5c 78 32 32 3a 5c 78 32 32 45 73 73 61 79 65 7a 20 61 76 65 63 20 63 65 74 74 65 20 6f 72 74 68 6f 67 72 61 70 68 65 20 3a 5c 78 32 32 2c 5c 78 32 32 6c 63 6b 79 5c 78 32 32 3a 5c 78 32 32 4a 5c 5c 75 30 30 32 36 23 33 39 3b 61 69 20 64 65 20 6c 61 20 63 68 61 6e 63 65 5c 78 32 Data Ascii: \x22fl\x22:true,\x22host\x22:\x22google.com\x22,\x22isbh\x22:28,\x22jsonp\x22:true,\x22lm\x22:true,\x22msgs\x22:{\x22cibl\x22:\x22Effacer la recherche\x22,\x22dym\x22:\x22Essayez avec cette orthographe :\x22,\x22lcky\x22:\x22J\\u0026#39;ai de la chance\x2
2021-10-19 14:29:27 UTC	48	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 19, 2021 16:31:10.883949995 CEST	587	49836	173.231.223.186	192.168.2.3	220-server.oishi7.com ESMTP Exim 4.94.2 #2 Tue, 19 Oct 2021 07:31:10 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 19, 2021 16:31:10.884293079 CEST	49836	587	192.168.2.3	173.231.223.186	EHLO 305090
Oct 19, 2021 16:31:11.016813040 CEST	587	49836	173.231.223.186	192.168.2.3	250-server.oishi7.com Hello 305090 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 19, 2021 16:31:11.017040968 CEST	49836	587	192.168.2.3	173.231.223.186	STARTTLS
Oct 19, 2021 16:31:11.151046038 CEST	587	49836	173.231.223.186	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 987421.exe PID: 4344 Parent PID: 2220

General

Start time:	16:29:24
Start date:	19/10/2021

Path:	C:\Users\user\Desktop\987421.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\987421.exe'
Imagebase:	0xf90000
File size:	1335296 bytes
MD5 hash:	75E71BA1842DC3F63198386ADB92716F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.443975090.000000000446D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.443975090.000000000446D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.443975090.000000000446D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.443975090.000000000446D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.443975090.000000000446D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.444506297.0000000004633000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.444506297.0000000004633000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.444506297.0000000004633000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.444506297.0000000004633000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.444506297.0000000004633000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: InstallUtil.exe PID: 6920 Parent PID: 4344

General

Start time:	16:30:20
Start date:	19/10/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x390000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000A.00000002.557838555.0000000000762000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000002.557838555.0000000000762000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000A.00000002.557838555.0000000000762000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000002.557838555.0000000000762000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000A.00000002.557838555.0000000000762000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000000A.00000002.563407277.0000000007B80000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000000A.00000002.563118770.00000000074D0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000002.560993203.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000002.560993203.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000A.00000002.560027305.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000A.00000002.560027305.00000000027F1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: vbc.exe PID: 7160 Parent PID: 6920

General

Start time:	16:30:58
Start date:	19/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000002.500947062.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6412 Parent PID: 6920

General

Start time:	16:30:58
Start date:	19/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.491382176.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis