ID: 431544
Sample Name: unpacked.bin
Cookbook: default.jbs
Time: 21:45:03
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

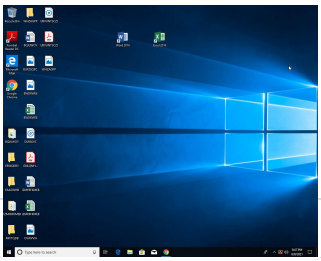
Analysis Report unpacked.bin

Overview

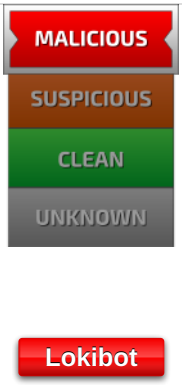
General Information

Sample Name:	unpacked.bin (renamed file extension from bin to exe)
Analysis ID:	431544
MD5:	1917f888cacd48b..
SHA1:	d732e6a78ea44b..
SHA256:	3deeb55fefe05f5…
Tags:	exe lokibot
Infos:	

Most interesting Screenshot:



Detection

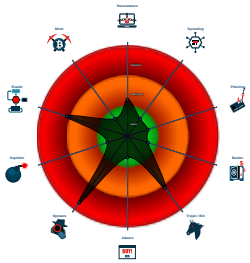


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Yara detected Lokibot
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- unpacked.exe (PID: 6916 cmdline: 'C:\Users\user\Desktop\unpacked.exe' MD5: 1917F888CACD48B9A8D4832449E8D34F)
- **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"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
unpacked.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x13e80:$s2: https:// • 0x18074:$s2: \x97\x8B\x8B\x8F\x8C\xC5\xD0\xD0 • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
unpacked.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
unpacked.exe	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	

Source	Rule	Description	Author	Strings
unpacked.exe	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
unpacked.exe	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.907785402.000000000415000.00000002.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.907785402.000000000415000.00000002.00020000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.907785402.000000000415000.00000002.00020000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000000.643480909.000000000415000.00000002.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000000.643480909.000000000415000.00000002.00020000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.unpacked.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.unpacked.exe.400000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.unpacked.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0.2.unpacked.exe.400000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
0.2.unpacked.exe.400000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected aPLib compressed binary

Stealing of Sensitive Information:

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

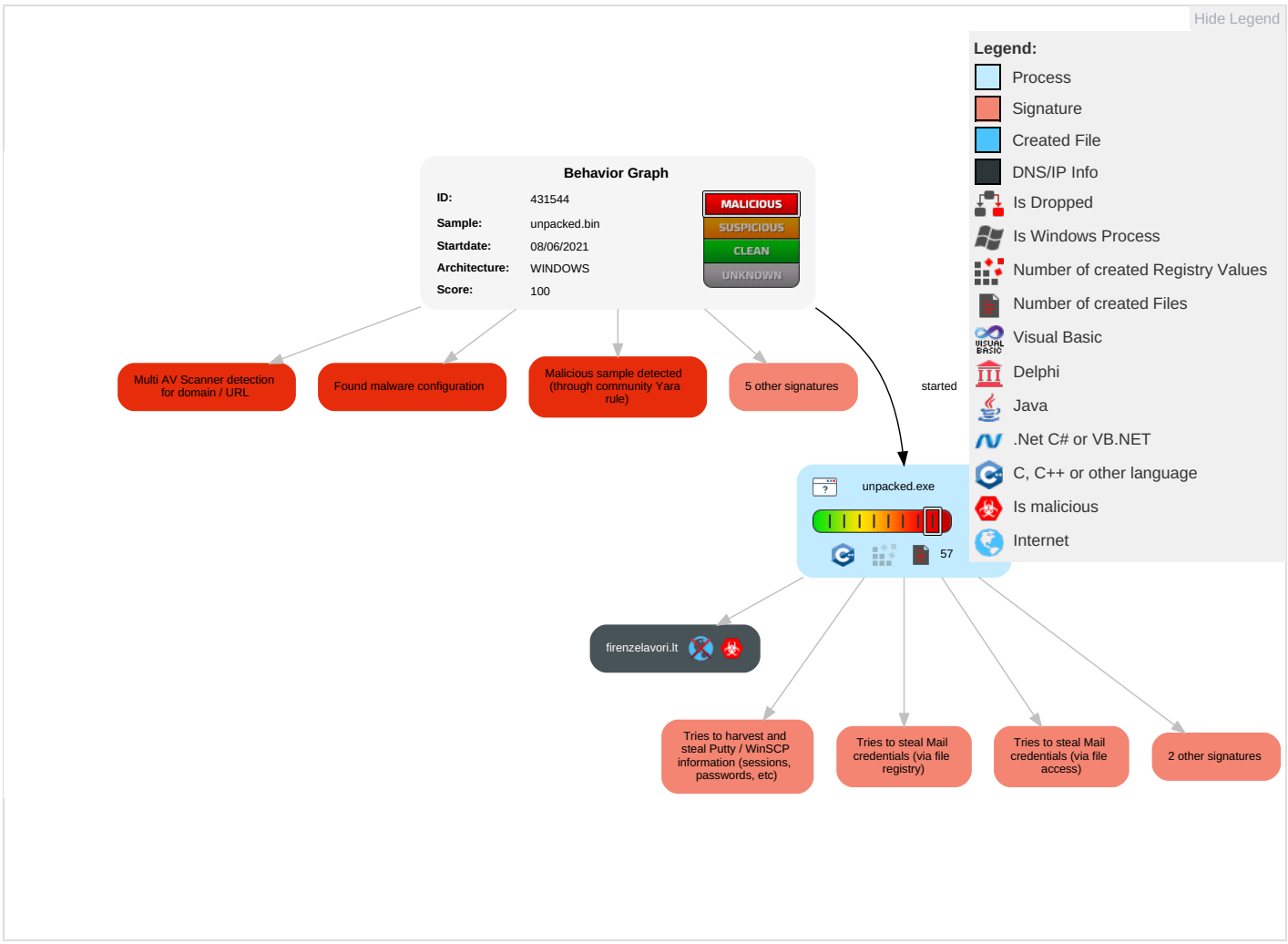
Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Credentials in Registry 2	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco

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
unpacked.exe	100%	Avira	TR/Crypt.XPACK.Gen	
unpacked.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.unpacked.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.unpacked.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
firenzelavori.lt	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://https://firenzelavori.lt/loki/Panel/five/fre.php	10%	Virustotal		Browse
http://https://firenzelavori.lt/loki/Panel/five/fre.php	0%	Avira URL Cloud	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	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.ibsensoftware.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
firenzelavori.lt	unknown	unknown	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431544

Start date:	08.06.2021
Start time:	21:45:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	unpacked.bin (renamed file extension from bin to 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:	16
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@1/2@157/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.9%) • Quality average: 76.9% • Quality standard deviation: 28.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:46:02	API Interceptor	26x Sleep call for process: unpacked.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\unpacked.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\unpacked.exe
File Type:	data
Category:	dropped
Size (bytes):	10718
Entropy (8bit):	0.6039339853994985
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/gg:w
MD5:	C7ADD3D3A64EBD1148853BB23AFBA9BB
SHA1:	B5D425C10D7730DB432E9B0DCC74707132299F86
SHA-256:	AF8070E934B1B40B485E661925D15D2A5B362A6924B3B7F7FFF6AF9373BAF7BA
SHA-512:	19D4BA9560BE7F43FC7F2F86A5F9BE2CE3F11D46F99EF4FA0652364702FF42A62E9E363CA25B9B0319F1D5508B3BB5C9850266C6CAC086A74005A1A99697A8E(
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, for MS Windows
Entropy (8bit):	6.054379657980403
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	unpacked.exe
File size:	106496
MD5:	1917f888cacd48b9a8d4832449e8d34f
SHA1:	d732e6a78ea44b77943c1e74e19c9ea92d0b7a28
SHA256:	3deeb55fefe05f51c41b1724780e5de1e33a432e01f455e3ab5d2af5ca655464
SHA512:	901b095813605c89945e1b5354fef210b0a68d94a79156b5d405116c5f00a15571046a0e9d65830cdaea8a3deda657a6d4ac6744ecef30cca6b26033d8b61b55

General

SSDEEP:	1536:czvQSZpGS4/31A6mQgL2eYCGDwRcMkVQd8YhY0/EqfIzmd:nSHIG6mQwGmfOQd8YhY0/EqUG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x.....K.K.....=2.....=2.....=2.....Rich.....PE..L.....IW...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4139de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x576C0885 [Thu Jun 23 16:04:21 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	0239fd611af3d0e9b0c46c5837c80e09

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x136f5	0x13800	False	0.568509615385	data	6.49204829439	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x4060	0x4200	False	0.365944602273	data	4.25599948305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1a000	0x85e24	0x200	False	0.056640625	data	0.321716074313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.x	0xa0000	0x2000	0x2000	False	0.0194091796875	data	0.215612772574	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/08/21-21:45:54.964981	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/08/21-21:45:56.099009	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:45:57.298036	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:45:58.656733	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:00.751806	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:01.754117	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:02.956035	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:04.041251	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:05.052317	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:06.495672	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:07.523806	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:08.667938	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:10.878494	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:11.909233	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:13.112330	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:14.141931	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:15.412834	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:16.459862	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:17.552955	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:18.558916	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:20.849702	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:22.067990	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:22.966525	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:24.303998	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:25.381509	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:26.549659	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:27.582089	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:29.147828	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:30.159692	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:31.392048	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:32.534581	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:34.568874	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:36.930081	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:39.055318	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:41.273154	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:42.322420	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:43.383142	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:44.412509	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/08/21-21:46:46.192174	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:48.177418	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:49.217508	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:50.474508	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:51.461367	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:52.631150	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:53.835880	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:55.850179	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:56.895356	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:57.928431	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:46:59.167510	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:00.166543	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:01.306661	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:02.311429	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:03.650406	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:04.635429	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:05.742289	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:06.741761	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:09.007209	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:10.111150	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:11.101358	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:12.360436	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:13.478896	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:15.729908	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:16.714200	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:18.537071	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:21.017088	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:23.136770	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:24.175057	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:25.384551	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:26.427195	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:27.523031	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:28.824177	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:29.824469	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:30.916586	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:33.152055	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:34.167246	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/08/21-21:47:35.231782	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:36.266106	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:37.494183	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:38.520658	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:39.622604	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:41.862796	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:44.070337	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:45.015619	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:46.256576	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:47.254045	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:48.341446	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:49.365798	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:50.575788	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:52.731560	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:53.965149	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/08/21-21:47:56.097590	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 21:45:51.877125025 CEST	192.168.2.4	8.8.8.8	0xbfee	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:52.904454947 CEST	192.168.2.4	8.8.8.8	0xbfee	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:53.949357033 CEST	192.168.2.4	8.8.8.8	0xbfee	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:54.131951094 CEST	192.168.2.4	8.8.8.8	0xbfff	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:55.152808905 CEST	192.168.2.4	8.8.8.8	0xbfff	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:55.462305069 CEST	192.168.2.4	8.8.8.8	0xdba7	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:56.496690035 CEST	192.168.2.4	8.8.8.8	0xdba7	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:57.594887972 CEST	192.168.2.4	8.8.8.8	0xa13a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:58.606086016 CEST	192.168.2.4	8.8.8.8	0xa13a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:59.606571913 CEST	192.168.2.4	8.8.8.8	0xa13a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:59.883620977 CEST	192.168.2.4	8.8.8.8	0xe1e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:00.903748035 CEST	192.168.2.4	8.8.8.8	0xe1e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:01.950437069 CEST	192.168.2.4	8.8.8.8	0xe1e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 21:46:02.012041092 CEST	192.168.2.4	8.8.8.8	0x2348	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:02.997443914 CEST	192.168.2.4	8.8.8.8	0x2348	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:03.437616110 CEST	192.168.2.4	8.8.8.8	0x3944	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:04.434828997 CEST	192.168.2.4	8.8.8.8	0x3944	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:05.453898907 CEST	192.168.2.4	8.8.8.8	0x3944	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:05.570528984 CEST	192.168.2.4	8.8.8.8	0x7d6	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:06.612905025 CEST	192.168.2.4	8.8.8.8	0x7d6	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:07.839531898 CEST	192.168.2.4	8.8.8.8	0x9c1f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:08.827095032 CEST	192.168.2.4	8.8.8.8	0x9c1f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:09.857043028 CEST	192.168.2.4	8.8.8.8	0x9c1f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:09.970566988 CEST	192.168.2.4	8.8.8.8	0x70ed	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:10.966896057 CEST	192.168.2.4	8.8.8.8	0x70ed	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:11.998529911 CEST	192.168.2.4	8.8.8.8	0x70ed	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:12.360927105 CEST	192.168.2.4	8.8.8.8	0xbbc0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:13.357603073 CEST	192.168.2.4	8.8.8.8	0xbbc0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:14.404340982 CEST	192.168.2.4	8.8.8.8	0xbbc0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:14.492835999 CEST	192.168.2.4	8.8.8.8	0x38f9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:15.482626915 CEST	192.168.2.4	8.8.8.8	0x38f9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:16.498698950 CEST	192.168.2.4	8.8.8.8	0x38f9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:16.765202045 CEST	192.168.2.4	8.8.8.8	0x5abe	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:17.779926062 CEST	192.168.2.4	8.8.8.8	0x5abe	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:18.795504093 CEST	192.168.2.4	8.8.8.8	0x5abe	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:18.877701044 CEST	192.168.2.4	8.8.8.8	0x87d9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:19.904709101 CEST	192.168.2.4	8.8.8.8	0x87d9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:20.905123949 CEST	192.168.2.4	8.8.8.8	0x87d9	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:21.246056080 CEST	192.168.2.4	8.8.8.8	0xaa5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:22.248971939 CEST	192.168.2.4	8.8.8.8	0xaa5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:23.330734015 CEST	192.168.2.4	8.8.8.8	0xaa5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:23.491897106 CEST	192.168.2.4	8.8.8.8	0x671c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:24.499166965 CEST	192.168.2.4	8.8.8.8	0x671c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:25.520415068 CEST	192.168.2.4	8.8.8.8	0x671c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:26.081139088 CEST	192.168.2.4	8.8.8.8	0xf9eb	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:27.093158960 CEST	192.168.2.4	8.8.8.8	0xf9eb	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:28.108696938 CEST	192.168.2.4	8.8.8.8	0xf9eb	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:28.202702045 CEST	192.168.2.4	8.8.8.8	0x465b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:29.249587059 CEST	192.168.2.4	8.8.8.8	0x465b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:30.471527100 CEST	192.168.2.4	8.8.8.8	0x6046	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 21:46:31.468352079 CEST	192.168.2.4	8.8.8.8	0x6046	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:32.499547005 CEST	192.168.2.4	8.8.8.8	0x6046	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:32.584973097 CEST	192.168.2.4	8.8.8.8	0xe466	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:33.609155893 CEST	192.168.2.4	8.8.8.8	0xe466	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:34.842267036 CEST	192.168.2.4	8.8.8.8	0x1ca4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:35.876543045 CEST	192.168.2.4	8.8.8.8	0x1ca4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:35.967943907 CEST	192.168.2.4	8.8.8.8	0xb8fe	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:37.000228882 CEST	192.168.2.4	8.8.8.8	0xb8fe	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:38.201216936 CEST	192.168.2.4	8.8.8.8	0x4458	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:39.203886986 CEST	192.168.2.4	8.8.8.8	0x4458	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:40.251085043 CEST	192.168.2.4	8.8.8.8	0x4458	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:40.319829941 CEST	192.168.2.4	8.8.8.8	0xfd45	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:41.328957081 CEST	192.168.2.4	8.8.8.8	0xfd45	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:42.362428904 CEST	192.168.2.4	8.8.8.8	0xfd45	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:43.006941080 CEST	192.168.2.4	8.8.8.8	0xdf11	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:44.133902073 CEST	192.168.2.4	8.8.8.8	0xdf11	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:45.122220993 CEST	192.168.2.4	8.8.8.8	0xe24a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:46.111083984 CEST	192.168.2.4	8.8.8.8	0xe24a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:47.157222033 CEST	192.168.2.4	8.8.8.8	0xe24a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:47.389873028 CEST	192.168.2.4	8.8.8.8	0x967d	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:48.407136917 CEST	192.168.2.4	8.8.8.8	0x967d	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:49.407537937 CEST	192.168.2.4	8.8.8.8	0x967d	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:49.508212090 CEST	192.168.2.4	8.8.8.8	0x498d	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:50.549647093 CEST	192.168.2.4	8.8.8.8	0x498d	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:51.747528076 CEST	192.168.2.4	8.8.8.8	0xcdd8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:52.751557112 CEST	192.168.2.4	8.8.8.8	0xcdd8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:53.798799992 CEST	192.168.2.4	8.8.8.8	0xcdd8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:53.847084999 CEST	192.168.2.4	8.8.8.8	0x92e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:54.845546007 CEST	192.168.2.4	8.8.8.8	0x92e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:55.860851049 CEST	192.168.2.4	8.8.8.8	0x92e4	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:56.081727028 CEST	192.168.2.4	8.8.8.8	0xef23	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:57.111162901 CEST	192.168.2.4	8.8.8.8	0xef23	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:58.111620903 CEST	192.168.2.4	8.8.8.8	0xef23	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:58.231235981 CEST	192.168.2.4	8.8.8.8	0x94f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:59.252168894 CEST	192.168.2.4	8.8.8.8	0x94f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:00.252022982 CEST	192.168.2.4	8.8.8.8	0x94f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:00.577198029 CEST	192.168.2.4	8.8.8.8	0xa055	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 21:47:01.580754995 CEST	192.168.2.4	8.8.8.8	0xa055	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:02.580833912 CEST	192.168.2.4	8.8.8.8	0xa055	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:02.692893028 CEST	192.168.2.4	8.8.8.8	0xa7f0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:03.689793110 CEST	192.168.2.4	8.8.8.8	0xa7f0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:04.690243959 CEST	192.168.2.4	8.8.8.8	0xa7f0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:04.949143887 CEST	192.168.2.4	8.8.8.8	0xb68e	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:05.940279007 CEST	192.168.2.4	8.8.8.8	0xb68e	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:06.955763102 CEST	192.168.2.4	8.8.8.8	0xb68e	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:07.054735899 CEST	192.168.2.4	8.8.8.8	0x17b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:08.049606085 CEST	192.168.2.4	8.8.8.8	0x17b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:09.050389051 CEST	192.168.2.4	8.8.8.8	0x17b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:09.295856953 CEST	192.168.2.4	8.8.8.8	0x24d0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:10.299781084 CEST	192.168.2.4	8.8.8.8	0x24d0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:10.411015987 CEST	192.168.2.4	8.8.8.8	0x94d3	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:11.410487890 CEST	192.168.2.4	8.8.8.8	0x94d3	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:12.409337044 CEST	192.168.2.4	8.8.8.8	0x94d3	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:12.634934902 CEST	192.168.2.4	8.8.8.8	0x8f0b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:13.659801006 CEST	192.168.2.4	8.8.8.8	0x8f0b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:14.659584045 CEST	192.168.2.4	8.8.8.8	0x8f0b	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:15.185108900 CEST	192.168.2.4	8.8.8.8	0x366a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:16.481981039 CEST	192.168.2.4	8.8.8.8	0x366a	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:17.961178064 CEST	192.168.2.4	8.8.8.8	0xd515	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:18.956878901 CEST	192.168.2.4	8.8.8.8	0xd515	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:20.004018068 CEST	192.168.2.4	8.8.8.8	0xd515	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:20.076462984 CEST	192.168.2.4	8.8.8.8	0x6df5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:21.066327095 CEST	192.168.2.4	8.8.8.8	0x6df5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:22.113267899 CEST	192.168.2.4	8.8.8.8	0x6df5	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:22.336220980 CEST	192.168.2.4	8.8.8.8	0x5d9f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:23.332197905 CEST	192.168.2.4	8.8.8.8	0x5d9f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:24.363570929 CEST	192.168.2.4	8.8.8.8	0x5d9f	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:24.449955940 CEST	192.168.2.4	8.8.8.8	0x28c7	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:25.457873106 CEST	192.168.2.4	8.8.8.8	0x28c7	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:25.717809916 CEST	192.168.2.4	8.8.8.8	0xb6fc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:26.754235029 CEST	192.168.2.4	8.8.8.8	0xb6fc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:27.754870892 CEST	192.168.2.4	8.8.8.8	0xb6fc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:27.845082045 CEST	192.168.2.4	8.8.8.8	0xf0e0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:28.863986969 CEST	192.168.2.4	8.8.8.8	0xf0e0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 21:47:30.084748030 CEST	192.168.2.4	8.8.8.8	0x11f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:31.083328962 CEST	192.168.2.4	8.8.8.8	0x11f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:32.114192009 CEST	192.168.2.4	8.8.8.8	0x11f1	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:32.189172983 CEST	192.168.2.4	8.8.8.8	0xd4a0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:33.176843882 CEST	192.168.2.4	8.8.8.8	0xd4a0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:34.208899021 CEST	192.168.2.4	8.8.8.8	0xd4a0	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:34.429323912 CEST	192.168.2.4	8.8.8.8	0x6de8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:35.443193913 CEST	192.168.2.4	8.8.8.8	0x6de8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:36.458527088 CEST	192.168.2.4	8.8.8.8	0x6de8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:36.563122034 CEST	192.168.2.4	8.8.8.8	0x466e	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:37.552800894 CEST	192.168.2.4	8.8.8.8	0x466e	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:38.807032108 CEST	192.168.2.4	8.8.8.8	0xd63c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:39.802510023 CEST	192.168.2.4	8.8.8.8	0xd63c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:40.864825010 CEST	192.168.2.4	8.8.8.8	0xd63c	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:40.934251070 CEST	192.168.2.4	8.8.8.8	0xebf8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:41.927423000 CEST	192.168.2.4	8.8.8.8	0xebf8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:42.958767891 CEST	192.168.2.4	8.8.8.8	0xebf8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:43.184807062 CEST	192.168.2.4	8.8.8.8	0x3cb8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:44.193227053 CEST	192.168.2.4	8.8.8.8	0x3cb8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:45.193996906 CEST	192.168.2.4	8.8.8.8	0x3cb8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:45.297132015 CEST	192.168.2.4	8.8.8.8	0xd6db	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:46.287997961 CEST	192.168.2.4	8.8.8.8	0xd6db	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:47.303075075 CEST	192.168.2.4	8.8.8.8	0xd6db	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:47.535079002 CEST	192.168.2.4	8.8.8.8	0x6347	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:48.522089958 CEST	192.168.2.4	8.8.8.8	0x6347	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:48.657644987 CEST	192.168.2.4	8.8.8.8	0x1cdc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:49.647190094 CEST	192.168.2.4	8.8.8.8	0x1cdc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:50.662636995 CEST	192.168.2.4	8.8.8.8	0x1cdc	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:50.917951107 CEST	192.168.2.4	8.8.8.8	0x52ab	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:51.912719011 CEST	192.168.2.4	8.8.8.8	0x52ab	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:52.959919930 CEST	192.168.2.4	8.8.8.8	0x52ab	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:53.047916889 CEST	192.168.2.4	8.8.8.8	0x6bb8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:54.037939072 CEST	192.168.2.4	8.8.8.8	0x6bb8	Standard query (0)	firenzelavori.lt	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:45:54.031042099 CEST	8.8.8.8	192.168.2.4	0xbfee	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:45:54.964849949 CEST	8.8.8.8	192.168.2.4	0xbfee	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:55.283318996 CEST	8.8.8.8	192.168.2.4	0xbfff	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:56.096419096 CEST	8.8.8.8	192.168.2.4	0xbfee	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:57.297934055 CEST	8.8.8.8	192.168.2.4	0xbfff	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:57.530993938 CEST	8.8.8.8	192.168.2.4	0xdba7	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:58.656579018 CEST	8.8.8.8	192.168.2.4	0xdba7	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:45:59.748205900 CEST	8.8.8.8	192.168.2.4	0xa13a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:00.751663923 CEST	8.8.8.8	192.168.2.4	0xa13a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:01.754004955 CEST	8.8.8.8	192.168.2.4	0xa13a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:01.954190969 CEST	8.8.8.8	192.168.2.4	0xe1e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:02.955827951 CEST	8.8.8.8	192.168.2.4	0xe1e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:03.166112900 CEST	8.8.8.8	192.168.2.4	0x2348	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:04.041093111 CEST	8.8.8.8	192.168.2.4	0xe1e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:05.052217960 CEST	8.8.8.8	192.168.2.4	0x2348	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:05.497453928 CEST	8.8.8.8	192.168.2.4	0x3944	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:06.495476007 CEST	8.8.8.8	192.168.2.4	0x3944	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:07.523649931 CEST	8.8.8.8	192.168.2.4	0x3944	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:07.637537956 CEST	8.8.8.8	192.168.2.4	0x7d6	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:08.667673111 CEST	8.8.8.8	192.168.2.4	0x7d6	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:09.898715973 CEST	8.8.8.8	192.168.2.4	0x9c1f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:10.878359079 CEST	8.8.8.8	192.168.2.4	0x9c1f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:11.909037113 CEST	8.8.8.8	192.168.2.4	0x9c1f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:12.116466045 CEST	8.8.8.8	192.168.2.4	0x70ed	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:13.111957073 CEST	8.8.8.8	192.168.2.4	0x70ed	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:14.141757011 CEST	8.8.8.8	192.168.2.4	0x70ed	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:14.428513050 CEST	8.8.8.8	192.168.2.4	0xbbc0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:46:15.412590027 CEST	8.8.8.8	192.168.2.4	0xbbc0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:16.459697962 CEST	8.8.8.8	192.168.2.4	0xbbc0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:16.559284925 CEST	8.8.8.8	192.168.2.4	0x38f9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:17.551523924 CEST	8.8.8.8	192.168.2.4	0x38f9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:18.558773994 CEST	8.8.8.8	192.168.2.4	0x38f9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:18.817079067 CEST	8.8.8.8	192.168.2.4	0x5abe	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:18.845583916 CEST	8.8.8.8	192.168.2.4	0x5abe	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:20.849522114 CEST	8.8.8.8	192.168.2.4	0x5abe	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:21.023518085 CEST	8.8.8.8	192.168.2.4	0x87d9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:22.067851067 CEST	8.8.8.8	192.168.2.4	0x87d9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:22.966429949 CEST	8.8.8.8	192.168.2.4	0x87d9	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:23.406764984 CEST	8.8.8.8	192.168.2.4	0xaa5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:24.303822994 CEST	8.8.8.8	192.168.2.4	0xaa5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:25.381407022 CEST	8.8.8.8	192.168.2.4	0xaa5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:25.544979095 CEST	8.8.8.8	192.168.2.4	0x671c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:26.549565077 CEST	8.8.8.8	192.168.2.4	0x671c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:27.578676939 CEST	8.8.8.8	192.168.2.4	0x671c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:28.133059978 CEST	8.8.8.8	192.168.2.4	0xf9eb	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:29.147697926 CEST	8.8.8.8	192.168.2.4	0xf9eb	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:30.159603119 CEST	8.8.8.8	192.168.2.4	0xf9eb	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:30.252590895 CEST	8.8.8.8	192.168.2.4	0x465b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:31.391915083 CEST	8.8.8.8	192.168.2.4	0x465b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:32.521692991 CEST	8.8.8.8	192.168.2.4	0x6046	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:32.534461021 CEST	8.8.8.8	192.168.2.4	0x6046	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:34.568773985 CEST	8.8.8.8	192.168.2.4	0x6046	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:34.649571896 CEST	8.8.8.8	192.168.2.4	0xe466	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:46:34.676616907 CEST	8.8.8.8	192.168.2.4	0xe466	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:35.903491020 CEST	8.8.8.8	192.168.2.4	0x1ca4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:36.929928064 CEST	8.8.8.8	192.168.2.4	0x1ca4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:38.021327019 CEST	8.8.8.8	192.168.2.4	0xb8fe	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:39.055157900 CEST	8.8.8.8	192.168.2.4	0xb8fe	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:40.255594969 CEST	8.8.8.8	192.168.2.4	0x4458	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:41.272996902 CEST	8.8.8.8	192.168.2.4	0x4458	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:42.322325945 CEST	8.8.8.8	192.168.2.4	0x4458	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:42.377063036 CEST	8.8.8.8	192.168.2.4	0xfd45	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:43.381939888 CEST	8.8.8.8	192.168.2.4	0xfd45	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:44.412440062 CEST	8.8.8.8	192.168.2.4	0xfd45	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:45.058058977 CEST	8.8.8.8	192.168.2.4	0xdf11	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:46.191679001 CEST	8.8.8.8	192.168.2.4	0xdf11	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:47.190107107 CEST	8.8.8.8	192.168.2.4	0xe24a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:48.177098989 CEST	8.8.8.8	192.168.2.4	0xe24a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:49.217385054 CEST	8.8.8.8	192.168.2.4	0xe24a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:49.458240032 CEST	8.8.8.8	192.168.2.4	0x967d	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:50.473567009 CEST	8.8.8.8	192.168.2.4	0x967d	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:51.460020065 CEST	8.8.8.8	192.168.2.4	0x967d	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:51.563159943 CEST	8.8.8.8	192.168.2.4	0x498d	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:52.630448103 CEST	8.8.8.8	192.168.2.4	0x498d	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:53.799050093 CEST	8.8.8.8	192.168.2.4	0xcdd8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:53.833877087 CEST	8.8.8.8	192.168.2.4	0xcdd8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:55.848917961 CEST	8.8.8.8	192.168.2.4	0xcdd8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:55.906429052 CEST	8.8.8.8	192.168.2.4	0x92e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:56.895240068 CEST	8.8.8.8	192.168.2.4	0x92e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:46:57.927381039 CEST	8.8.8.8	192.168.2.4	0x92e4	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:58.141593933 CEST	8.8.8.8	192.168.2.4	0xef23	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:46:59.167232990 CEST	8.8.8.8	192.168.2.4	0xef23	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:00.166117907 CEST	8.8.8.8	192.168.2.4	0xef23	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:00.375360012 CEST	8.8.8.8	192.168.2.4	0x94f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:01.303164005 CEST	8.8.8.8	192.168.2.4	0x94f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:02.311242104 CEST	8.8.8.8	192.168.2.4	0x94f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:02.639693975 CEST	8.8.8.8	192.168.2.4	0xa055	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:03.650212049 CEST	8.8.8.8	192.168.2.4	0xa055	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:04.635265112 CEST	8.8.8.8	192.168.2.4	0xa055	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:04.753757954 CEST	8.8.8.8	192.168.2.4	0xa7f0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:05.742089987 CEST	8.8.8.8	192.168.2.4	0xa7f0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:06.741580009 CEST	8.8.8.8	192.168.2.4	0xa7f0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:06.995599985 CEST	8.8.8.8	192.168.2.4	0xb68e	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:06.999622107 CEST	8.8.8.8	192.168.2.4	0xb68e	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:09.006959915 CEST	8.8.8.8	192.168.2.4	0xb68e	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:09.118876934 CEST	8.8.8.8	192.168.2.4	0x17b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:10.110972881 CEST	8.8.8.8	192.168.2.4	0x17b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:10.346471071 CEST	8.8.8.8	192.168.2.4	0x24d0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:11.101150036 CEST	8.8.8.8	192.168.2.4	0x17b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:12.360198021 CEST	8.8.8.8	192.168.2.4	0x24d0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:12.463222027 CEST	8.8.8.8	192.168.2.4	0x94d3	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:13.478159904 CEST	8.8.8.8	192.168.2.4	0x94d3	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:13.478791952 CEST	8.8.8.8	192.168.2.4	0x94d3	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:14.685441971 CEST	8.8.8.8	192.168.2.4	0x8f0b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:15.729770899 CEST	8.8.8.8	192.168.2.4	0x8f0b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:47:16.714116096 CEST	8.8.8.8	192.168.2.4	0x8f0b	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:17.254282951 CEST	8.8.8.8	192.168.2.4	0x366a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:18.536780119 CEST	8.8.8.8	192.168.2.4	0x366a	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:20.016000032 CEST	8.8.8.8	192.168.2.4	0xd515	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:21.015921116 CEST	8.8.8.8	192.168.2.4	0xd515	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:21.054079056 CEST	8.8.8.8	192.168.2.4	0xd515	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:22.136045933 CEST	8.8.8.8	192.168.2.4	0x6df5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:23.136607885 CEST	8.8.8.8	192.168.2.4	0x6df5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:24.174911976 CEST	8.8.8.8	192.168.2.4	0x6df5	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:24.389036894 CEST	8.8.8.8	192.168.2.4	0x5d9f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:25.384382963 CEST	8.8.8.8	192.168.2.4	0x5d9f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:25.519726038 CEST	8.8.8.8	192.168.2.4	0x28c7	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:26.427104950 CEST	8.8.8.8	192.168.2.4	0x5d9f	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:27.522811890 CEST	8.8.8.8	192.168.2.4	0x28c7	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:27.780371904 CEST	8.8.8.8	192.168.2.4	0xb6fc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:28.824048042 CEST	8.8.8.8	192.168.2.4	0xb6fc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:29.824358940 CEST	8.8.8.8	192.168.2.4	0xb6fc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:29.909408092 CEST	8.8.8.8	192.168.2.4	0xf0e0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:30.916280031 CEST	8.8.8.8	192.168.2.4	0xf0e0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:32.136877060 CEST	8.8.8.8	192.168.2.4	0x11f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:33.151773930 CEST	8.8.8.8	192.168.2.4	0x11f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:34.166973114 CEST	8.8.8.8	192.168.2.4	0x11f1	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:34.240186930 CEST	8.8.8.8	192.168.2.4	0xd4a0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:35.231642962 CEST	8.8.8.8	192.168.2.4	0xd4a0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:36.265803099 CEST	8.8.8.8	192.168.2.4	0xd4a0	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:36.501844883 CEST	8.8.8.8	192.168.2.4	0x6de8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 21:47:37.493937969 CEST	8.8.8.8	192.168.2.4	0x6de8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:38.519963026 CEST	8.8.8.8	192.168.2.4	0x6de8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:38.613956928 CEST	8.8.8.8	192.168.2.4	0x466e	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:39.622416973 CEST	8.8.8.8	192.168.2.4	0x466e	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:40.868098021 CEST	8.8.8.8	192.168.2.4	0xd63c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:41.862596035 CEST	8.8.8.8	192.168.2.4	0xd63c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:41.915184021 CEST	8.8.8.8	192.168.2.4	0xd63c	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:43.001543045 CEST	8.8.8.8	192.168.2.4	0xebf8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:44.070219040 CEST	8.8.8.8	192.168.2.4	0xebf8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:45.015480042 CEST	8.8.8.8	192.168.2.4	0xebf8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:45.244647980 CEST	8.8.8.8	192.168.2.4	0x3cb8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:46.256390095 CEST	8.8.8.8	192.168.2.4	0x3cb8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:47.253948927 CEST	8.8.8.8	192.168.2.4	0x3cb8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:47.349199057 CEST	8.8.8.8	192.168.2.4	0xd6db	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:48.341305017 CEST	8.8.8.8	192.168.2.4	0xd6db	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:48.602914095 CEST	8.8.8.8	192.168.2.4	0x6347	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:49.365561962 CEST	8.8.8.8	192.168.2.4	0xd6db	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:50.575690985 CEST	8.8.8.8	192.168.2.4	0x6347	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:50.713604927 CEST	8.8.8.8	192.168.2.4	0x1cdc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:50.718641043 CEST	8.8.8.8	192.168.2.4	0x1cdc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:52.731357098 CEST	8.8.8.8	192.168.2.4	0x1cdc	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:52.988394976 CEST	8.8.8.8	192.168.2.4	0x52ab	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:53.964979887 CEST	8.8.8.8	192.168.2.4	0x52ab	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:54.010020018 CEST	8.8.8.8	192.168.2.4	0x52ab	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:54.116904020 CEST	8.8.8.8	192.168.2.4	0x6bb8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)
Jun 8, 2021 21:47:56.097395897 CEST	8.8.8.8	192.168.2.4	0x6bb8	Server failure (2)	firenzelavori.lt	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: unpacked.exe PID: 6916 Parent PID: 5976

General

Start time:	21:45:49
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\unpacked.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\unpacked.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	1917F888CACD48B9A8D4832449E8D34F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.907785402.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.907785402.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.907785402.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.643480909.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000000.643480909.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000000.643480909.0000000000415000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis