ID: 483625
Sample Name: PO-INV 21460041492040401.PDF.exe
Cookbook: default.jbs
Time: 10:18:59
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

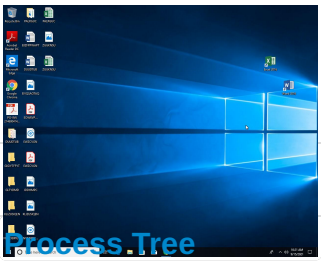
Windows Analysis Report PO-INV 21460041492040401.P…

Overview

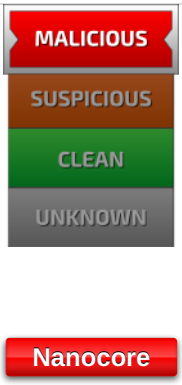
General Information

Sample Name:	PO-INV 21460041492040401.PDF.exe
Analysis ID:	483625
MD5:	8e23941e7d2bd9..
SHA1:	afd72705c4b572a.
SHA256:	3c3a536252b1c7..
Tags:	exe nanocore
Infos:	

Most interesting Screenshot:



Detection

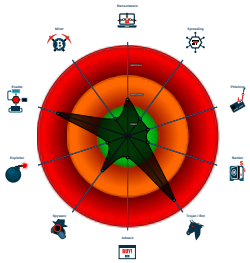


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



- **System is w10x64**
- PO-INV 21460041492040401.PDF.exe (PID: 6016 cmdline: 'C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe' MD5: 8E23941E7D2BD97F91B83AA52CE9D2EE)
  - RegAsm.exe (PID: 6304 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - schtasks.exe (PID: 6380 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD621.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6436 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDAD5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegAsm.exe (PID: 6488 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6532 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 6552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7020 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.361666966.000000000389 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x434bf:$x1: NanoCore.ClientPluginHost • 0x7619f:$x1: NanoCore.ClientPluginHost • 0xa8e6f:$x1: NanoCore.ClientPluginHost • 0x434fc:$x2: IClientNetworkHost • 0x761dc:$x2: IClientNetworkHost • 0xa8eac:$x2: IClientNetworkHost • 0x4702f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x79d0f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xac9df:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.361666966.000000000389 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.361666966.000000000389 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x43227:$a: NanoCore • 0x43237:$a: NanoCore • 0x4346b:$a: NanoCore • 0x4347f:$a: NanoCore • 0x434bf:$a: NanoCore • 0x75f07:$a: NanoCore • 0x75f17:$a: NanoCore • 0x7614b:$a: NanoCore • 0x7615f:$a: NanoCore • 0x7619f:$a: NanoCore • 0xa8bd7:$a: NanoCore • 0xa8be7:$a: NanoCore • 0xa8e1b:$a: NanoCore • 0xa8e2f:$a: NanoCore • 0xa8e6f:$a: NanoCore • 0x43286:$b: ClientPlugin • 0x43488:$b: ClientPlugin • 0x434c8:$b: ClientPlugin • 0x75f66:$b: ClientPlugin • 0x76168:$b: ClientPlugin • 0x761a8:$b: ClientPlugin
00000010.00000002.512833462.0000000002F0 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.517406804.000000000057B 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.RegAsm.exe.57b0000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
16.2.RegAsm.exe.57b0000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0.2.PO-INV 21460041492040401.PDF.exe.392cce2.4.raw .unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.PO-INV 21460041492040401.PDF.exe.392cce2.4.raw .unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.2.PO-INV 21460041492040401.PDF.exe.392cce2.4.raw .unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 68 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Yara detected Nanocore RAT

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Uses an obfuscated file name to hide its real file extension (double extension)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

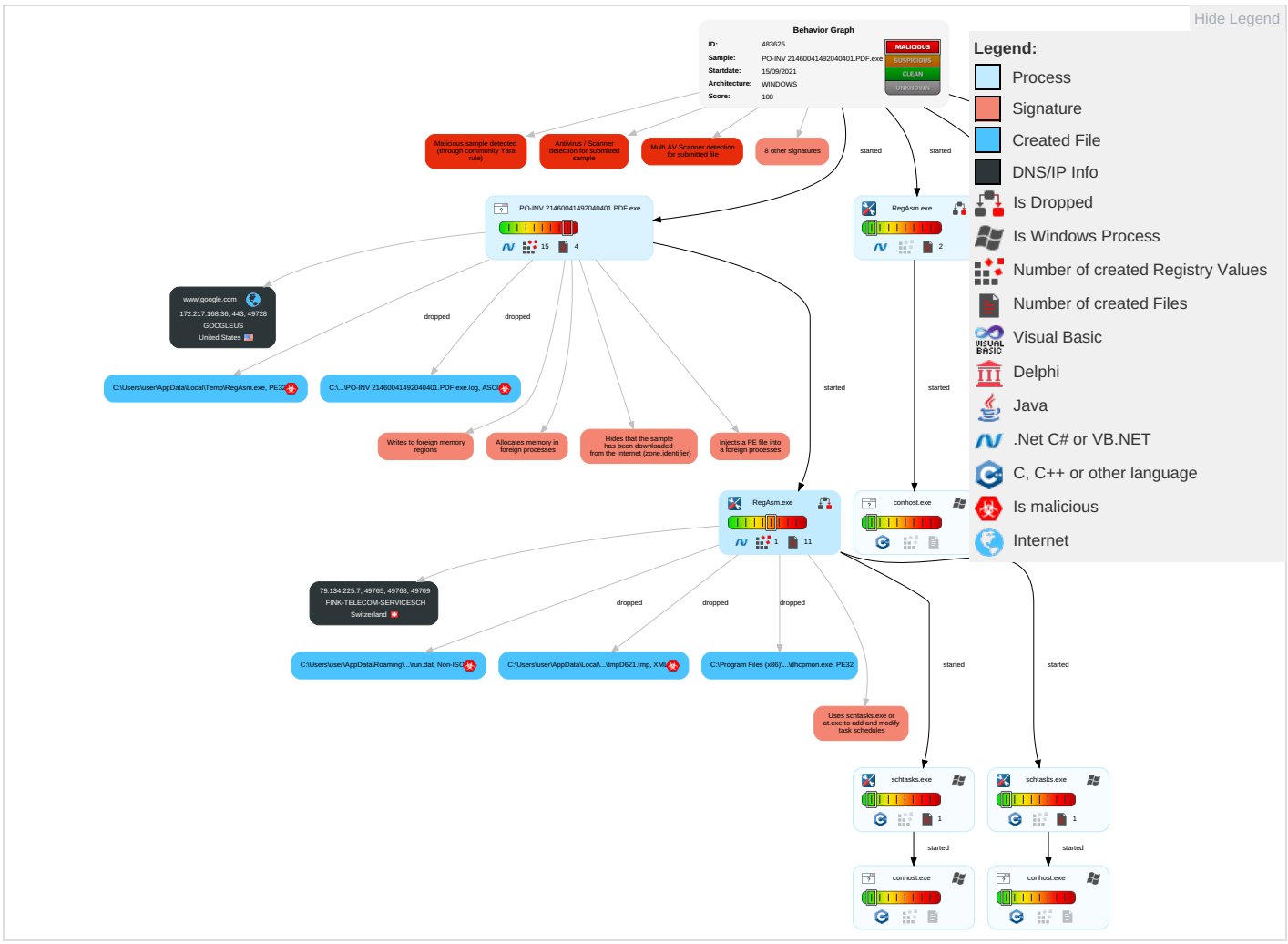
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1 2	Input Capture 2 1	Security Software Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 3	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base

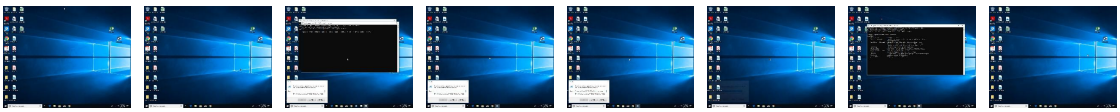
Behavior Graph



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
PO-INV 21460041492040401.PDF.exe	31%	Virustotal		Browse
PO-INV 21460041492040401.PDF.exe	20%	ReversingLabs	Win32.Trojan.Pwsx	
PO-INV 21460041492040401.PDF.exe	100%	Avira	HEUR/AGEN.1141554	
PO-INV 21460041492040401.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.PO-INV 21460041492040401.PDF.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1141554		Download File
16.2.RegAsm.exe.5870000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.2.PO-INV 21460041492040401.PDF.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1141554		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/ProductDataSet1.xsd#CustomerDataTableuThe	0%	Avira URL Cloud	safe	
http://tempuri.org/login2DataSet.xsd	0%	Avira URL Cloud	safe	
http://ns.adobe.c/gz	0%	Avira URL Cloud	safe	
http://tempuri.org/PendingProList.xsd	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/ProductDataSet.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/ProductDataSet1.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	172.217.168.36	true	false		high

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
79.134.225.7	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483625
Start date:	15.09.2021
Start time:	10:18:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-INV 21460041492040401.PDF.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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/12@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.7%) • Quality average: 54.4% • Quality standard deviation: 41.4%
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
10:20:13	API Interceptor	220x Sleep call for process: PO-INV 21460041492040401.PDF.exe modified
10:20:53	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegAsm.exe" s>$(Arg0)
10:20:53	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
10:20:53	API Interceptor	604x Sleep call for process: RegAsm.exe modified
10:20:53	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o..... .*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!...,..{T.....{U.....o"....+(.ra..p.o!...,..{T.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-INV 21460041492040401.PDF.exe.log	
Process:	C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	5.343667025898124
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csXE4D8Q:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHe
MD5:	379135DE3C31F3A766187BD9B6C730C9
SHA1:	BEFFE8BDE231861A3FD901A12F51523399B9A5E7
SHA-256:	BDE88F5C7F95E26FFC5EBE86C38AE61E78E0A5AA932A83DE00F2A46DB24DD22D
SHA-512:	2897AAB0225823AC258D5D5E52B43140F2B47603689C968243F515B516A2712CAC69A0D7317C53575CF725D7EBDC85C93637F57E626778117364D5666C9FB993
Malicious:	**true**
Reputation:	unknown
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\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070I
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o.....*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!...,..{T.....{U.....o"....+(.ra..p.o!...,..{T.....

C:\Users\user\AppData\Local\Temp\tmpD621.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.0974407842325995
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK04a5xtn:cbk4oL600QydbQxIYODOLedq35a5j
MD5:	5B2692CD41D7623477AF0906E03FCA7F
SHA1:	BDDB88619AF2FE9DA471194DD23C704FC20B53DB
SHA-256:	86976A03D4B50E7DA1773A36320C0BFDFDE01BA5CC6FF707D582FAFB9B209069
SHA-512:	E6949C9801E4C154B87E2C8C3DFA60A0C0AE7428DD1648883777708E6B894B627B37068A8B99FDE8C56A73F2DA526515F42661E415D8FC91677131A0580DB0892
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpDAD5.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C

C:\Users\user\AppData\Local\Temp\tmpDAD5.tmp	
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mtn:mtn
MD5:	1D178B2ECC232213B75A22978BE18A54
SHA1:	24A6B1258B916618F759627255FF34D58E0A94AA
SHA-256:	1B4300C16CFE2B76F2C9411DE9D112A808E67CFADC8941C72891309E68F62026
SHA-512:	740812A65BDD7679C748CEA8893C2CFB7D6E0A2DA758E7009313F9CCDFCDB4F129CD475DD794043F89638CB5492190DE78F64B6087DE6A0452745B6DE7C94B
Malicious:	**true**
Reputation:	unknown
Preview:	8.S*mx.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.250201918975736
Encrypted:	false
SSDEEP:	3:oNUkh4E2J5xAI0L4A:oN923f0L4A
MD5:	5E4571028368101EFC20DC157BA8FFAF
SHA1:	2365FD6D5C6178F421641578F1A3E77A3A41C3B8
SHA-256:	185C43C8D367C0CD55C84BA1630CDC7F901233E4F74411E8FCAECDB6D444AC99
SHA-512:	03424D2A44695F04CF7F470B1EBCB3D84DCD3E42BAF2F25712144AEFA31C60A32104ED0D923F4ECE698EF16EC25A1C20C4CAD802F54AFA5CFA408DA67BDC396
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\RegAsm.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.2989523990568035
Encrypted:	false
SSDEEP:	24:z3U3g4DO/0XZd3Wo3opQ5ZKBQFYVgt7ovrNOYlK:zEw4DBXZxo4ABV+SrUYE
MD5:	970EE6AEAB63008333D1D883327DA660
SHA1:	A71E19F66886B1888A183BA1777A23FABAE9822E
SHA-256:	D270D397EB3CF1173D25795834B240466EFEE213E11B1B31CDC101015AFFCAD9
SHA-512:	EB49AEE1B4524E6F15C08345A380D7D28DC845DEBA5408A7D034F2F7F5A652C8A2E2FF293BFB307DE87DCC2FAA111BA3BE8BEF9C4752A73DE1835DCD844D3BB
Malicious:	false
Reputation:	unknown

\Device\ConDrv	
Preview:	Microsoft .NET Framework Assembly Registration Utility version 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Syntax: RegAsm AssemblyName [Options]..Options:.. /unregister Unregister types.. /tlb[:FileName] Export the assembly to the specified type library.. and register it.. /regfile[:FileName] Generate a reg file with the specified name.. instead of registering the types. This option.. cannot be used with the /u or /tlb options.. /codebase Set the code base in the registry.. /registered Only refer to already regist ered type libraries.. /asmpath:Directory Look for assembly references here.. /nologo Prevents RegAsm from displaying logo.. /silent Silent mode. Prevents displaying of success messages.. /verbose Displays extra information..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	6.277873760598072
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:	PO-INV 21460041492040401.PDF.exe
File size:	961024
MD5:	8e23941e7d2bd97f91b83aa52ce9d2ee
SHA1:	afd72705c4b572aa33e7e14938b25e02160f8964
SHA256:	3c3a536252b1c720434579c37748f0ba4178e7eedea1d8 41aa05e772118185b7
SHA512:	cd7ef30f0b17652f0988695009c297794ee16c12f7a564c cf6bb9bfa194236f335cd094beb69bb3405182c01e609e1 00efa1ccb27de2d48be05edc987f62ebee
SSDEEP:	24576:fhlBqZAwq3AhuQT4Tx/rlOxO8OvOgOtOAOBI7g Uwjyo7g/OZR59Y8LGSpeXIvC8R:9q2p6T4Tx/
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L... T.#..... .....@.. ....`.....

File Icon

Icon Hash:	149c9a581a2ea61a

Static PE Info

General

Entrypoint:	0x4ab6fe
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:	0x1E23CE54 [Thu Jan 9 13:57:40 1986 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	0xa9704	0xa9800	False	0.598245356287	data	6.69959737535	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x40c80	0x40e00	False	0.124909682081	data	3.12625118346	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	0xc	0x200	False	0.041015625	data	0.0815394123432	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
Sep 15, 2021 10:19:58.029768944 CEST	192.168.2.5	8.8.8.8	0xa2eb	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
Sep 15, 2021 10:19:58.059954882 CEST	8.8.8.8	192.168.2.5	0xa2eb	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49728	172.217.168.36	443	C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	0	OUT	GET / HTTP/1.1 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 08:19:58 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+570; 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
2021-09-15 08:19:58 UTC	0	IN	Data Raw: 35 33 39 31 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 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 Data Ascii: 5391<!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 content="/images/branding/googleg/1x/goog leg_standard_color_128dp.png" itemprop="image
2021-09-15 08:19:58 UTC	1	IN	Data Raw: 35 31 34 2c 36 30 36 2c 32 30 32 35 2c 32 32 39 35 2c 36 33 34 35 2c 38 33 32 35 2c 33 32 32 37 2c 32 38 34 35 2c 37 2c 31 32 33 35 34 2c 35 30 39 36 2c 37 35 33 39 2c 38 37 38 31 2c 39 30 38 2c 32 2c 37 33 33 39 2c 39 33 35 38 2c 33 2c 33 34 36 2c 32 33 30 2c 31 30 31 34 2c 31 2c 35 34 34 34 2c 31 34 39 2c 31 31 33 32 33 2c 32 36 35 32 2c 34 2c 31 35 32 38 2c 32 33 30 34 2c 31 32 33 36 2c 35 38 30 33 2c 37 34 2c 31 39 38 33 2c 32 36 32 36 2c 32 30 34 2c 31 38 31 31 2c 31 38 33 37 35 2c 32 36 35 38 2c 34 32 34 33 2c 33 31 31 32 2c 33 32 2c 31 33 36 32 38 2c 32 33 30 35 2c 36 33 38 2c 31 34 39 34 2c 35 35 38 36 2c 31 31 32 30 30 2c 35 37 38 38 2c 32 35 36 39 2c 34 30 39 34 2c 33 31 33 38 2c 36 2c 39 30 38 2c 33 2c 33 35 34 31 2c 31 2c 31 34 37 31 30 2c 31 Data Ascii: 514,606,2025,2295,6345,8325,3227,2845,7,12354,5096,7539,8781,908,2,7339,9358,3,346,230,1014,1,5444 ,149,11323,2652,4,1528,2304,1236,5803,74,1983,2626,204,1811,18375,2658,4243,3112,32,13628,2305,638,1494,5586,1 1200,5788,2569,4094,3138,6,908,3,3541,1,14710,1
2021-09-15 08:19:58 UTC	2	IN	Data Raw: 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 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 20 65 3d 22 22 3b 63 7c 7c 2d 31 21 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 65 69 3d 22 29 7c 7c 28 65 3d 22 26 65 69 3d 22 2b 6c 28 64 29 2c 2d 31 3d 3d 3d 62 2e 73 65 61 72 63 68 28 22 26 6c 65 69 3d 22 29 26 26 28 64 3d 6d 28 64 29 29 26 26 28 65 2b 3d 22 26 6c 65 69 3d 22 2b 64 29 29 3b 64 3d 22 22 3b 21 63 26 26 66 2e 5f 63 73 68 69 64 26 26 2d 31 3d 3d 3d 62 2e 73 65 61 72 63 Data Ascii: ction 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 e="";c||-1!==b.search("&ei=")||(e="&ei="+l(d),-1===b.search("&lei=")&&(d=m(d))&&(e+="&lei="+d));d="";!c&&f._cshid&&-1===b.searc
2021-09-15 08:19:58 UTC	3	IN	Data Raw: 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 29 29 7d 2c 21 30 29 3b 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 63 6c 69 63 6b 22 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 61 3b 61 3a 7b 66 6f 72 28 61 3d 62 2e 74 61 72 67 65 74 3b 61 26 26 61 21 3d 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 3b 61 3d Data Ascii: Attribute("data-submitfalse");a="1"===c||"q"===c&&!a.elements.q.value?!0:!1}else a=!1;a&&(b.preventDefault() ,b.stopPropagation())},!0);document.documentElement.addEventListener("click",function(b){var a;a:{for(a=b.target;a&&a!== document.documentElement;a=
2021-09-15 08:19:58 UTC	5	IN	Data Raw: 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 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 2c 30 2c 30 2c 2e 32 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 34 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 72 74 6c 20 2e 67 62 6d 7b 2d 6d 6f 7a 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 31 70 78 20 31 70 78 20 31 70 78 20 72 67 Data Ascii: 99;top:-999px;visibility:hidden;text-align:left;border:1px solid #bebebe;background:#fff;-moz-box-shadow:-1px 1px 1px rgba(0,0,0,.2);-webkit-box-shadow:0 2px 4px rgba(0,0,0,.2);box-shadow:0 2px 4px rgba(0,0,0,.2)}.gbrtl .gbm{-mo z-box-shadow:1px 1px 1px rg
2021-09-15 08:19:58 UTC	6	IN	Data Raw: 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 2c 30 2c 30 2c 2e 32 29 7d 2e 67 62 7a 74 2c 2e 67 62 67 74 7b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 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 73 70 61 6e 23 67 62 67 36 2c 73 70 61 6e 23 67 62 67 34 7b 63 75 72 73 6f 72 3a 64 65 66 61 75 6c 74 7d 2e 67 62 74 73 7b 62 6f 72 64 65 Data Ascii: y: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(0,0,0,.2)}.gbzt,.gbgt{cursor:pointer;display:block;text-decoration:none !important}span#gbg6,span#gbg4 {cursor:default}.gbts{borde

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	7	IN	Data Raw: 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 65 3a 6e 6f 6e 65 7d 2e 67 62 67 34 61 7b 66 6f 6e 74 2d 73 69 7a 65 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 30 7d 2e 67 62 67 34 61 20 2e 67 62 74 73 7b 70 61 64 64 69 6e 67 3a 32 37 70 78 20 35 70 78 20 30 3b 2a 70 61 64 64 69 6e 67 3a 32 35 70 78 20 35 70 78 20 30 7d 2e 67 62 74 6f 20 2e 67 62 67 34 61 20 2e 67 62 74 73 7b 70 61 64 64 69 6e 67 3a 32 39 70 78 20 35 70 78 20 Data Ascii: :#dd4b39!important}#gbi4s,#gbi4s1{font-weight:bold}#gbg6.gbgt-hvr,#gbg6.gbgt:focus{background-color:transparent;background-image:none}.gbg4a{font-size:0;line-height:0}.gbg4a .gbts{padding:27px 5px 0;*padding:25px 5px 0}.gbto .gbg4a .gbts{padding:29px 5px
2021-09-15 08:19:58 UTC	8	IN	Data Raw: 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 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 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 67 62 6d 6c 31 2c 2e 67 62 6d 6c 31 3a 76 69 73 69 74 65 64 7b 70 61 64 64 69 6e 67 3a 30 20 31 30 70 78 7d 2e 67 62 6d 6c 31 2d 68 76 72 2c 2e 67 62 6d 6c 31 3a 66 6f 63 75 73 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 Data Ascii: mportant}.gbmt,.gbmt:visited{display:block}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{display:inline-block;margin:0 10px}.gbml1,.gbmlb,.gbml1:visited,.gbmlb:visited{*display:inline}.gbml1,.gbml1:visited{padding:0 10px}.gbml1-hvr,.gbml1:focus{outline:none
2021-09-15 08:19:58 UTC	10	IN	Data Raw: 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 69 64 20 23 62 65 62 65 62 65 7d 23 67 62 64 34 20 2e 67 62 70 63 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 31 36 70 78 20 30 20 31 30 70 78 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 35 30 70 78 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 23 67 62 64 34 20 2e 67 62 70 63 7b 2a 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 Data Ascii: bmps{*zoom:1}#gbd4 .gbpc,#gbmpas .gbmt{line-height:17px}#gbd4 .gbpgs .gbmtc{line-height:27px}#gbd4 .gbmtc{border-bottom:1px solid #bebebe}#gbd4 .gbpc{display:inline-block;margin:16px 0 10px;padding-right:50px;vertical-align:top}#gbd4 .gbpc{*display:inline
2021-09-15 08:19:58 UTC	11	IN	Data Raw: 69 61 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 36 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 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 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 7d 2e 67 62 6d 70 69 61 61 72 3a 6e 6f 6e 65 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 34 38 70 78 3b 77 69 64 74 68 3a 34 38 70 78 7d 2e 67 62 6d 70 6e 77 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 3b 76 65 Data Ascii: iaw{display:inline-block;padding-right:10px;margin-bottom:6px;margin-top:10px}.gbxv{visibility:hidden}.gbmpiaa{display:block;margin-top:10px}.gbmpia{border:none;display:block;height:48px;width:48px}.gbmpnw{display:inline-block;height:auto;margin:10px 0;ve
2021-09-15 08:19:58 UTC	12	IN	Data Raw: 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 7b 62 6f 72 64 65 72 3a 30 7d 2e 67 62 71 66 62 61 2c 2e 67 62 71 66 62 62 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 63 64 63 64 63 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 3b 63 6f 6c 6f 72 3a 23 34 34 34 20 21 69 6d 70 6f 72 74 61 6e 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 7d 2e 67 62 71 66 62 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f Data Ascii: ,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:0}.gbqfba,.gbqfbb{border:1px solid #dcdcdc;border-color:rgba(0,0,0,.1);color:#444 !important;font-size:11px}.gbqfb{background-co
2021-09-15 08:19:58 UTC	14	IN	Data Raw: 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 28 30 2c 20 30 2c 20 30 2c 20 30 2e 33 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 20 30 2c 20 30 2c 20 30 2e 33 29 7d 2e 67 62 71 66 62 61 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 66 35 66 35 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 Data Ascii: bqfb: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(0, 0, 0, 0.3);box-shadow:inset 0 1px 2px rgba(0, 0, 0, 0.3)}.gbqfba{background-color:#f5f5f5;background-image:-webkit-gradient(
2021-09-15 08:19:58 UTC	15	IN	Data Raw: 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 6c 65 66 74 2c 62 6f 74 74 6f 6d 2c 66 72 6f 6d 28 23 66 66 66 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 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 66 66 2c 23 66 62 66 62 66 62 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 70 2c 23 66 66 66 Data Ascii: top,left bottom,from(#fff),to(#fbfbfb));background-image:-webkit-linear-gradient(top,#fff,#fbfbfb);background-image:-moz-linear-gradient(top,#fff,#fbfbfb);background-image:-ms-linear-gradient(top,#fff,#fbfbfb);background-image:-o-linear-gradient(top,#fff
2021-09-15 08:19:58 UTC	16	IN	Data Raw: 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 74 69 76 65 3b 2a 7a 6f 6f 6d 3a 31 7d 2e 67 62 73 62 63 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 7d 2e 67 62 73 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 Data Ascii: rgba(0,0,0,.1)}#gbmpas{max-height:220px}#gbmm{max-height:530px}.gbsb{-webkit-box-sizing:border-box;display:block;position:relative;*zoom:1}.gbsbic{overflow:auto}.gbsbis .gbsbt,.gbsbis .gbsbb{-webkit-mask-box-image:-webkit-gradient(linear,left top,right t

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	17	IN	Data Raw: 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 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 6f 7a 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 30 2c 2e 32 29 2c 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6d 73 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 Data Ascii: ,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));background-image:-moz-linear-gradient(bottom,rgba(0,0,0,.2),rgba(0,0,0,0));background-image:-ms-linear-gradient(bottom,rgba(0,0,0,.2),rg
2021-09-15 08:19:58 UTC	19	IN	Data Raw: 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 74 2d 78 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 68 65 69 67 68 74 3a 33 30 70 78 3b 6d 61 72 67 69 6e 3a 30 3b 6f 75 74 6c 69 6e 65 3a 30 3b 66 6f 6e 74 3a 31 35 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 6f 70 7d 2e 6c 73 62 3a 61 63 74 69 Data Ascii: px}.lsbb{display:block}#WqQANb a{display:inline-block;margin:0 12px}.lsb{background:url(/images/nav_logo229.png) 0 -261px repeat-x;border:none;color:#000;cursor:pointer;height:30px;margin:0;outline:0;font:15px arial,sans-serif;vertical-align:top}.lsb:acti
2021-09-15 08:19:58 UTC	20	IN	Data Raw: 32 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 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 65 3d 74 68 69 73 7c 7c 73 65 6c 66 3b 76 61 72 20 61 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 64 3d 64 7c 7c 7b 7d 3b 64 2e 5f 73 6e 3d 5b 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 Data Ascii: 2);p=null;l&&n>=k&&(window.onerror=null)};})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var e=this||self;var aa=function(a,b,c,d){d=d||{};d._sn=["cfg",b,c].join(".");window.gbar.logger.ml(a,d)};va
2021-09-15 08:19:58 UTC	21	IN	Data Raw: 31 31 31 0d 0a 2c 6e 61 3d 68 2e 61 28 22 31 22 2c 21 30 29 2c 6f 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 77 2e 70 75 73 68 28 5b 61 2c 62 5d 29 7d 2c 70 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 5b 61 5d 3d 62 7d 2c 71 61 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 20 69 6e 20 76 7d 2c 78 3d 7b 7d 2c 41 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 78 5b 61 5d 3d 5b 5d 29 3b 78 5b 61 5d 2e 70 75 73 68 28 62 29 7d 2c 42 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 41 28 22 6d 22 2c 61 29 7d 2c 72 61 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 63 2e 73 72 63 3d 61 3b 63 2e 61 73 79 6e 63 3d Data Ascii: 111,na=h.a("1",!0),oa=function(a,b){w.push([a,b])},pa=function(a,b){v[a]=b},qa=function(a){return a in v},x={},A=function(a,b){x[a]||(x[a]=[]);x[a].push(b)},B=function(a){A("m",a)},ra=function(a,b){var c=document.createElement("script");c.src=a;c.async=
2021-09-15 08:19:58 UTC	21	IN	Data Raw: 36 61 63 38 0d 0a 2e 6f 6e 65 72 72 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 63 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 3b 74 28 45 72 72 6f 72 28 22 42 75 6e 64 6c 65 20 6c 6f 61 64 20 66 61 69 6c 65 64 3a 20 6e 61 6d 65 3d 22 2b 28 28 62 7c 7c 22 55 4e 4b 22 29 2b 22 20 75 72 6c 3d 22 2b 61 29 29 7d 29 3b 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 78 6a 73 63 22 29 7c 7c 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 7c 7c 0a 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 29 7d 2c 44 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 66 6f 72 28 Data Ascii: 6ac8.onerror=function(){c.onerror=null;t(Error("Bundle load failed: name="+(b||"UNK")+" url="+a))});(document.getElementById("xjsc")||document.getElementsByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(c)},D=function(a){for(
2021-09-15 08:19:58 UTC	23	IN	Data Raw: 2e 67 61 70 69 2e 65 6e 2e 37 52 70 68 74 4e 63 47 48 44 51 2e 4f 2f 64 3d 31 2f 72 73 3d 41 48 70 4f 6f 6f 5f 2d 7a 6d 59 68 70 5f 49 72 37 5f 43 43 78 4d 33 6c 2d 41 63 6b 4d 76 61 49 39 41 2f 6d 3d 5f 5f 66 65 61 74 75 72 65 73 5f 5f 22 29 3b 47 2e 6d 73 3d 46 28 47 2e 6d 73 2c 22 68 74 74 70 73 3a 2f 2f 61 70 69 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 29 3b 47 2e 6d 3d 46 28 47 2e 6d 2c 22 22 29 3b 47 2e 6c 3d 46 28 47 2e 6c 2c 5b 5d 29 3b 47 2e 64 70 6f 3d 46 28 47 2e 64 70 6f 2c 22 22 29 3b 78 61 7c 7c 77 2e 70 75 73 68 28 5b 22 67 6c 22 2c 7b 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 6c 6d 5f 65 37 62 62 33 39 61 37 65 31 61 32 34 35 38 31 66 66 34 66 38 64 31 39 39 36 37 38 62 31 62 39 2e Data Ascii: .gapi.en.7RphtNcGHDQ.O/d=1/rs=AHpOoo_-zmYhp_Ir7_CCxM3l-AckMvaI9A/m=__features__");G.ms=F(G.ms,"https://apis.google.com");G.m=F(G.m,"");G.l=F(G.l,[]);G.dpo=F(G.dpo,"");xa||w.push(["gl",{url:"//ssl.gstatic.com/gb/js/abc/glm_e7bb39a7e1a24581ff4f8d199678b1b9.
2021-09-15 08:19:58 UTC	24	IN	Data Raw: 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 48 28 61 2c 62 29 7c 7c 28 61 2e 63 6c 61 73 73 4e 61 6d 65 2b 3d 28 22 22 21 3d 63 3f 22 20 22 3a 22 22 29 2b 62 29 7d 2c 4b 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 73 3f 5c 5c 62 22 2b 62 2b 22 5c 5c 62 22 29 3b 63 26 26 63 2e 6d 61 74 63 68 28 62 29 26 26 28 61 2e 63 6c 61 73 73 4e 61 6d 65 3d 63 2e 72 65 70 6c 61 63 65 28 62 2c 22 22 29 29 7d 2c 48 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 5c 5c 73 3f 5c 5c 62 22 2b 62 2b 22 5c 5c 62 22 29 3b 61 3d 61 2e 63 6c 61 73 73 4e 61 6d 65 3b 72 65 74 75 72 6e 21 28 21 61 7c 7c 21 Data Ascii: nction(a,b){var c=a.className;H(a,b)||(a.className+=(""!=c?" ":"")+b)},K=function(a,b){var c=a.className;b=new RegExp("\\s?\\b"+b+"\\b");c&&c.match(b)&&(a.className=c.replace(b,""))},H=function(a,b){b=new RegExp("\\b"+b+"\\b");a=a.className;return!(!a||!a
2021-09-15 08:19:58 UTC	25	IN	Data Raw: 6c 65 6e 67 74 68 3f 61 5b 30 5d 3a 6e 75 6c 6c 7d 2c 57 61 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 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 37 30 22 29 7d 2c 4c 3d 7b 7d 2c 4d 3d 7b 7d 2c 58 61 3d 7b 7d 2c 4e 3d 7b 7d 2c 4f 3d 76 6f 69 64 20 30 2c 62 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 72 79 7b 76 61 72 20 63 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 3b 4a 28 63 2c 22 67 62 70 64 6a 73 22 29 3b 50 28 29 3b 59 61 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 67 62 22 29 29 26 26 4a 28 63 2c 22 67 62 72 74 6c 22 29 3b 69 66 28 62 26 26 62 2e 67 65 74 41 74 74 72 69 62 75 74 65 29 7b 76 61 72 20 64 3d 62 Data Ascii: length?a[0]:null},Wa=function(){return document.getElementById("gb_70")},L={},M={},Xa={},N={},O=void 0,bb=function(a,b){try{var c=document.getElementById("gb");J(c,"gbpdjs");P();Ya(document.getElementById("gb"))&&J(c,"gbrtl");if(b&&b.getAttribute){var d=b

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>26</td><td>IN</td><td>Data Raw: 6f 72 28 3b 64 3c 6e 26 26 48 28 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 5d 2c 49 29 3b 29 64 2b 2b 3b 69 66 28 49 3d 3d 62 29 7b 6b 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 6d 2c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 5d 7c 7c 0a 6e 75 6c 6c 29 3b 66 3d 21 30 3b 62 72 65 61 6b 7d 7d 69 66 28 66 29 7b 69 66 28 64 2b 31 3c 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 56 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2b 31 5d 3b 48 28 56 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d 68 22 29 7c 7c 65 62 28 56 2c 45 29 7c 7c 28 6c 3d 64 2b 31 29 7d 65 6c 73 65 20 69 66 28 30 3c 3d 64 2d 31 29 7b 76 61 72 20 57 3d 6b 2e 63 68 69 6c 64 4e 6f 64 65 73 5b 64 2d 31 5d 3b 48 28 57 2e 66 69 72 73 74 43 68 69 6c 64 2c 22 67 62 6d
Data Ascii: or(;d<n&&H(k.childNodes[d],I);)d++;if(I==b){k.insertBefore(m,k.childNodes[d]||null);f=!0;break}}if(f){if(d+1<k.childNodes.length){var V=k.childNodes[d+1];H(V.firstChild,"gbmh")||eb(V,E)||(l=d+1)}else if(0<=d-1){var W=k.childNodes[d-1];H(W.firstChild,"gbm</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>28</td><td>IN</td><td>Data Raw: 29 29 7d 2c 72 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 74 72 79 7b 50 28 29 3b 76 61 72 20 62 3d 61 7c 7c 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 62 26 26 28 71 62 28 62 2c 22 54 68 69 73 20 73 65 72 76 69 63 65 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 25 31 24 73 50 6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20 6c 61 74 65 72 2e 22 2c 22 25 31 24 73 22 29 2c 51 28 62 2c 21 30 29 29 7d 63 61 74 63 68 28 63 29 7b 72 28 63 2c 22 73 62 22 2c 22 73 64 68 65 22 29 7d 7d 2c 71 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 61 26 26 62 29 7b 76 61 72 20 64 3d 5a 61 28 61 29 3b 69 66 28 64 29 7b 69 66 28 63 29 7b 64 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 22 22 3b 62
Data Ascii:))},rb=function(a){try{P();var b=a||document.getElementById(O);b&&(qb(b,"This service is currently unavailable.%1$sPlease try again later.","%1$s"),Q(b,!0))}catch(c){r(c,"sb","sdhe")}},qb=function(a,b,c){if(a&&b){var d=Za(a);if(d){if(c){d.textContent="";b</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>29</td><td>IN</td><td>Data Raw: 78 62 3d 7b 74 69 77 3a 68 2e 63 28 22 31 35 30 30 30 22 2c 30 29 2c 74 69 65 3a 68 2e 63 28 22 33 30 30 30 30 22 2c 30 29 7d 3b 76 2e 77 67 3d 78 62 3b 76 61 72 20 79 62 3d 7b 74 68 69 3a 68 2e 63 28 22 31 30 30 30 30 22 2c 30 29 2c 74 68 70 3a 68 2e 63 28 22 31 38 30 30 30 30 22 2c 30 29 2c 74 68 6f 3a 68 2e 63 28 22 35 30 30 30 22 2c 30 29 2c 74 65 74 3a 68 2e 62 28 22 30 2e 35 22 2c 30 29 7d 3b 76 2e 77 6d 3d 79 62 3b 69 66 28 68 2e 61 28 22 31 22 29 29 7b 76 61 72 20 7a 62 3d 68 2e 61 28 22 22 29 3b 77 2e 70 75 73 68 28 5b 22 67 63 22 2c 7b 61 75 74 6f 3a 7a 62 2c 75 72 6c 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 67 62 2f 6a 73 2f 61 62 63 2f 67 63 69 5f 39 31 66 33 30 37 35 35 64 36 61 36 62 37 38 37 64 63 63 32 61 34 30 36 32 65
Data Ascii: xb={tiw:h.c("15000",0),tie:h.c("30000",0)};v.wg=xb;var yb={thi:h.c("10000",0),thp:h.c("180000",0),tho:h.c("5000",0),tet:h.b("0.5",0)};v.wm=yb;if(h.a("1")){var zb=h.a("");w.push(["gc",{auto:zb,url:"//ssl.gstatic.com/gb/js/abc/gci_91f30755d6a6b787dcc2a4062e</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>30</td><td>IN</td><td>Data Raw: 7b 76 61 72 20 4f 62 3d 4d 61 74 68 2e 72 61 6e 64 6f 6d 28 29 3b 4f 62 3c 4b 62 26 26 28 4d 62 3d 21 30 29 3b 4f 62 3c 4c 62 26 26 28 4e 62 3d 21 30 29 7d 76 61 72 20 52 3d 6e 75 6c 6c 3b 0a 66 75 6e 63 74 69 6f 6e 20 50 62 28 61 2c 62 29 7b 76 61 72 20 63 3d 4b 62 2c 64 3d 4d 62 3b 76 61 72 20 66 3d 61 3b 69 66 28 21 52 29 7b 52 3d 7b 7d 3b 66 6f 72 28 76 61 72 20 6b 3d 30 3b 6b 3c 4a 62 2e 6c 65 6e 67 74 68 3b 6b 2b 2b 29 7b 76 61 72 20 6d 3d 4a 62 5b 6b 5d 3b 52 5b 6d 5d 3d 21 30 7d 7d 69 66 28 66 3d 21 21 52 5b 66 5d 29 63 3d 4c 62 2c 64 3d 4e 62 3b 69 66 28 64 29 7b 64 3d 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 3b 69 66 28 67 2e 72 70 29 7b 76 61 72 20 6e 3d 67 2e 72 70 28 29 3b 6e 3d 22 2d 31 22 21 3d 6e 3f 6e 3a 22 22 7d 65 6c 73 65
Data Ascii: {var Ob=Math.random();Ob<Kb&&(Mb=!0);Ob<Lb&&(Nb=!0)}var R=null;function Pb(a,b){var c=Kb,d=Mb;var f=a;if(!R){R={};for(var k=0;k<Jb.length;k++){var m=Jb[k];R[m]=!0}}if(f=!!R[f])c=Lb,d=Nb;if(d){d=encodeURIComponent;if(g.rp){var n=g.rp();n="-1"!=n?n:""}else</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>32</td><td>IN</td><td>Data Raw: 37 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 2c 22 32 37 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 2c 22 32 37 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77 2f 64 65 66 61 75 6c 74 2d 75 73 65 72 3d 73 32 34 22 7d 2c 59 62 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 28 61 3d 58 62 5b 61 5d 29 7c 7c 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 6f 67 77
Data Ascii: 7":"https://lh3.googleusercontent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/ogw/default-user=s24","27":"https://lh3.googleusercontent.com/ogw/default-user=s24"},Yb=function(a){return(a=Xb[a])||"https://lh3.googleusercontent.com/ogw</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>33</td><td>IN</td><td>Data Raw: 6f 6e 28 29 7b 74 72 79 7b 69 66 28 58 3d 32 2c 21 62 63 29 7b 62 63 3d 21 30 3b 66 6f 72 28 76 61 72 20 61 20 69 6e 20 53 29 66 6f 72 28 76 61 72 20 62 3d 53 5b 61 5d 2c 63 3d 30 3b 63 3c 62 2e 6c 65 6e 67 74 68 3b 63 2b 2b 29 74 72 79 7b 62 5b 63 5d 28 64 63 28 61 29 29 7d 63 61 74 63 68 28 64 29 7b 72 28 64 2c 22 75 70 22 2c 22 74 70 22 29 7d 7d 7d 63 61 74 63 68 28 64 29 7b 72 28 64 2c 22 75 70 22 2c 22 6d 74 70 22 29 7d 7d 2c 64 63 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 59 28 5b 32 5d 2c 22 73 73 70 22 29 29 7b 76 61 72 20 62 3d 21 61 63 5b 61 5d 3b 54 26 26 28 62 3d 62 26 26 21 21 54 5b 61 5d 29 3b 72 65 74 75 72 6e 20 62 7d 7d 3b 62 63 3d 21 31 3b 53 3d 7b 7d 3b 61 63 3d 7b 7d 3b 54 3d 6e 75 6c 6c 3b 58 3d 31 3b 0a 76 61 72 20 69 63 3d 66
Data Ascii: on(){try{if(X=2,!bc){bc=!0;for(var a in S)for(var b=S[a],c=0;c<b.length;c++)try{b[c](dc(a))}catch(d){r(d,"up","tp")}}}catch(d){r(d,"up","mtp")}},dc=function(a){if(Y([2],"ssp")){var b=!ac[a];T&&(b=b&&!!T[a]);return b}};bc=!1;S={};ac={};T=null;X=1;var ic=f</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>34</td><td>IN</td><td>Data Raw: 28 64 5b 31 5d 2c 31 30 29 7d 7d 63 61 74 63 68 28 66 29 7b 66 2e 63 6f 64 65 21 3d 44 4f 4d 45 78 63 65 70 74 69 6f 6e 2e 51 55 4f 54 41 5f 45 58 43 45 45 44 45 44 5f 45 52 52 26 26 72 28 66 2c 22 75 70 22 2c 22 67 63 63 22 29 7d 72 65 74 75 72 6e 2d 31 7d 3b 70 28 22 75 70 22 2c 7b 72 3a 65 63 2c 6e 61 70 3a 66 63 2c 61 6f 70 3a 67 63 2c 74 70 3a 68 63 2c 73 73 70 3a 64 63 2c 73 70 64 3a 6c 63 2c 67 70 64 3a 6d 63 2c 61 65 68 3a 6e 63 2c 61 61 6c 3a 6f 63 2c 67 63 63 3a 70 63 7d 29 3b 76 61 72 20 5a 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 5b 62 5d 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 72 67 75 6d 65 6e 74 73 3b 67 2e 71 6d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 5b 62 5d 2e 61 70 70 6c 79 28 74 68 69 73 2c 64 29 7d 29 7d 7d
Data Ascii: (d[1],10)}}catch(f){f.code!=DOMException.QUOTA_EXCEEDED_ERR&&r(f,"up","gcc")}return-1};p("up",{r:ec,nap:fc,aop:gc,tp:hc,ssp:dc,spd:lc,gpd:mc,aeh:nc,aal:oc,gcc:pc});var Z=function(a,b){a[b]=function(c){var d=arguments;g.qm(function(){a[b].apply(this,d)})}}</td></tr>
<tr><td>2021-09-15 08:19:58 UTC</td><td>35</td><td>IN</td><td>Data Raw: 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 2e 6d 6c 28 65 2c 7b 22 5f 73 6e 22 3a 22 63 66 67 2e 69 6e 69 74 22 7d 29 3b 7d 7d 29 28 29 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 72 79 7b 2f 2a 0a 0a 20 43 6f 70 79 72 69 67 68 74 20 54 68 65 20 43 6c 6f 73 75 72 65 20 4c 69 62 72 61 72 79 20 41 75 74 68 6f 72 73 2e 0a 20 53 50 44 58 2d 4c 69 63 65 6e 73 65 2d 49 64 65 6e 74 69 66 69 65 72 3a 20 41 70 61 63 68 65 2d 32 2e 30 0a 2a 2f 0a 76 61 72 20 61 3d 77 69 6e 64 6f 77 2e 67 62 61 72 3b 61 2e 6d 63 66 28 22 6d 6d 22 2c 7b 73 3a 22 31 22 7d 29 3b 7d 63 61 74 63 68 28 65 29 7b 77 69 6e 64 6f 77 2e 67 62 61 72 26 26 67 62 61 72 2e 6c 6f 67 67 65 72 26 26 67 62
Data Ascii: catch(e){window.gbar&&gbar.logger&&gbar.logger.ml(e,{"_sn":"cfg.init"});}})();(function(){try{/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0*/var a=window.gbar;a.mcf("mm",{s:"1"});}catch(e){window.gbar&&gbar.logger&&gb</td></tr>
</table>

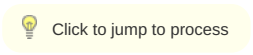
Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	37	IN	Data Raw: 76 61 72 20 64 3d 63 2e 61 2c 65 3d 63 2e 63 2c 66 3d 7b 63 74 79 3a 22 47 42 52 22 2c 63 76 3a 22 33 39 35 33 37 32 39 35 34 22 2c 64 62 67 3a 64 28 22 22 29 2c 65 63 76 3a 22 30 22 2c 65 69 3a 65 28 22 72 71 78 42 59 5a 57 49 4a 76 6e 46 79 74 4d 50 77 62 69 33 73 41 49 22 29 2c 65 6c 65 3a 64 28 22 31 22 29 2c 65 73 72 3a 65 28 22 30 2e 31 22 29 2c 65 76 74 73 3a 5b 22 6d 6f 75 73 65 64 6f 77 6e 22 2c 22 74 6f 75 63 68 73 74 61 72 74 22 2c 22 74 6f 75 63 68 6d 6f 76 65 22 2c 22 77 68 65 65 6c 22 2c 22 6b 65 79 64 6f 77 6e 22 5d 2c 67 62 6c 3a 22 65 73 5f 70 6c 75 73 6f 6e 65 5f 67 63 5f 32 30 32 31 30 38 30 33 2e 30 5f 70 31 22 2c 68 64 3a 22 63 6f 6d 22 2c 68 6c 3a 22 65 6e 22 2c 69 72 70 3a 64 28 22 22 29 2c 70 69 64 3a 65 28 22 31 22 29 2c 0a 73 6e Data Ascii: var d=c.a,e=c.c,f={cty:"GBR",cv:"395372954",dbg:d(""),ecv:"0",ei:e("rqxBYZWIJvnFytMPwbi3sAI"),ele:d("1"),esr:e("0.1"),evts:["mousedown","touchstart","touchmove","wheel","keydown"],gbl:"es_plusone_gc_20210803.0_p1",hd:"com",hl:"en",irp:d(""),pid:e("1"),sn
2021-09-15 08:19:58 UTC	38	IN	Data Raw: 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 22 67 62 7a 74 20 67 62 7a 30 6c 20 67 62 70 31 22 20 69 64 3d 67 62 5f 31 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 77 65 62 68 70 3f 74 61 62 3d 77 77 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 53 65 61 72 63 68 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 74 3e 3c 61 20 63 6c 61 73 73 3d 67 62 7a 74 20 69 64 3d 67 62 5f 32 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 69 6d 67 68 70 3f 68 6c 3d 65 6e 26 74 61 62 3d 77 69 22 3e 3c 73 70 61 6e 20 63 6c 61 73 Data Ascii: <li class=gbt>Search <li class=gbt><span clas
2021-09-15 08:19:58 UTC	39	IN	Data Raw: 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 74 62 32 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 69 64 3d 67 62 7a 74 6d 73 20 63 6c 61 73 73 3d 22 67 62 74 73 20 67 62 74 73 61 22 3e 3c 73 70 61 6e 20 69 64 3d 67 62 7a 74 6d 73 31 3e 4d 6f 72 65 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 67 62 6d 61 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 43 33 79 6c 73 55 66 41 2b 4c 6f 77 6b 38 36 58 57 31 51 63 76 77 3d 3d 27 3e 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 67 62 7a 74 6d 27 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 63 6c 69 63 6b 27 2c 20 66 75 6e 63 74 69 6f 6e 20 63 6c 69 63 6b 48 61 6e 64 6c 65 72 28 29 20 7b 20 67 62 61 72 2e Data Ascii: >More<script nonce='C3ylsUfA+Lowk86XW1Qcvw==='>document.getElementById('gbztm').addEventListener('click', function clickHandler() { gbar.
2021-09-15 08:19:58 UTC	41	IN	Data Raw: 6f 63 75 6d 65 6e 74 2f 3f 75 73 70 3d 64 6f 63 73 5f 61 6c 63 22 3e 44 6f 63 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 62 6d 74 20 67 62 6d 68 22 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 61 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 69 6e 74 6c 2f 65 6e 2f 61 62 6f 75 74 2f 70 72 6f 64 75 63 74 73 3f 68 6c 3d 65 6e 26 73 6d 3d 31 26 74 62 3d 77 68 22 20 63 6c 61 73 73 3d 67 62 6d 74 3e 45 76 65 6e 20 6d 6f 72 65 20 26 72 61 71 75 6f 3b 3c 2f 61 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 27 43 33 79 6c 73 55 66 41 2b 4c 6f 77 6b 38 36 58 57 31 51 63 76 77 3d 3d 27 3e 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 Data Ascii: ocument/?usp=docs_alc">Docs <li class=gbmtc> <li class=gbmtc>Even more »<script nonce='C3ylsUfA+Lowk86XW1Qcvw==='>document.query
2021-09-15 08:19:58 UTC	42	IN	Data Raw: 6c 61 73 73 3d 67 62 6d 63 3e 3c 6f 6c 20 69 64 3d 67 62 6f 6d 20 63 6c 61 73 73 3d 67 62 6d 63 63 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 63 20 67 62 6d 74 63 22 3e 3c 61 20 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 2f 70 72 65 66 65 72 65 6e 63 65 73 3f 68 6c 3d 65 6e 22 3e 53 65 61 72 63 68 20 73 65 74 74 69 6e 67 73 3c 2f 61 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 67 62 6d 74 63 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 67 62 6d 74 20 67 62 6d 68 22 3e 3c 2f 64 69 76 3e 3c 2f 6c 69 3e 3c 6c 69 20 63 6c 61 73 73 3d 22 67 62 6b 70 20 67 62 6d 74 63 22 3e 3c 61 20 63 6c 61 73 73 3d 67 62 6d 74 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 2e 75 6b 2f 68 69 73 74 6f 72 79 2f 6f 70 74 6f 75 74 3f 68 Data Ascii: lass=gbmc><ol id=gbom class=gbmcc><li class="gbkc gbmtc">Search settings <li class=gbmtc> <li class="gbkp gbmtc"><a class=gbmt href="http://www.google.co.uk/history/optout?h
2021-09-15 08:19:58 UTC	43	IN	Data Raw: 70 61 6e 20 63 6c 61 73 73 3d 22 6c 73 62 62 22 3e 3c 69 6e 70 75 74 20 63 6c 61 73 73 3d 22 6c 73 62 22 20 76 61 6c 75 65 3d 22 47 6f 6f 67 6c 65 20 53 65 61 72 63 68 22 20 6e 61 6d 65 3d 22 62 74 6e 47 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 6c 73 62 22 20 69 64 3d 22 74 73 75 69 64 31 22 20 76 61 6c 75 65 3d 22 49 27 6d 20 46 65 65 6c 69 6e 67 20 4c 75 63 6b 79 22 20 6e 61 6d 65 3d 22 62 74 6e 49 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 43 33 79 6c 73 55 66 41 2b 4c 6f 77 6b 38 36 58 57 31 51 63 76 77 3d Data Ascii: pan class="lsbb"><input class="lsb" value="Google Search" name="btnG" type="submit"><input class="lsb" id="tsuid1" value="I'm Feeling Lucky" name="btnI" type="submit"><script nonce="C3ylsUfA+Lowk86XW1Qcvw=
2021-09-15 08:19:58 UTC	44	IN	Data Raw: 73 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 66 6f 72 6d 3e 3c 64 69 76 20 69 64 3d 22 67 61 63 5f 73 63 6f 6e 74 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 38 33 25 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 2e 35 65 6d 22 3e 3c 62 72 3e 3c 2f 64 69 76 3e 3c 73 70 61 6e 20 69 64 3d 22 66 6f 6f 74 65 72 22 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 70 74 22 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 31 39 70 78 20 61 75 74 6f 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 22 20 69 64 3d 22 57 71 51 41 4e 62 22 3e 3c 61 20 68 72 65 66 3d 22 2f 69 6e 74 6c 2f 65 6e 2f 61 64 73 2f 22 3e 41 64 76 65 72 74 69 73 69 6e 67 a0 50 72 6f 67 72 61 6d 6d 65 73 3c 2f 61 3e Data Ascii: s);</script></form> AdvertisingProgrammes
2021-09-15 08:19:58 UTC	46	IN	Data Raw: 6d 5c 78 33 64 41 50 67 45 57 41 2f 64 5c 78 33 64 31 2f 65 64 5c 78 33 64 31 2f 72 73 5c 78 33 64 41 43 54 39 30 6f 47 4a 35 4e 76 76 74 44 74 50 62 6e 57 75 79 68 74 75 53 55 76 36 6a 57 41 43 36 77 2f 6d 5c 78 33 64 73 62 5f 68 65 2c 64 27 3b 0a 76 61 72 20 65 3d 74 68 69 73 7c 7c 73 65 6c 66 2c 66 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 7d 3b 76 61 72 20 67 3b 76 61 72 20 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 68 69 73 2e 67 3d 62 3d 3d 3d 68 3f 61 3a 22 22 7d 3b 6c 2e 70 72 6f 74 6f 74 79 70 65 2e 74 6f 53 74 72 69 6e 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 67 2b 22 22 7d 3b 76 61 72 20 68 3d 7b 7d 3b 66 75 6e 63 74 69 6f 6e 20 6d 28 29 7b 76 61 72 20 61 3d 75 3b 67 6f 6f 67 6c 65 Data Ascii: m\x3dAPgEWA/d\x3d1/ed\x3d1/rs\x3dACT90oGJ5NvvtDtPbnWuyhtuSUv6jWAC6w/m\x3dsb_he,d';var e=this||self,f=function(a){return a};var g;var l=function(a,b){this.g=b===h?a:""};l.prototype.toString=function(){return this.g+""};var h={};function m(){var a=u;google

Timestamp	kBytes transferred	Direction	Data
2021-09-15 08:19:58 UTC	47	IN	Data Raw: 7d 29 28 29 3b 66 75 6e 63 74 69 6f 6e 20 5f 44 75 6d 70 45 78 63 65 70 74 69 6f 6e 28 65 29 7b 74 68 72 6f 77 20 65 3b 7d 0a 66 75 6e 63 74 69 6f 6e 20 5f 46 5f 69 6e 73 74 61 6c 6c 43 73 73 28 63 29 7b 7d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 67 6f 6f 67 6c 65 2e 6a 6c 3d 7b 61 74 74 6e 3a 66 61 6c 73 65 2c 62 6c 74 3a 27 6e 6f 6e 65 27 2c 63 68 6e 6b 3a 30 2c 64 77 3a 66 61 6c 73 65 2c 65 6d 74 6e 3a 30 2c 65 6e 64 3a 30 2c 69 6e 65 3a 66 61 6c 73 65 2c 6c 6c 73 3a 27 64 65 66 61 75 6c 74 27 2c 70 64 74 3a 30 2c 72 65 70 3a 30 2c 73 69 66 3a 74 72 75 65 2c 73 6e 65 74 3a 74 72 75 65 2c 73 74 72 74 3a 30 2c 75 62 6d 3a 66 61 6c 73 65 2c 75 77 70 3a 74 72 75 65 7d 3b 7d 29 28 29 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 70 6d 63 3d 27 7b 5c 78 Data Ascii: })();function _DumpException(e){throw e;}function _F_installCss(c){}(function(){google.jl={attn:false,blt:'none',chnk:0,dw:false,emtn:0,end:0,ine:false,lls:'default',pdt:0,rep:0,sif:true,snet:true,strt:0,ubm:false,uwp:true};})();(function(){var pmc='{\x
2021-09-15 08:19:58 UTC	48	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO-INV 21460041492040401.PDF.exe PID: 6016 Parent PID: 5704

General

Start time:	10:19:56
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO-INV 21460041492040401.PDF.exe'
Imagebase:	0x310000
File size:	961024 bytes
MD5 hash:	8E23941E7D2BD97F91B83AA52CE9D2EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361666966.0000000003894000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361666966.0000000003894000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361666966.0000000003894000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361495255.00000000037B5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361495255.00000000037B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361495255.00000000037B5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361849157.0000000003992000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361849157.0000000003992000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361849157.0000000003992000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 6304 Parent PID: 6016

General

Start time:	10:20:44
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0xb50000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.512833462.0000000002F01000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.517406804.00000000057B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.517406804.00000000057B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.508601961.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.508601961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.508601961.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.517482154.0000000005870000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000010.00000002.517482154.0000000005870000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.517482154.0000000005870000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.516134110.0000000003F09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.516134110.0000000003F09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6380 Parent PID: 6304

General

Start time:	10:20:51
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD621.tmp'
Imagebase:	0xfa0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6388 Parent PID: 6380

General

Start time:	10:20:51
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: schtasks.exe PID: 6436 Parent PID: 6304

General

Start time:	10:20:52
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDAD5.tmp'
Imagebase:	0xfa0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6444 Parent PID: 6436

General

Start time:	10:20:52
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegAsm.exe PID: 6488 Parent PID: 904

General

Start time:	10:20:53
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe 0
Imagebase:	0x8d0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6504 Parent PID: 6488

General

Start time:	10:20:54
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: dhcpmon.exe PID: 6532 Parent PID: 904

General

Start time:	10:20:54
Start date:	15/09/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x420000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6552 Parent PID: 6532

General

Start time:	10:20:54
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 7020 Parent PID: 3472

General

Start time:	10:21:02
Start date:	15/09/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x120000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 7060 Parent PID: 7020

General

Start time:	10:21:02
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis