ID: 694557
Sample Name:
eW1QrimJYd.exe
Cookbook: default.jbs
Time: 23:47:37
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

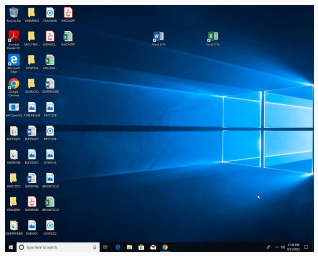
Windows Analysis Report

eW1QrimJYd.exe

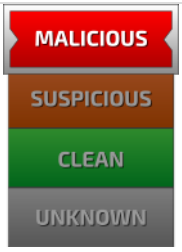
Overview

General Information

Sample Name:	eW1QrimJYd.exe
Analysis ID:	694557
MD5:	b7325e075262ffd.
SHA1:	2dee9b7321c736..
SHA256:	88a85792d16b3e.
Tags:	exe
Infos:	



Detection



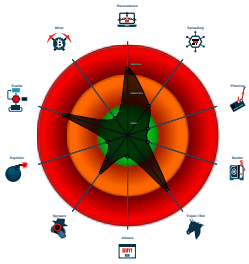
Gandcrab

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

Signatures

- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Found evasive API chain (may stop…
- Contains functionality to determine t…
- Found Tor onion address
- Uses nslookup.exe to query domains
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- eW1QrimJYd.exe (PID: 4500 cmdline: "C:\Users\user\Desktop\eW1QrimJYd.exe" MD5: B7325E075262FFDEAA68CAE94018CADB)
  - nslookup.exe (PID: 5720 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5916 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5400 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5732 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4788 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 3572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5276 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6148 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6220 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6316 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6372 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6528 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6632 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6720 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6808 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6920 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7028 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7100 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7156 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)

- conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6164 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6288 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 2852 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 1432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 2408 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6392 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- qvvfpl.exe (PID: 3252 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe" MD5: E5E0C9F951E9947AEA55720B7D0299F2)
- qvvfpl.exe (PID: 68 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe" MD5: E5E0C9F951E9947AEA55720B7D0299F2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
eW1QrimJYd.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
eW1QrimJYd.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
eW1QrimJYd.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xf70c:$string1: GDCB-DECRYPT.txt • 0xf77a:$string1: GDCB-DECRYPT.txt • 0xf460:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xf70c:$string1: GDCB-DECRYPT.txt • 0xf77a:$string1: GDCB-DECRYPT.txt • 0xf460:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.311448565.0000000000D79000.00000004.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000018.00000000.308301094.0000000000D79000.00000008.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0000000B.00000000.290444735.0000000000D79000.00000008.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000001.00000000.250804234.0000000000A89000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
11.0.qvvfpl.exe.d70000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
11.0.qvvfpl.exe.d70000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
11.0.qvvfpl.exe.d70000.0.unpack	Gandcrab	Gandcrab Payload	kevoreilly	• 0xf70c:$string1: GDCB-DECRYPT.txt • 0xf77a:$string1: GDCB-DECRYPT.txt • 0xf460:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
11.2.qvvfpl.exe.d70000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
11.2.qvvfpl.exe.d70000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 13 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.860695532026737 08/31/22-23:49:57.078873
SID:	2026737
Source Port:	60695
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.864649532026737 08/31/22-23:50:23.329807
SID:	2026737
Source Port:	64649
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.850255532829498 08/31/22-23:50:34.185397
SID:	2829498
Source Port:	50255
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.862039532829498 08/31/22-23:50:37.987567
SID:	2829498
Source Port:	62039
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.857518532829498 08/31/22-23:49:46.207614
SID:	2829498

Source Port:	57518
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849468532026737 08/31/22-23:50:44.319184
SID:	2026737
Source Port:	49468
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856571532829500 08/31/22-23:49:21.389711
SID:	2829500
Source Port:	56571
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863674532829500 08/31/22-23:50:38.481064
SID:	2829500
Source Port:	63674
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861613532829500 08/31/22-23:49:00.911463
SID:	2829500
Source Port:	61613
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854197532829500 08/31/22-23:50:08.085752
SID:	2829500
Source Port:	54197
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861175532026737 08/31/22-23:50:41.147699
SID:	2026737
Source Port:	61175
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851324532829500 08/31/22-23:49:50.142801
SID:	2829500
Source Port:	51324
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852486532026737 08/31/22-23:49:02.339569
SID:	2026737
Source Port:	52486
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849335532829498 08/31/22-23:50:15.024115
SID:	2829498
Source Port:	49335
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851891532829498 08/31/22-23:50:24.371077
SID:	2829498
Source Port:	51891
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864544532026737 08/31/22-23:50:11.785305
SID:	2026737
Source Port:	64544
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853945532829498 08/31/22-23:49:03.940196
SID:	2829498
Source Port:	53945
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862852532829500 08/31/22-23:49:39.251383
SID:	2829500
Source Port:	62852
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854906532829500 08/31/22-23:48:50.247066
SID:	2829500
Source Port:	54906
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852869532829500 08/31/22-23:49:26.819001
SID:	2829500
Source Port:	52869

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856360532829500 08/31/22-23:50:13.477447
SID:	2829500
Source Port:	56360
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857327532026737 08/31/22-23:49:34.029795
SID:	2026737
Source Port:	57327
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864652532026737 08/31/22-23:50:23.390728
SID:	2026737
Source Port:	64652
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852847532026737 08/31/22-23:50:18.746734
SID:	2026737
Source Port:	52847
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862850532829500 08/31/22-23:49:39.210928
SID:	2829500
Source Port:	62850
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853198532829498 08/31/22-23:50:30.152335
SID:	2829498
Source Port:	53198
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864408532829498 08/31/22-23:49:37.493948
SID:	2829498
Source Port:	64408
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852845532026737 08/31/22-23:50:18.663879
SID:	2026737
Source Port:	52845
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861173532026737 08/31/22-23:50:41.105316
SID:	2026737
Source Port:	61173
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856435532829500 08/31/22-23:50:42.448009
SID:	2829500
Source Port:	56435
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863265532829500 08/31/22-23:50:03.877266
SID:	2829500
Source Port:	63265
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852818532829500 08/31/22-23:50:07.911995
SID:	2829500
Source Port:	52818
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853195532829498 08/31/22-23:50:29.933502
SID:	2829498
Source Port:	53195
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856551532026737 08/31/22-23:49:08.399946
SID:	2026737
Source Port:	56551
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851777532829498 08/31/22-23:50:06.235822
SID:	2829498
Source Port:	51777

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864801532829500 08/31/22-23:50:34.885486
SID:	2829500
Source Port:	64801
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862734532829500 08/31/22-23:49:54.828233
SID:	2829500
Source Port:	62734
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852484532026737 08/31/22-23:49:02.302880
SID:	2026737
Source Port:	52484
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855958532026737 08/31/22-23:49:42.850589
SID:	2026737
Source Port:	55958
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863672532829500 08/31/22-23:50:38.440019
SID:	2829500
Source Port:	63672
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849234532026737 08/31/22-23:49:22.846612
SID:	2026737
Source Port:	49234
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854881532829498 08/31/22-23:50:45.644561
SID:	2829498
Source Port:	54881
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852867532829500 08/31/22-23:49:26.766420
SID:	2829500
Source Port:	52867
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860011532829500 08/31/22-23:50:33.089754
SID:	2829500
Source Port:	60011
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851365532026737 08/31/22-23:50:14.017877
SID:	2026737
Source Port:	51365
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863267532829500 08/31/22-23:50:03.917309
SID:	2829500
Source Port:	63267
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856124532829498 08/31/22-23:48:57.941241
SID:	2829498
Source Port:	56124
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862040532829498 08/31/22-23:50:38.007802
SID:	2829498
Source Port:	62040
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864650532026737 08/31/22-23:50:23.349894
SID:	2026737
Source Port:	64650
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862736532829500 08/31/22-23:49:54.873826
SID:	2829500
Source Port:	62736

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862225532829498 08/31/22-23:50:03.325419
SID:	2829498
Source Port:	62225
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860013532829500 08/31/22-23:50:33.131001
SID:	2829500
Source Port:	60013
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854883532829498 08/31/22-23:50:45.681352
SID:	2829498
Source Port:	54883
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853592532829498 08/31/22-23:50:12.408515
SID:	2829498
Source Port:	53592
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856363532829500 08/31/22-23:50:13.551243
SID:	2829500
Source Port:	56363
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851775532829498 08/31/22-23:50:06.195982
SID:	2829498
Source Port:	51775
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859883532829498 08/31/22-23:49:13.365736
SID:	2829498
Source Port:	59883
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854513532026737 08/31/22-23:50:28.034455
SID:	2026737
Source Port:	54513
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855634532829498 08/31/22-23:49:19.687489
SID:	2829498
Source Port:	55634
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856574532829500 08/31/22-23:49:21.461712
SID:	2829500
Source Port:	56574
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856754532829498 08/31/22-23:49:57.581695
SID:	2829498
Source Port:	56754
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853947532829498 08/31/22-23:49:03.979774
SID:	2829498
Source Port:	53947
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854510532026737 08/31/22-23:50:25.933530
SID:	2026737
Source Port:	54510
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855960532026737 08/31/22-23:49:42.892259
SID:	2026737
Source Port:	55960
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864799532829500 08/31/22-23:50:34.845123
SID:	2829500
Source Port:	64799

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862539532026737 08/31/22-23:50:35.857432
SID:	2026737
Source Port:	62539
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859885532829498 08/31/22-23:49:13.407922
SID:	2829498
Source Port:	59885
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855632532829498 08/31/22-23:49:19.646853
SID:	2829498
Source Port:	55632
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864407532829498 08/31/22-23:49:37.460209
SID:	2829498
Source Port:	64407
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853196532829498 08/31/22-23:50:30.011263
SID:	2829498
Source Port:	53196
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856549532026737 08/31/22-23:49:08.357396
SID:	2026737
Source Port:	56549
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858920532829500 08/31/22-23:49:15.820662
SID:	2829500
Source Port:	58920
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853044532829500 08/31/22-23:50:24.850862
SID:	2829500
Source Port:	53044
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851534532026737 08/31/22-23:48:55.046078
SID:	2026737
Source Port:	51534
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858160532829500 08/31/22-23:50:17.191071
SID:	2829500
Source Port:	58160
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852718532026737 08/31/22-23:50:01.216655
SID:	2026737
Source Port:	52718
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862223532829498 08/31/22-23:50:03.241400
SID:	2829498
Source Port:	62223
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853045532829500 08/31/22-23:50:24.871066
SID:	2829500
Source Port:	53045
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850348532026737 08/31/22-23:49:17.376161
SID:	2026737
Source Port:	50348
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860693532026737 08/31/22-23:49:57.038533
SID:	2026737
Source Port:	60693

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864963532829498 08/31/22-23:50:19.837606
SID:	2829498
Source Port:	64963
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864798532829500 08/31/22-23:50:34.824859
SID:	2829500
Source Port:	64798
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854511532026737 08/31/22-23:50:27.946240
SID:	2026737
Source Port:	54511
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852717532026737 08/31/22-23:50:01.196442
SID:	2026737
Source Port:	52717
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856552532026737 08/31/22-23:49:08.420766
SID:	2026737
Source Port:	56552
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851366532026737 08/31/22-23:50:14.041221
SID:	2026737
Source Port:	51366
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860010532829500 08/31/22-23:50:33.071442
SID:	2829500
Source Port:	60010
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856430532829498 08/31/22-23:50:42.033912
SID:	2829498
Source Port:	56430
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856573532829500 08/31/22-23:49:21.437590
SID:	2829500
Source Port:	56573
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859886532829498 08/31/22-23:49:13.428276
SID:	2829498
Source Port:	59886
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855631532829498 08/31/22-23:49:19.625742
SID:	2829498
Source Port:	55631
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854202532026737 08/31/22-23:50:33.636817
SID:	2026737
Source Port:	54202
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854301532829500 08/31/22-23:50:47.037037
SID:	2829500
Source Port:	54301
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851774532829498 08/31/22-23:50:06.176893
SID:	2829498
Source Port:	51774
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854884532829498 08/31/22-23:50:45.706056
SID:	2829498
Source Port:	54884

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849237532026737 08/31/22-23:49:22.906523
SID:	2026737
Source Port:	49237
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857520532829498 08/31/22-23:49:46.246339
SID:	2829498
Source Port:	57520
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856128532829498 08/31/22-23:49:24.926548
SID:	2829498
Source Port:	56128
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862541532026737 08/31/22-23:50:35.901068
SID:	2026737
Source Port:	62541
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849337532829498 08/31/22-23:50:15.074780
SID:	2829498
Source Port:	49337
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862543532829498 08/31/22-23:48:47.529672
SID:	2829498
Source Port:	62543
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860001532026737 08/31/22-23:50:04.504698
SID:	2026737
Source Port:	60001
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862540532829498 08/31/22-23:48:47.468455
SID:	2829498
Source Port:	62540
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857325532026737 08/31/22-23:49:33.986496
SID:	2026737
Source Port:	57325
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853946532829498 08/31/22-23:49:03.959032
SID:	2829498
Source Port:	53946
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853593532829498 08/31/22-23:50:12.431169
SID:	2829498
Source Port:	53593
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849334532829498 08/31/22-23:50:15.005623
SID:	2829498
Source Port:	49334
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856434532829500 08/31/22-23:50:42.427928
SID:	2829500
Source Port:	56434
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864966532829498 08/31/22-23:50:19.899743
SID:	2829498
Source Port:	64966
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850345532026737 08/31/22-23:49:17.315311
SID:	2026737
Source Port:	50345

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862769532829498 08/31/22-23:49:54.349513
SID:	2829498
Source Port:	62769
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856297532829500 08/31/22-23:50:22.360506
SID:	2829500
Source Port:	56297
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856125532829498 08/31/22-23:49:24.863671
SID:	2829498
Source Port:	56125
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852819532829500 08/31/22-23:50:07.952331
SID:	2829500
Source Port:	52819
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861174532026737 08/31/22-23:50:41.125728
SID:	2026737
Source Port:	61174
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862041532829498 08/31/22-23:50:38.028308
SID:	2829498
Source Port:	62041
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854908532829500 08/31/22-23:48:50.285779
SID:	2829500
Source Port:	54908
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861091532026737 08/31/22-23:49:53.336151
SID:	2026737
Source Port:	61091
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852720532026737 08/31/22-23:50:01.261421
SID:	2026737
Source Port:	52720
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859340532829500 08/31/22-23:49:59.107861
SID:	2829500
Source Port:	59340
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856090532829500 08/31/22-23:49:06.157622
SID:	2829500
Source Port:	56090
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860131532829498 08/31/22-23:49:54.397250
SID:	2829498
Source Port:	60131
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862226532829498 08/31/22-23:50:03.343591
SID:	2829498
Source Port:	62226
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857326532026737 08/31/22-23:49:34.009679
SID:	2026737
Source Port:	57326
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859341532829500 08/31/22-23:49:59.128177
SID:	2829500
Source Port:	59341

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862735532829500 08/31/22-23:49:54.851676
SID:	2829500
Source Port:	62735
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851889532829498 08/31/22-23:50:24.330289
SID:	2829498
Source Port:	51889
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856436532829500 08/31/22-23:50:42.466214
SID:	2829500
Source Port:	56436
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849336532829498 08/31/22-23:50:15.044470
SID:	2829498
Source Port:	49336
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851323532829500 08/31/22-23:49:50.073092
SID:	2829500
Source Port:	51323
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863266532829500 08/31/22-23:50:03.897271
SID:	2829500
Source Port:	63266
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851776532829498 08/31/22-23:50:06.216035
SID:	2829498
Source Port:	51776
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864800532829500 08/31/22-23:50:34.865341
SID:	2829500
Source Port:	64800
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856550532026737 08/31/22-23:49:08.378525
SID:	2026737
Source Port:	56550
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851892532829498 08/31/22-23:50:24.391367
SID:	2829498
Source Port:	51892
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859338532829500 08/31/22-23:49:59.065543
SID:	2829500
Source Port:	59338
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852846532026737 08/31/22-23:50:18.728478
SID:	2026737
Source Port:	52846
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863673532829500 08/31/22-23:50:38.460458
SID:	2829500
Source Port:	63673
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857519532829498 08/31/22-23:49:46.227969
SID:	2829498
Source Port:	57519
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851532532026737 08/31/22-23:48:55.006743
SID:	2026737
Source Port:	51532

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854203532026737 08/31/22-23:50:33.657267
SID:	2026737
Source Port:	54203
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862038532829498 08/31/22-23:50:37.962895
SID:	2829498
Source Port:	62038
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862540532026737 08/31/22-23:50:35.877444
SID:	2026737
Source Port:	62540
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861094532026737 08/31/22-23:49:53.390900
SID:	2026737
Source Port:	61094
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855959532026737 08/31/22-23:49:42.870749
SID:	2026737
Source Port:	55959
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849470532026737 08/31/22-23:50:44.362254
SID:	2026737
Source Port:	49470
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850256532829498 08/31/22-23:50:34.205420
SID:	2829498
Source Port:	50256
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856429532829498 08/31/22-23:50:42.013339
SID:	2829498
Source Port:	56429
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849469532026737 08/31/22-23:50:44.340126
SID:	2026737
Source Port:	49469
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852868532829500 08/31/22-23:49:26.794257
SID:	2829500
Source Port:	52868
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854905532829500 08/31/22-23:48:50.163893
SID:	2829500
Source Port:	54905
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860000532026737 08/31/22-23:50:04.486610
SID:	2026737
Source Port:	60000
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862851532829500 08/31/22-23:49:39.232388
SID:	2829500
Source Port:	62851
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852485532026737 08/31/22-23:49:02.321191
SID:	2026737
Source Port:	52485
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861614532829500 08/31/22-23:49:00.931789
SID:	2829500
Source Port:	61614

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864545532026737 08/31/22-23:50:11.805562
SID:	2026737
Source Port:	64545
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850346532026737 08/31/22-23:49:17.336643
SID:	2026737
Source Port:	50346
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862853532829500 08/31/22-23:49:39.272143
SID:	2829500
Source Port:	62853
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854205532026737 08/31/22-23:50:33.702038
SID:	2026737
Source Port:	54205
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856361532829500 08/31/22-23:50:13.505571
SID:	2829500
Source Port:	56361
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863675532829500 08/31/22-23:50:38.501186
SID:	2829500
Source Port:	63675
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857517532829498 08/31/22-23:49:46.187199
SID:	2829498
Source Port:	57517
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856091532829500 08/31/22-23:49:06.177940
SID:	2829500
Source Port:	56091
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854300532829500 08/31/22-23:50:47.016428
SID:	2829500
Source Port:	54300
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854907532829500 08/31/22-23:48:50.267487
SID:	2829500
Source Port:	54907
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852848532026737 08/31/22-23:50:18.768533
SID:	2026737
Source Port:	52848
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856088532829500 08/31/22-23:49:06.118498
SID:	2829500
Source Port:	56088
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851325532829500 08/31/22-23:49:50.167078
SID:	2829500
Source Port:	51325
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856300532829500 08/31/22-23:50:22.423249
SID:	2829500
Source Port:	56300
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849236532026737 08/31/22-23:49:22.885858
SID:	2026737
Source Port:	49236

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858161532829500 08/31/22-23:50:17.209347
SID:	2829500
Source Port:	58161
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850254532829498 08/31/22-23:50:34.167189
SID:	2829498
Source Port:	50254
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856753532829498 08/31/22-23:49:57.561313
SID:	2829498
Source Port:	56753
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860694532026737 08/31/22-23:49:57.058875
SID:	2026737
Source Port:	60694
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851535532026737 08/31/22-23:48:55.066318
SID:	2026737
Source Port:	51535
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861612532829500 08/31/22-23:49:00.891035
SID:	2829500
Source Port:	61612
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856432532829498 08/31/22-23:50:42.072023
SID:	2829498
Source Port:	56432
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864965532829498 08/31/22-23:50:19.877923
SID:	2829498
Source Port:	64965
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860002532026737 08/31/22-23:50:04.523120
SID:	2026737
Source Port:	60002
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857324532026737 08/31/22-23:49:33.965954
SID:	2026737
Source Port:	57324
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858921532829500 08/31/22-23:49:15.846001
SID:	2829500
Source Port:	58921
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860692532026737 08/31/22-23:49:57.020058
SID:	2026737
Source Port:	60692
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862542532026737 08/31/22-23:50:35.921513
SID:	2026737
Source Port:	62542
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856126532829498 08/31/22-23:49:24.882022
SID:	2829498
Source Port:	56126
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864964532829498 08/31/22-23:50:19.857963
SID:	2829498
Source Port:	64964

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856298532829500 08/31/22-23:50:22.380545
SID:	2829500
Source Port:	56298
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862768532829498 08/31/22-23:49:54.327766
SID:	2829498
Source Port:	62768
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860003532026737 08/31/22-23:50:04.543015
SID:	2026737
Source Port:	60003
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853595532829498 08/31/22-23:50:12.473746
SID:	2829498
Source Port:	53595
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861092532026737 08/31/22-23:49:53.354265
SID:	2026737
Source Port:	61092
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854298532829500 08/31/22-23:50:46.975693
SID:	2829500
Source Port:	54298
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856433532829500 08/31/22-23:50:42.407533
SID:	2829500
Source Port:	56433
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850347532026737 08/31/22-23:49:17.355597
SID:	2026737
Source Port:	50347
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854299532829500 08/31/22-23:50:46.996273
SID:	2829500
Source Port:	54299
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861172532026737 08/31/22-23:50:41.082366
SID:	2026737
Source Port:	61172
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853594532829498 08/31/22-23:50:12.453787
SID:	2829498
Source Port:	53594
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864406532829498 08/31/22-23:49:37.435154
SID:	2829498
Source Port:	64406
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862542532829498 08/31/22-23:48:47.509378
SID:	2829498
Source Port:	62542
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850257532829498 08/31/22-23:50:34.225599
SID:	2829498
Source Port:	50257
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856299532829500 08/31/22-23:50:22.403218
SID:	2829500
Source Port:	56299

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851890532829498 08/31/22-23:50:24.350751
SID:	2829498
Source Port:	51890
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862541532829498 08/31/22-23:48:47.488892
SID:	2829498
Source Port:	62541
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855961532026737 08/31/22-23:49:42.910756
SID:	2026737
Source Port:	55961
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856755532829498 08/31/22-23:49:57.601932
SID:	2829498
Source Port:	56755
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856127532829498 08/31/22-23:49:24.900788
SID:	2829498
Source Port:	56127
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853197532829498 08/31/22-23:50:30.133681
SID:	2829498
Source Port:	53197
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851533532026737 08/31/22-23:48:55.025305
SID:	2026737
Source Port:	51533
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861093532026737 08/31/22-23:49:53.372548
SID:	2026737
Source Port:	61093
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855633532829498 08/31/22-23:49:19.667081
SID:	2829498
Source Port:	55633
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858162532829500 08/31/22-23:50:17.227551
SID:	2829500
Source Port:	58162
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856431532829498 08/31/22-23:50:42.053871
SID:	2829498
Source Port:	56431
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852870532829500 08/31/22-23:49:26.845476
SID:	2829500
Source Port:	52870
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858159532829500 08/31/22-23:50:17.168323
SID:	2829500
Source Port:	58159
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853046532829500 08/31/22-23:50:24.891150
SID:	2829500
Source Port:	53046
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853043532829500 08/31/22-23:50:24.832633
SID:	2829500
Source Port:	53043

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859884532829498 08/31/22-23:49:13.387386
SID:	2829498
Source Port:	59884
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851367532026737 08/31/22-23:50:14.061249
SID:	2026737
Source Port:	51367
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858919532829500 08/31/22-23:49:15.787076
SID:	2829500
Source Port:	58919
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862737532829500 08/31/22-23:49:54.897559
SID:	2829500
Source Port:	62737
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864651532026737 08/31/22-23:50:23.369931
SID:	2026737
Source Port:	64651
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856572532829500 08/31/22-23:49:21.410257
SID:	2829500
Source Port:	56572
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858922532829500 08/31/22-23:49:15.872217
SID:	2829500
Source Port:	58922
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864546532026737 08/31/22-23:50:11.917623
SID:	2026737
Source Port:	64546
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863268532829500 08/31/22-23:50:03.935068
SID:	2829500
Source Port:	63268
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849467532026737 08/31/22-23:50:44.300593
SID:	2026737
Source Port:	49467
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856089532829500 08/31/22-23:49:06.139177
SID:	2829500
Source Port:	56089
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854882532829498 08/31/22-23:50:45.662904
SID:	2829498
Source Port:	54882
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854512532026737 08/31/22-23:50:27.967773
SID:	2026737
Source Port:	54512
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859339532829500 08/31/22-23:49:59.087833
SID:	2829500
Source Port:	59339
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862770532829498 08/31/22-23:49:54.371674
SID:	2829498
Source Port:	62770

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856752532829498 08/31/22-23:49:57.536553
SID:	2829498
Source Port:	56752
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852719532026737 08/31/22-23:50:01.237344
SID:	2026737
Source Port:	52719
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856362532829500 08/31/22-23:50:13.529988
SID:	2829500
Source Port:	56362
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852820532829500 08/31/22-23:50:08.063038
SID:	2829500
Source Port:	52820
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854204532026737 08/31/22-23:50:33.679529
SID:	2026737
Source Port:	54204
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864409532829498 08/31/22-23:49:37.527288
SID:	2829498
Source Port:	64409
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864543532026737 08/31/22-23:50:11.740058
SID:	2026737
Source Port:	64543
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852483532026737 08/31/22-23:49:02.284760
SID:	2026737
Source Port:	52483
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853948532829498 08/31/22-23:49:04.012398
SID:	2829498
Source Port:	53948
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862224532829498 08/31/22-23:50:03.259743
SID:	2829498
Source Port:	62224
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851326532829500 08/31/22-23:49:50.186179
SID:	2829500
Source Port:	51326
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860012532829500 08/31/22-23:50:33.110094
SID:	2829500
Source Port:	60012
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861611532829500 08/31/22-23:49:00.850076
SID:	2829500
Source Port:	61611
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851364532026737 08/31/22-23:50:13.994431
SID:	2026737
Source Port:	51364
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849235532026737 08/31/22-23:49:22.865636
SID:	2026737
Source Port:	49235

Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Contains functionality to determine the online IP of the system

Found Tor onion address

Uses nslookup.exe to query domains

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands

Yara detected Gandcrab

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

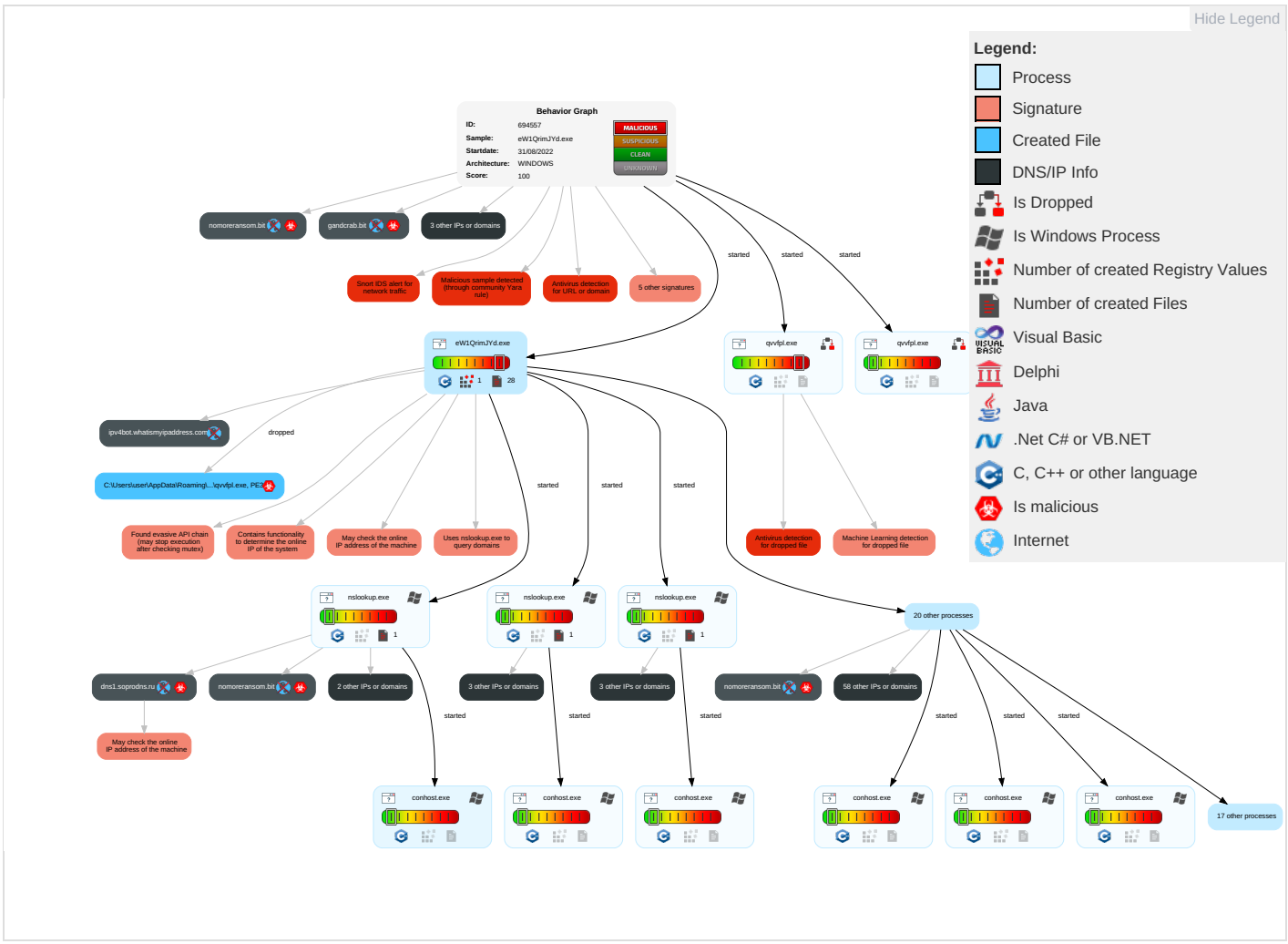
Found evasive API chain (may stop execution after checking mutex)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 2 Native API	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Software Packing	1 Input Capture	1 1 Peripheral Device Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Masquerading	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 System Network Connections Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	4 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Proxy	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	2 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

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
eW1QrimJYd.exe	82%	Virustotal		Browse
eW1QrimJYd.exe	86%	Metadefender		Browse
eW1QrimJYd.exe	100%	ReversingLabs	Win32.Ransomware.GandCrab	
eW1QrimJYd.exe	100%	Avira	TR/FileCoder.oytet	
eW1QrimJYd.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe	100%	Avira	TR/FileCoder.oytet	
C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.qvvfpl.exe.d70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.0.eW1QrimJYd.exe.a80000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.qvvfpl.exe.d70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
24.0.qvvfpl.exe.d70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.2.eW1QrimJYd.exe.a80000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
24.2.qvvfpl.exe.d70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbghvjyqy7jclk.onion.casa/5432c2cfc05a5a97	100%	Avira URL Cloud	malware	
http://gdcbghvjyqy7jclk.onion/5432c2cfc05a5a97	0%	Avira URL Cloud	safe	
http://gdcbghvjyqy7jclk.onion.top/5432c2cfc05a5a97	100%	Avira URL Cloud	phishing	

Domains and IPs

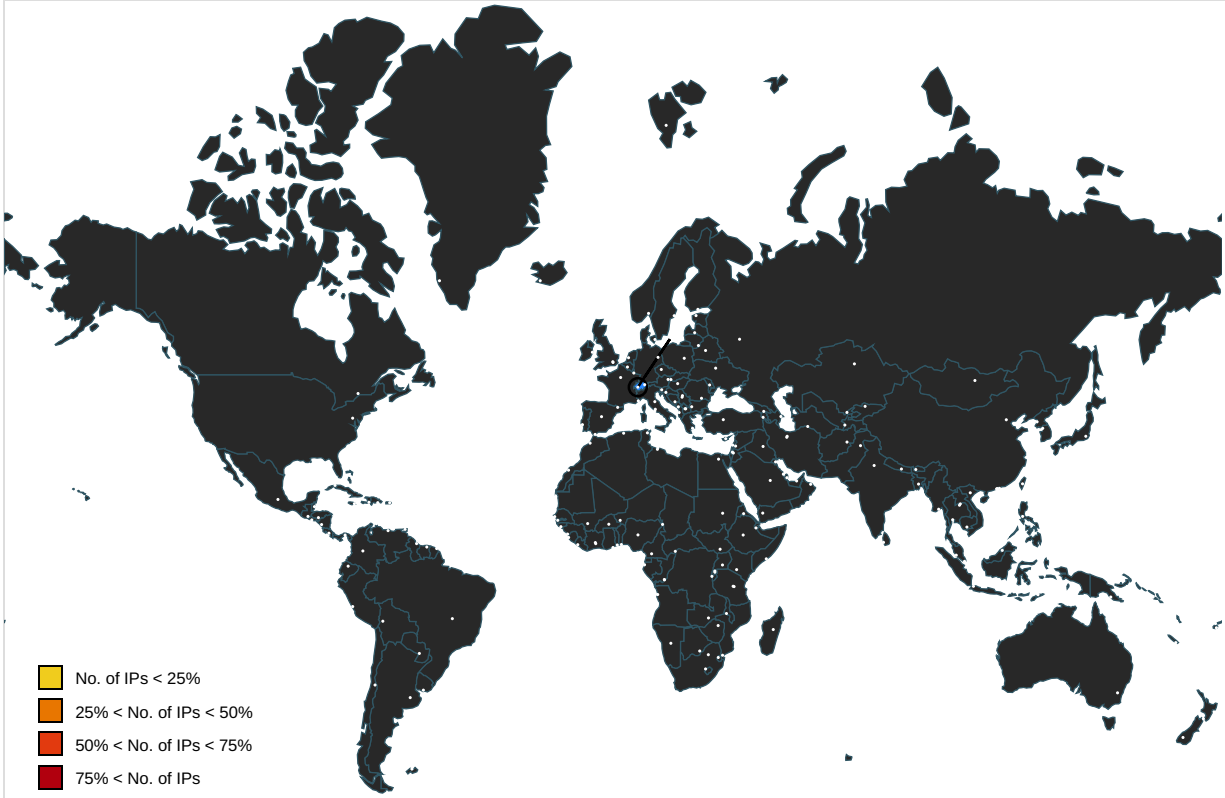
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
emsisoft.bit	unknown	unknown	true		unknown
ipv4bot.whatismyipaddress.com	unknown	unknown	false		high
nomoreransom.bit	unknown	unknown	true		unknown
gandcrab.bit	unknown	unknown	true		unknown
dns1.soprodns.ru	unknown	unknown	true		unknown
8.8.8.8.in-addr.arpa	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gdcbghvjyqy7jclk.onion.guide/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/0	eW1QrimJYd.exe, 00000001.00000002.531861425.00000000008CA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.torproject.org/	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/D	eW1QrimJYd.exe, 00000001.00000002.531861425.00000000008CA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://gdcbghvjyqy7jclk.onion.casa/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: malware	unknown
http://gdcbghvjyqy7jclk.onion.rip/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	eW1QrimJYd.exe, 00000001.00000002.531861425.00000000008CA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://gdcbghvjyqy7jclk.onion/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: safe	unknown
http://gdcbghvjyqy7jclk.onion.plus/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	false		high
http://gdcbghvjyqy7jclk.onion.top/5432c2cfc05a5a97	eW1QrimJYd.exe, 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: phishing	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694557
Start date and time:	2022-08-31 23:47:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eW1QrimJYd.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	63
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.rans.troj.evad.winEXE@110/2@410/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 82%) • Quality average: 70.4% • Quality standard deviation: 36.5%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:48:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce cfbtnelfyrp "C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe"
23:48:47	API Interceptor	61x Sleep call for process: eW1QrimJYd.exe modified
23:48:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce cfbtnelfyrp "C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\eW1QrimJYd.exe
File Type:	data
Category:	dropped
Size (bytes):	2221
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	8882037A0674A329B5AB8C870E58C422
SHA1:	FA2B896CE7908548EB54F6897A57DFCC9A333A49
SHA-256:	BF58499BF43BEC8D41F04779DAC5618A081455A657667C157DE019657224FEAD
SHA-512:	AAE711E67CAB35A320C533B2B939B1C171F9219B4813292F7CE0A64AF785679DDC23DBD61A3D31876558FA19C4E88D3DF845242C2210C226FB5D9D3DAECE681
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe

Process:	C:\Users\user\Desktop\eW1QrimJYd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	75264
Entropy (8bit):	6.466749493074102
Encrypted:	false
SSDEEP:	1536:155u555555555pmgSeGDjtQhnwmmB0ybMqqU+2bbbAV2/S2mr3IdE8mne0Avu5rJ:dMSjOnrmBTMqqDL2/mr3IdE8we0Avu5h
MD5:	E5E0C9F951E9947AEA55720B7D0299F2
SHA1:	9148294CFF65346DAE05816F89AB098028DB1E24
SHA-256:	06F88A3EBA2757CDB84315CEA92091049AE145F299D1A9D856C450CD2A6B42E3
SHA-512:	3A1F47F92D3AD8991A75A07DCE8615ACEC84258E9DBB60E12A621FB6AAAC28589783DA79F1C039D0DC15B637889EF361D130A78AA483A4671058194AA767BEB7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: Joe Security • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: kevoreilly
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....Y...D.us..dvx@ .Z<*.....m<.rrj^....|..(|d.1...^.....:.Gn.^. ..%..(.....e2.i>..a..b.<.QD.....2...T..#Lr.....7..t...Z.&Fv...;).s.,,.e....X?..%..RT.#.!..y$..l..G..]x]8i:.]n.....a.k..@ ..Mj..-a".....8_.....y.w.?PE..L...].vZ.....J.....@.....`.....@.....p.....@.....P..... .....text..... ..`.rdata.....@....data..... .....@....CRT.....0.....@..@.rsrc.....@..... .@..@.reloc.....P.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.466704339730406
TrID:	• Win32 Executable (generic) a (10002005/4) 99.98% • DOS Executable Generic (2002/1) 0.02%
File name:	eW1QrimJYd.exe
File size:	75264
MD5:	b7325e075262ffdeaa68cae94018cadb
SHA1:	2dee9b7321c736f73831ad5bc9be380b7c81680b
SHA256:	88a85792d16b3e48876aa0ea696784d045499a7ba8e7648d9bb7fb27e94b0ad2
SHA512:	0f7b3e11073023eb09bf3b603db80bd133ac9f51d58d64e6a954d0be2c298b0af1221ce5f8e5e31167e5f67037c62d29774db440f906e88c6a357342fce49203
SSDEEP:	1536:a55u555555555pmgSeGDjtQhnwmmB0ybMqqU+2bbbAV2/S2mr3IdE8mne0Avu5rJ:AMSjOnrmBTMqqDL2/mr3IdE8we0Avu5h

TLSH:	DF73391528D08223F6E3F977F5B47DE558397F8817883AEF10A254FA28251D24D39B8E
File Content Preview:	MZ.....Y...D.us..dvx@ .Z<*.....m<.rrj^.....|..(|d.1...^.....:.Gn.^. ...%..(..l.....e2.i>...a..b. <.QD.....2...T..#Lr.....7..t...Z.&Fv...;).s.,,.e.....X?..%..RT.#.!..y$..l..G..]x]8i:.]n.....a.k..@..Mj..-a".....8_.....y.w.?PE..L...].vZ...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404af0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5A76065D [Sat Feb 3 18:58:37 2018 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:	40306b615af659fc1f93cfb121cc38d9

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
call 00007F5D70CA565Dh
push 00000000h
call dword ptr [00409168h]
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 5Ch
push esi
push 00000044h
lea eax, dword ptr [ebp-58h]

Instruction
xorps xmm0, xmm0
push 00000000h
push eax
mov esi, ecx
movdqu dqword ptr [ebp-10h], xmm0
call 00007F5D70CA98B7h
mov eax, dword ptr [00412B0Ch]
add esp, 0Ch
mov dword ptr [ebp-18h], eax
mov dword ptr [ebp-1Ch], eax
mov eax, dword ptr [00412B08h]
or dword ptr [ebp-2Ch], 00000101h
mov dword ptr [ebp-20h], eax
xor eax, eax
mov word ptr [ebp-28h], ax
lea eax, dword ptr [ebp-10h]
push eax
lea eax, dword ptr [ebp-58h]
mov dword ptr [ebp-58h], 00000044h
push eax
push 00000000h
push 00000000h
push 00000000h
push 00000001h
push 00000000h
push 00000000h
push esi
push 00000000h
call dword ptr [00409164h]
test eax, eax
jne 00007F5D70CA58BDh
call dword ptr [00409064h]
pop esi
mov esp, ebp
pop ebp
ret
push dword ptr [ebp-10h]
mov esi, dword ptr [0040910Ch]
call esi
push dword ptr [ebp-0Ch]
call esi
pop esi
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 10h
movq xmm0, qword ptr [0040FF2Ch]
mov al, byte ptr [0040FF34h]
push ebx
mov ebx, dword ptr [ebp+08h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10970	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15000	0xab0	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8000	0x8000	False	0.448028564453125	data	6.296861858288883	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x9000	0x8600	False	0.45848880597014924	data	6.1322099086141595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.data	0x12000	0x1000	0xc00	False	0.25390625	data	3.450195070880191	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x13000	0x1000	0x200	False	0.03125	UTF-8 Unicode text, with no line terminators	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1000	0x200	False	0.52734375	data	4.710061382693063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15000	0x1000	0xc00	False	0.7750651041666666	data	6.434410350416442	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x14060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFilePointer, GetFileAttributesW, ReadFile, GetLastError, MoveFileW, lstrcpyW, SetFileAttributesW, CreateMutexW, GetDriveTypeW, VerSetConditionMask, WaitForSingleObject, GetTickCount, InitializeCriticalSection, OpenProcess, GetSystemDirectoryW, TerminateThread, Sleep, TerminateProcess, VerifyVersionInfoW, WaitForMultipleObjects, DeleteCriticalSection, ExpandEnvironmentStringsW, lstrlenW, SetHandleInformation, lstrcatA, MultiByteToWideChar, CreatePipe, lstrcmpiA, Process32NextW, CreateToolhelp32Snapshot, LeaveCriticalSection, EnterCriticalSection, FindFirstFileW, lstrcmpW, FindClose, FindNextFileW, GetNativeSystemInfo, GetComputerNameW, GetDiskFreeSpaceW, GetWindowsDirectoryW, GetVolumeInformationW, LoadLibraryA, lstrcmpiW, VirtualFree, CreateThread, CloseHandle, lstrcatW, CreateFileMappingW, ExitThread, CreateFileW, GetModuleFileNameW, WriteFile, GetModuleHandleW, UnmapViewOfFile, MapViewOfFile, GetFileSize, GetEnvironmentVariableW, lstrcpyA, GetModuleHandleA, VirtualAlloc, Process32FirstW, GetTempPathW, GetProcAddress, GetProcessHeap, HeapFree, HeapAlloc, lstrlenA, CreateProcessW, ExitProcess, IsProcessorFeaturePresent
USER32.dll	wsprintfW, TranslateMessage, RegisterClassExW, LoadIconW, SetWindowLongW, EndPaint, BeginPaint, LoadCursorW, GetMessageW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, GetForegroundWindow, DestroyWindow
GDI32.dll	TextOutW
ADVAPI32.dll	CryptExportKey, AllocateAndInitializeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, FreeSid

DLL	Import
SHELL32.dll	SHGetSpecialFolderPathW, ShellExecuteExW, ShellExecuteW
CRYPT32.dll	CryptStringToBinaryA, CryptBinaryToStringA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8606955 32026737 08/31/22-23:49:57.078873	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60695	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8646495 32026737 08/31/22-23:50:23.329807	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64649	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8502555 32829498 08/31/22-23:50:34.185397	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50255	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8620395 32829498 08/31/22-23:50:37.987567	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62039	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8575185 32829498 08/31/22-23:49:46.207614	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57518	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494685 32026737 08/31/22-23:50:44.319184	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49468	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565715 32829500 08/31/22-23:49:21.389711	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56571	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8636745 32829500 08/31/22-23:50:38.481064	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63674	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8616135 32829500 08/31/22-23:49:00.911463	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61613	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8541975 32829500 08/31/22-23:50:08.085752	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54197	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8611755 32026737 08/31/22-23:50:41.147699	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61175	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513245 32829500 08/31/22-23:49:50.142801	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51324	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8524865 32026737 08/31/22-23:49:02.339569	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52486	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8493355 32829498 08/31/22-23:50:15.024115	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49335	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8518915 32829498 08/31/22-23:50:24.371077	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51891	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8645445 32026737 08/31/22-23:50:11.785305	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64544	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8539455 32829498 08/31/22-23:49:03.940196	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53945	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8628525 32829500 08/31/22-23:49:39.251383	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62852	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8549065 32829500 08/31/22-23:48:50.247066	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54906	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528695 32829500 08/31/22-23:49:26.819001	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52869	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8563605 32829500 08/31/22-23:50:13.477447	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56360	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8573275 32026737 08/31/22-23:49:34.029795	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57327	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8646525 32026737 08/31/22-23:50:23.390728	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64652	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528475 32026737 08/31/22-23:50:18.746734	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52847	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8628505 32829500 08/31/22-23:49:39.210928	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62850	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8531985 32829498 08/31/22-23:50:30.152335	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53198	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8644085 32829498 08/31/22-23:49:37.493948	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64408	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528455 32026737 08/31/22-23:50:18.663879	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52845	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8611735 32026737 08/31/22-23:50:41.105316	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61173	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564355 32829500 08/31/22-23:50:42.448009	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56435	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8632655 32829500 08/31/22-23:50:03.877266	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63265	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528185 32829500 08/31/22-23:50:07.911995	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52818	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8531955 32829498 08/31/22-23:50:29.933502	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53195	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565515 32026737 08/31/22-23:49:08.399946	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56551	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8517775 32829498 08/31/22-23:50:06.235822	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51777	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8648015 32829500 08/31/22-23:50:34.885486	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	64801	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627345 32829500 08/31/22-23:49:54.828233	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62734	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8524845 32026737 08/31/22-23:49:02.302880	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52484	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8559585 32026737 08/31/22-23:49:42.850589	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55958	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8636725 32829500 08/31/22-23:50:38.440019	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63672	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8492345 32026737 08/31/22-23:49:22.846612	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49234	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8548815 32829498 08/31/22-23:50:45.644561	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54881	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528675 32829500 08/31/22-23:49:26.766420	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52867	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600115 32829500 08/31/22-23:50:33.089754	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60011	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513655 32026737 08/31/22-23:50:14.017877	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51365	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8632675 32829500 08/31/22-23:50:03.917309	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63267	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8561245 32829498 08/31/22-23:48:57.941241	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56124	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8620405 32829498 08/31/22-23:50:38.007802	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62040	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8646505 32026737 08/31/22-23:50:23.349894	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64650	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627365 32829500 08/31/22-23:49:54.873826	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62736	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8622255 32829498 08/31/22-23:50:03.325419	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62225	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600135 32829500 08/31/22-23:50:33.131001	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60013	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8548835 32829498 08/31/22-23:50:45.681352	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54883	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8535925 32829498 08/31/22-23:50:12.408515	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53592	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8563635 32829500 08/31/22-23:50:13.551243	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56363	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8517755 32829498 08/31/22-23:50:06.195982	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51775	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8598835 32829498 08/31/22-23:49:13.365736	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59883	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8545135 32026737 08/31/22-23:50:28.034455	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54513	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8556345 32829498 08/31/22-23:49:19.687489	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55634	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565745 32829500 08/31/22-23:49:21.461712	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56574	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8567545 32829498 08/31/22-23:49:57.581695	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56754	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8539475 32829498 08/31/22-23:49:03.979774	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53947	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8545105 32026737 08/31/22-23:50:25.933530	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54510	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8559605 32026737 08/31/22-23:49:42.892259	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55960	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8647995 32829500 08/31/22-23:50:34.845123	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	64799	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625395 32026737 08/31/22-23:50:35.857432	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62539	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8598855 32829498 08/31/22-23:49:13.407922	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59885	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8556325 32829498 08/31/22-23:49:19.646853	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55632	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8644075 32829498 08/31/22-23:49:37.460209	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64407	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8531965 32829498 08/31/22-23:50:30.011263	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53196	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565495 32026737 08/31/22-23:49:08.357396	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56549	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8589205 32829500 08/31/22-23:49:15.820662	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58920	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8530445 32829500 08/31/22-23:50:24.850862	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53044	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8515345 32026737 08/31/22-23:48:55.046078	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51534	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8581605 32829500 08/31/22-23:50:17.191071	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58160	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8527185 32026737 08/31/22-23:50:01.216655	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52718	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8622235 32829498 08/31/22-23:50:03.241400	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62223	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8530455 32829500 08/31/22-23:50:24.871066	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53045	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8503485 32026737 08/31/22-23:49:17.376161	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50348	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8606935 32026737 08/31/22-23:49:57.038533	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60693	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8649635 32829498 08/31/22-23:50:19.837606	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64963	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8647985 32829500 08/31/22-23:50:34.824859	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	64798	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8545115 32026737 08/31/22-23:50:27.946240	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54511	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8527175 32026737 08/31/22-23:50:01.196442	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52717	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565525 32026737 08/31/22-23:49:08.420766	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56552	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513665 32026737 08/31/22-23:50:14.041221	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51366	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600105 32829500 08/31/22-23:50:33.071442	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60010	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564305 32829498 08/31/22-23:50:42.033912	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56430	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565735 32829500 08/31/22-23:49:21.437590	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56573	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8598865 32829498 08/31/22-23:49:13.428276	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59886	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8556315 32829498 08/31/22-23:49:19.625742	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55631	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8542025 32026737 08/31/22-23:50:33.636817	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54202	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8543015 32829500 08/31/22-23:50:47.037037	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54301	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8517745 32829498 08/31/22-23:50:06.176893	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51774	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8548845 32829498 08/31/22-23:50:45.706056	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54884	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8492375 32026737 08/31/22-23:49:22.906523	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49237	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8575205 32829498 08/31/22-23:49:46.246339	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57520	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8561285 32829498 08/31/22-23:49:24.926548	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56128	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625415 32026737 08/31/22-23:50:35.901068	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62541	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8493375 32829498 08/31/22-23:50:15.074780	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49337	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625435 32829498 08/31/22-23:48:47.529672	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62543	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600015 32026737 08/31/22-23:50:04.504698	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60001	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625405 32829498 08/31/22-23:48:47.468455	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62540	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8573255 32026737 08/31/22-23:49:33.986496	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57325	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8539465 32829498 08/31/22-23:49:03.959032	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53946	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8535935 32829498 08/31/22-23:50:12.431169	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53593	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8493345 32829498 08/31/22-23:50:15.005623	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49334	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564345 32829500 08/31/22-23:50:42.427928	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56434	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8649665 32829498 08/31/22-23:50:19.899743	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64966	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8503455 32026737 08/31/22-23:49:17.315311	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50345	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627695 32829498 08/31/22-23:49:54.349513	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62769	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8562975 32829500 08/31/22-23:50:22.360506	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56297	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8561255 32829498 08/31/22-23:49:24.863671	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56125	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528195 32829500 08/31/22-23:50:07.952331	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52819	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8611745 32026737 08/31/22-23:50:41.125728	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61174	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8620415 32829498 08/31/22-23:50:38.028308	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62041	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8549085 32829500 08/31/22-23:48:50.285779	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54908	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8610915 32026737 08/31/22-23:49:53.336151	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61091	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8527205 32026737 08/31/22-23:50:01.261421	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52720	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8593405 32829500 08/31/22-23:49:59.107861	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59340	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8560905 32829500 08/31/22-23:49:06.157622	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56090	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8601315 32829498 08/31/22-23:49:54.397250	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60131	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8622265 32829498 08/31/22-23:50:03.343591	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62226	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8573265 32026737 08/31/22-23:49:34.009679	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57326	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8593415 32829500 08/31/22-23:49:59.128177	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59341	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627355 32829500 08/31/22-23:49:54.851676	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62735	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8518895 32829498 08/31/22-23:50:24.330289	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51889	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564365 32829500 08/31/22-23:50:42.466214	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56436	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8493365 32829498 08/31/22-23:50:15.044470	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49336	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513235 32829500 08/31/22-23:49:50.073092	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51323	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8632665 32829500 08/31/22-23:50:03.897271	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63266	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8517765 32829498 08/31/22-23:50:06.216035	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51776	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8648005 32829500 08/31/22-23:50:34.865341	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	64800	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565505 32026737 08/31/22-23:49:08.378525	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56550	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8518925 32829498 08/31/22-23:50:24.391367	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51892	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8593385 32829500 08/31/22-23:49:59.065543	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59338	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528465 32026737 08/31/22-23:50:18.728478	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52846	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8636735 32829500 08/31/22-23:50:38.460458	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63673	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8575195 32829498 08/31/22-23:49:46.227969	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57519	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8515325 32026737 08/31/22-23:48:55.006743	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51532	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8542035 32026737 08/31/22-23:50:33.657267	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54203	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8620385 32829498 08/31/22-23:50:37.962895	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62038	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625405 32026737 08/31/22-23:50:35.877444	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62540	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8610945 32026737 08/31/22-23:49:53.390900	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61094	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8559595 32026737 08/31/22-23:49:42.870749	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55959	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494705 32026737 08/31/22-23:50:44.362254	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49470	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8502565 32829498 08/31/22-23:50:34.205420	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50256	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564295 32829498 08/31/22-23:50:42.013339	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56429	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494695 32026737 08/31/22-23:50:44.340126	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49469	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528685 32829500 08/31/22-23:49:26.794257	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52868	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8549055 32829500 08/31/22-23:48:50.163893	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54905	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600005 32026737 08/31/22-23:50:04.486610	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60000	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8628515 32829500 08/31/22-23:49:39.232388	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62851	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8524855 32026737 08/31/22-23:49:02.321191	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52485	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8616145 32829500 08/31/22-23:49:00.931789	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61614	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8645455 32026737 08/31/22-23:50:11.805562	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64545	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8503465 32026737 08/31/22-23:49:17.336643	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50346	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8628535 32829500 08/31/22-23:49:39.272143	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62853	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8542055 32026737 08/31/22-23:50:33.702038	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54205	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8563615 32829500 08/31/22-23:50:13.505571	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56361	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8636755 32829500 08/31/22-23:50:38.501186	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63675	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8575175 32829498 08/31/22-23:49:46.187199	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57517	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8560915 32829500 08/31/22-23:49:06.177940	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56091	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8543005 32829500 08/31/22-23:50:47.016428	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54300	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8549075 32829500 08/31/22-23:48:50.267487	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54907	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528485 32026737 08/31/22-23:50:18.768533	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52848	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8560885 32829500 08/31/22-23:49:06.118498	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56088	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513255 32829500 08/31/22-23:49:50.167078	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51325	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8563005 32829500 08/31/22-23:50:22.423249	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56300	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8492365 32026737 08/31/22-23:49:22.885858	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49236	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8581615 32829500 08/31/22-23:50:17.209347	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58161	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8502545 32829498 08/31/22-23:50:34.167189	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50254	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8567535 32829498 08/31/22-23:49:57.561313	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56753	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8606945 32026737 08/31/22-23:49:57.058875	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60694	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8515355 32026737 08/31/22-23:48:55.066318	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51535	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8616125 32829500 08/31/22-23:49:00.891035	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61612	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564325 32829498 08/31/22-23:50:42.072023	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56432	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8649655 32829498 08/31/22-23:50:19.877923	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64965	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600025 32026737 08/31/22-23:50:04.523120	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60002	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8573245 32026737 08/31/22-23:49:33.965954	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57324	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8589215 32829500 08/31/22-23:49:15.846001	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58921	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8606925 32026737 08/31/22-23:49:57.020058	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60692	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625425 32026737 08/31/22-23:50:35.921513	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62542	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8561265 32829498 08/31/22-23:49:24.882022	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56126	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8649645 32829498 08/31/22-23:50:19.857963	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64964	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8562985 32829500 08/31/22-23:50:22.380545	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56298	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627685 32829498 08/31/22-23:49:54.327766	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62768	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8600035 32026737 08/31/22-23:50:04.543015	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60003	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8535955 32829498 08/31/22-23:50:12.473746	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53595	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8610925 32026737 08/31/22-23:49:53.354265	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61092	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8542985 32829500 08/31/22-23:50:46.975693	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54298	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8564335 32829500 08/31/22-23:50:42.407533	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56433	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8503475 32026737 08/31/22-23:49:17.355597	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50347	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8542995 32829500 08/31/22-23:50:46.996273	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	54299	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8611725 32026737 08/31/22-23:50:41.082366	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61172	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8535945 32829498 08/31/22-23:50:12.453787	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53594	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8644065 32829498 08/31/22-23:49:37.435154	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64406	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625425 32829498 08/31/22-23:48:47.509378	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62542	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8502575 32829498 08/31/22-23:50:34.225599	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50257	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8562995 32829500 08/31/22-23:50:22.403218	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56299	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8518905 32829498 08/31/22-23:50:24.350751	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51890	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8625415 32829498 08/31/22-23:48:47.488892	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62541	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8559615 32026737 08/31/22-23:49:42.910756	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55961	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8567555 32829498 08/31/22-23:49:57.601932	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56755	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8561275 32829498 08/31/22-23:49:24.900788	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56127	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8531975 32829498 08/31/22-23:50:30.133681	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53197	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8515335 32026737 08/31/22-23:48:55.025305	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51533	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8610935 32026737 08/31/22-23:49:53.372548	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	61093	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8556335 32829498 08/31/22-23:49:19.667081	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55633	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8581625 32829500 08/31/22-23:50:17.227551	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58162	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8564315 32829498 08/31/22-23:50:42.053871	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56431	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528705 32829500 08/31/22-23:49:26.845476	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52870	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8581595 32829500 08/31/22-23:50:17.168323	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58159	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8530465 32829500 08/31/22-23:50:24.891150	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53046	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8530435 32829500 08/31/22-23:50:24.832633	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53043	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8598845 32829498 08/31/22-23:49:13.387386	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59884	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8513675 32026737 08/31/22-23:50:14.061249	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51367	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8589195 32829500 08/31/22-23:49:15.787076	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58919	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627375 32829500 08/31/22-23:49:54.897559	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62737	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8646515 32026737 08/31/22-23:50:23.369931	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64651	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565725 32829500 08/31/22-23:49:21.410257	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56572	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8589225 32829500 08/31/22-23:49:15.872217	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58922	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8645465 32026737 08/31/22-23:50:11.917623	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64546	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8632685 32829500 08/31/22-23:50:03.935068	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63268	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494675 32026737 08/31/22-23:50:44.300593	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49467	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8560895 32829500 08/31/22-23:49:06.139177	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56089	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8548825 32829498 08/31/22-23:50:45.662904	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54882	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8545125 32026737 08/31/22-23:50:27.967773	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54512	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8593395 32829500 08/31/22-23:49:59.087833	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59339	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8627705 32829498 08/31/22-23:49:54.371674	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62770	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8567525 32829498 08/31/22-23:49:57.536553	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56752	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8527195 32026737 08/31/22-23:50:01.237344	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52719	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8563625 32829500 08/31/22-23:50:13.529988	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	56362	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528205 32829500 08/31/22-23:50:08.063038	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52820	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8542045 32026737 08/31/22-23:50:33.679529	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54204	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8644095 32829498 08/31/22-23:49:37.527288	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64409	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8645435 32026737 08/31/22-23:50:11.740058	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64543	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8524835 32026737 08/31/22-23:49:02.284760	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52483	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8539485 32829498 08/31/22-23:49:04.012398	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53948	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8622245 32829498 08/31/22-23:50:03.259743	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62224	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513265 32829500 08/31/22-23:49:50.186179	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51326	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8600125 32829500 08/31/22-23:50:33.110094	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60012	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8616115 32829500 08/31/22-23:49:00.850076	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61611	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8513645 32026737 08/31/22-23:50:13.994431	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	51364	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8492355 32026737 08/31/22-23:49:22.865636	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49235	53	192.168.2.6	8.8.8.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:44.116539001 CEST	63229	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:44.136054039 CEST	53	63229	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:45.117125034 CEST	62538	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:46.120923042 CEST	62538	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.148174047 CEST	62538	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.429773092 CEST	53	62538	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:47.446198940 CEST	62539	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.465388060 CEST	53	62539	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:47.468455076 CEST	62540	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.488225937 CEST	53	62540	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:47.488892078 CEST	62541	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.508804083 CEST	53	62541	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:47.509377956 CEST	62542	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.529036045 CEST	53	62542	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:47.529671907 CEST	62543	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:47.549340963 CEST	53	62543	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:48.691446066 CEST	54903	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:49.264957905 CEST	53	62538	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:49.961707115 CEST	54903	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:49.988116026 CEST	53	54903	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.135879040 CEST	53	62538	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.144049883 CEST	54904	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:50.163110971 CEST	53	54904	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.163892984 CEST	54905	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:50.183588028 CEST	53	54905	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.247066021 CEST	54906	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:50.266885042 CEST	53	54906	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.267487049 CEST	54907	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:50.285155058 CEST	53	54907	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:50.285778999 CEST	54908	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:50.305613995 CEST	53	54908	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:53.708446980 CEST	53	54903	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:54.912518978 CEST	51530	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:54.940237045 CEST	53	51530	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:54.986932039 CEST	51531	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:55.005909920 CEST	53	51531	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:55.006742954 CEST	51532	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:55.024481058 CEST	53	51532	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:55.025305033 CEST	51533	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:55.044683933 CEST	53	51533	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:55.046077967 CEST	51534	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:55.065548897 CEST	53	51534	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:55.066318035 CEST	51535	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:55.085766077 CEST	53	51535	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:56.292723894 CEST	56122	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:57.294055939 CEST	56122	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:57.871090889 CEST	53	56122	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:57.923278093 CEST	56123	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:57.940429926 CEST	53	56123	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:57.941241026 CEST	56124	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:57.961014986 CEST	53	56124	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:57.961649895 CEST	56125	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:57.979434013 CEST	53	56125	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:57.979980946 CEST	56126	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:57.997720003 CEST	53	56126	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:58.002645016 CEST	56127	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:58.020783901 CEST	53	56127	8.8.8.8	192.168.2.6
Aug 31, 2022 23:48:59.203073978 CEST	52556	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:48:59.563860893 CEST	53	56122	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.248944044 CEST	52556	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.778501987 CEST	53	52556	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.827044010 CEST	61610	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.846194029 CEST	53	61610	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.850075960 CEST	61611	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.870034933 CEST	53	61611	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.891035080 CEST	61612	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.910629988 CEST	53	61612	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.911463022 CEST	61613	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.930983067 CEST	53	61613	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:00.931788921 CEST	61614	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:00.951646090 CEST	53	61614	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:01.369014978 CEST	53	52556	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.198327065 CEST	52481	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.226392031 CEST	53	52481	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.264911890 CEST	52482	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.283921003 CEST	53	52482	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.284759998 CEST	52483	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.302268028 CEST	53	52483	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.302880049 CEST	52484	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.320642948 CEST	53	52484	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.321191072 CEST	52485	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.338948965 CEST	53	52485	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:02.339569092 CEST	52486	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:02.359249115 CEST	53	52486	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:03.829682112 CEST	53943	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:03.865678072 CEST	53	53943	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:03.922105074 CEST	53944	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:03.939187050 CEST	53	53944	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:03.940196037 CEST	53945	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:03.958033085 CEST	53	53945	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:03.959032059 CEST	53946	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:03.978843927 CEST	53	53946	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:03.979773998 CEST	53947	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:03.997428894 CEST	53	53947	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:04.012398005 CEST	53948	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:04.032171965 CEST	53	53948	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:05.030595064 CEST	56086	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.028855085 CEST	56086	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.064717054 CEST	53	56086	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.098314047 CEST	56087	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.117698908 CEST	53	56087	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.118498087 CEST	56088	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.138461113 CEST	53	56088	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.139177084 CEST	56089	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:49:06.157145977 CEST	53	56089	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.157622099 CEST	56090	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.177340984 CEST	53	56090	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.177939892 CEST	56091	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:06.195765972 CEST	53	56091	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:06.744250059 CEST	53	56086	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:07.180340052 CEST	56547	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.172979116 CEST	56547	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.292459011 CEST	53	56547	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.337205887 CEST	56548	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.356190920 CEST	53	56548	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.357395887 CEST	56549	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.376708031 CEST	53	56549	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.378525019 CEST	56550	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.397835970 CEST	53	56550	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.399945974 CEST	56551	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.418164968 CEST	53	56551	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.420766115 CEST	56552	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:08.440345049 CEST	53	56552	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:08.824318886 CEST	53	56547	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:11.635112047 CEST	59881	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:12.929991007 CEST	59881	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.306567907 CEST	53	59881	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:13.344588995 CEST	59882	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.364543915 CEST	53	59882	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:13.365736008 CEST	59883	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.386758089 CEST	53	59883	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:13.387386084 CEST	59884	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.407160044 CEST	53	59884	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:13.407922029 CEST	59885	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.427547932 CEST	53	59885	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:13.428276062 CEST	59886	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:13.445738077 CEST	53	59886	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:14.049354076 CEST	53	59881	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:14.604439974 CEST	58917	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.610282898 CEST	58917	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.732141018 CEST	53	58917	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:15.762787104 CEST	58918	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.786143064 CEST	53	58918	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:15.787075996 CEST	58919	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.810261011 CEST	53	58919	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:15.820662022 CEST	58920	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.845424891 CEST	53	58920	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:15.846000910 CEST	58921	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.871382952 CEST	53	58921	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:15.872216940 CEST	58922	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:15.897437096 CEST	53	58922	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:16.308988094 CEST	53	58917	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.166126013 CEST	50343	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:17.240441084 CEST	53	50343	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.297399998 CEST	50344	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:17.314428091 CEST	53	50344	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.315310955 CEST	50345	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:17.335490942 CEST	53	50345	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.336642981 CEST	50346	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:17.354706049 CEST	53	50346	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.355597019 CEST	50347	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:17.375117064 CEST	53	50347	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:17.376161098 CEST	50348	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:49:17.394150019 CEST	53	50348	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:18.439655066 CEST	62520	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.436444044 CEST	62520	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.552881956 CEST	53	62520	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.605516911 CEST	55630	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.624495029 CEST	53	55630	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.625741959 CEST	55631	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.646193027 CEST	53	55631	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.646852970 CEST	55632	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.666341066 CEST	53	55632	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.667081118 CEST	55633	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.686774969 CEST	53	55633	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.687489033 CEST	55634	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:19.706923962 CEST	53	55634	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:19.966856956 CEST	53	62520	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:20.744438887 CEST	52079	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.322283030 CEST	53	52079	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:21.364559889 CEST	56570	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.388284922 CEST	53	56570	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:21.389710903 CEST	56571	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.409245014 CEST	53	56571	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:21.410257101 CEST	56572	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.428335905 CEST	53	56572	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:21.437589884 CEST	56573	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.460988045 CEST	53	56573	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:21.461711884 CEST	56574	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:21.481684923 CEST	53	56574	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.729974031 CEST	49232	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.802742958 CEST	53	49232	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.828344107 CEST	49233	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.845546007 CEST	53	49233	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.846611977 CEST	49234	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.864109993 CEST	53	49234	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.865636110 CEST	49235	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.885181904 CEST	53	49235	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.885858059 CEST	49236	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.905694008 CEST	53	49236	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:22.906522989 CEST	49237	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:22.924313068 CEST	53	49237	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.181659937 CEST	56123	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.794177055 CEST	53	56123	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.843636036 CEST	56124	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.862725973 CEST	53	56124	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.863671064 CEST	56125	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.881535053 CEST	53	56125	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.882021904 CEST	56126	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.900017977 CEST	53	56126	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.900788069 CEST	56127	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.918819904 CEST	53	56127	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:24.926548004 CEST	56128	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:24.944628000 CEST	53	56128	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:26.173096895 CEST	52865	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.704699039 CEST	53	52865	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:26.742422104 CEST	52866	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.762280941 CEST	53	52866	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:26.766419888 CEST	52867	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.786171913 CEST	53	52867	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:26.794256926 CEST	52868	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.815588951 CEST	53	52868	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:49:26.819000959 CEST	52869	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.840948105 CEST	53	52869	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:26.845475912 CEST	52870	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:26.868755102 CEST	53	52870	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:32.760355949 CEST	57322	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:33.801712990 CEST	57322	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:33.918472052 CEST	53	57322	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:33.948062897 CEST	57323	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:33.965091944 CEST	53	57323	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:33.965954065 CEST	57324	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:33.985773087 CEST	53	57324	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:33.986495972 CEST	57325	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:34.008980036 CEST	53	57325	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:34.009679079 CEST	57326	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:34.029289961 CEST	53	57326	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:34.029794931 CEST	57327	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:34.047578096 CEST	53	57327	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:34.840379000 CEST	53	57322	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:35.228359938 CEST	62958	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:36.246831894 CEST	62958	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.234587908 CEST	62958	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.368525028 CEST	53	62958	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.414644003 CEST	64405	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.434192896 CEST	53	64405	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.435153961 CEST	64406	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.455080986 CEST	53	64406	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.460208893 CEST	64407	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.479908943 CEST	53	64407	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.493947983 CEST	64408	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.513475895 CEST	53	64408	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.527287960 CEST	64409	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:37.546905994 CEST	53	64409	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:37.804033995 CEST	53	62958	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:38.629677057 CEST	62848	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.158519983 CEST	53	62848	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.190716982 CEST	62849	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.209886074 CEST	53	62849	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.210927963 CEST	62850	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.228986025 CEST	53	62850	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.232388020 CEST	62851	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.250422955 CEST	53	62851	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.251383066 CEST	62852	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.270978928 CEST	53	62852	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.272142887 CEST	62853	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:39.291903973 CEST	53	62853	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:39.578844070 CEST	53	62958	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:40.533377886 CEST	55956	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:41.548500061 CEST	55956	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.563077927 CEST	55956	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.803582907 CEST	53	55956	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:42.830462933 CEST	55957	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.849625111 CEST	53	55957	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:42.850589037 CEST	55958	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.870042086 CEST	53	55958	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:42.870748997 CEST	55959	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.890347004 CEST	53	55959	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:42.892258883 CEST	55960	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:42.910130978 CEST	53	55960	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:42.910756111 CEST	55961	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:49:42.930283070 CEST	53	55961	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:43.727183104 CEST	53	55956	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:43.926912069 CEST	57515	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:44.304563046 CEST	53	55956	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:44.985625029 CEST	57515	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:45.985445023 CEST	57515	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.151169062 CEST	53	57515	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:46.167262077 CEST	57516	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.186392069 CEST	53	57516	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:46.187199116 CEST	57517	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.206867933 CEST	53	57517	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:46.207613945 CEST	57518	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.227328062 CEST	53	57518	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:46.227968931 CEST	57519	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.245661020 CEST	53	57519	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:46.246339083 CEST	57520	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:46.263768911 CEST	53	57520	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:47.143296003 CEST	53	57515	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:47.290848970 CEST	51321	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:48.499587059 CEST	51321	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:48.946257114 CEST	53	57515	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:49.671741962 CEST	53	51321	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:49.956358910 CEST	51321	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.028801918 CEST	53	51321	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:50.054864883 CEST	51322	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.072125912 CEST	53	51322	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:50.073091984 CEST	51323	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.094736099 CEST	53	51323	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:50.142801046 CEST	51324	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.160806894 CEST	53	51324	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:50.167078018 CEST	51325	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.185210943 CEST	53	51325	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:50.186178923 CEST	51326	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:50.206547022 CEST	53	51326	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:52.308414936 CEST	53	51321	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:52.769992113 CEST	61089	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.300184965 CEST	53	61089	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.309271097 CEST	61090	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.328352928 CEST	53	61090	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.336150885 CEST	61091	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.353754044 CEST	53	61091	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.354264975 CEST	61092	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.372015953 CEST	53	61092	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.372548103 CEST	61093	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.390347004 CEST	53	61093	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.390899897 CEST	61094	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:53.411127090 CEST	53	61094	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:53.746059895 CEST	62766	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.282331944 CEST	53	62766	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.293313026 CEST	62767	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.312721014 CEST	53	62767	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.327765942 CEST	62768	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.346045017 CEST	53	62768	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.349513054 CEST	62769	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.369218111 CEST	53	62769	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.371674061 CEST	62770	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.389324903 CEST	53	62770	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.397249937 CEST	60131	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.415669918 CEST	53	60131	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:49:54.752284050 CEST	62732	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.786828041 CEST	53	62732	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.810272932 CEST	62733	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.827580929 CEST	53	62733	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.828233004 CEST	62734	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.848042965 CEST	53	62734	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.851675987 CEST	62735	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.871623039 CEST	53	62735	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.873826027 CEST	62736	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.893619061 CEST	53	62736	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:54.897558928 CEST	62737	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:54.917089939 CEST	53	62737	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:55.329066992 CEST	60690	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:56.358541012 CEST	60690	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:56.991584063 CEST	53	60690	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.000348091 CEST	60691	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.019478083 CEST	53	60691	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.020057917 CEST	60692	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.038048983 CEST	53	60692	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.038532972 CEST	60693	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.058454990 CEST	53	60693	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.058875084 CEST	60694	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.078458071 CEST	53	60694	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.078872919 CEST	60695	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.096430063 CEST	53	60695	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.445333958 CEST	56750	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.489593983 CEST	53	56750	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.516345978 CEST	56751	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.535823107 CEST	53	56751	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.536552906 CEST	56752	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.556433916 CEST	53	56752	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.561312914 CEST	56753	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.581238985 CEST	53	56753	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.581695080 CEST	56754	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.601391077 CEST	53	56754	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.601932049 CEST	56755	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:57.621717930 CEST	53	56755	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:57.951314926 CEST	59336	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:58.940262079 CEST	59336	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.038297892 CEST	53	59336	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.045651913 CEST	59337	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.064886093 CEST	53	59337	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.065542936 CEST	59338	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.085707903 CEST	53	59338	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.087832928 CEST	59339	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.107444048 CEST	53	59339	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.107861042 CEST	59340	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.127703905 CEST	53	59340	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.128176928 CEST	59341	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.148261070 CEST	53	59341	8.8.8.8	192.168.2.6
Aug 31, 2022 23:49:59.493012905 CEST	52715	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:49:59.514354944 CEST	53	59336	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:00.513597965 CEST	52715	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.090209007 CEST	53	52715	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.166991949 CEST	53	52715	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.178349018 CEST	52716	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.195605040 CEST	53	52716	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.196441889 CEST	52717	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.216135979 CEST	53	52717	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:01.216655016 CEST	52718	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.236490965 CEST	53	52718	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.237344027 CEST	52719	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.255160093 CEST	53	52719	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.261420965 CEST	52720	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:01.281599998 CEST	53	52720	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.376256943 CEST	53	60690	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:01.616338968 CEST	62221	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:02.627542019 CEST	62221	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.165421963 CEST	53	62221	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.219702959 CEST	62222	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.239063978 CEST	53	62222	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.241400003 CEST	62223	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.259295940 CEST	53	62223	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.259742975 CEST	62224	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.279720068 CEST	53	62224	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.325418949 CEST	62225	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.343146086 CEST	53	62225	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.343590975 CEST	62226	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.361332893 CEST	53	62226	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.789190054 CEST	53	62221	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.807167053 CEST	63263	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.843403101 CEST	53	63263	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.859025002 CEST	63264	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.876193047 CEST	53	63264	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.877265930 CEST	63265	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.896852016 CEST	53	63265	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.897270918 CEST	63266	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.916883945 CEST	53	63266	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.917309046 CEST	63267	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.934696913 CEST	53	63267	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:03.935067892 CEST	63268	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:03.954763889 CEST	53	63268	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.372958899 CEST	59998	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.441500902 CEST	53	59998	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.468360901 CEST	59999	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.485769033 CEST	53	59999	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.486609936 CEST	60000	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.504255056 CEST	53	60000	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.504698038 CEST	60001	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.522697926 CEST	53	60001	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.523119926 CEST	60002	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.542658091 CEST	53	60002	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:04.543015003 CEST	60003	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:04.562457085 CEST	53	60003	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:05.013535976 CEST	61229	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.002994061 CEST	61229	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.137584925 CEST	53	61229	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.159151077 CEST	51773	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.176224947 CEST	53	51773	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.176892996 CEST	51774	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.194561005 CEST	53	51774	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.195981979 CEST	51775	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.215605021 CEST	53	51775	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.216034889 CEST	51776	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.235455036 CEST	53	51776	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.235821962 CEST	51777	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:06.255532980 CEST	53	51777	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:06.749398947 CEST	53461	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:07.172410965 CEST	53	61229	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:07.752329111 CEST	53461	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:07.863023043 CEST	53	53461	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:07.872886896 CEST	52817	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:07.908613920 CEST	53	52817	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:07.911994934 CEST	52818	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:07.947222948 CEST	53	52818	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:07.952331066 CEST	52819	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:07.987987041 CEST	53	52819	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:08.063038111 CEST	52820	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:08.082803011 CEST	53	52820	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:08.085752010 CEST	54197	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:08.104629993 CEST	53	54197	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:08.879440069 CEST	53	53461	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:09.104058981 CEST	57754	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:10.170181990 CEST	57754	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:10.707927942 CEST	53	57754	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:10.771631002 CEST	53	57754	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:11.685503960 CEST	64542	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:11.704840899 CEST	53	64542	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:11.740057945 CEST	64543	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:11.759860039 CEST	53	64543	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:11.785305023 CEST	64544	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:11.805135965 CEST	53	64544	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:11.805562019 CEST	64545	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:11.825198889 CEST	53	64545	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:11.917623043 CEST	64546	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:11.937248945 CEST	53	64546	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.346817970 CEST	53590	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.383526087 CEST	53	53590	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.390027046 CEST	53591	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.407648087 CEST	53	53591	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.408514977 CEST	53592	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.429454088 CEST	53	53592	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.431169033 CEST	53593	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.453207016 CEST	53	53593	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.453787088 CEST	53594	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.473371029 CEST	53	53594	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.473746061 CEST	53595	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:12.493643045 CEST	53	53595	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:12.822731972 CEST	56358	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.443161964 CEST	53	56358	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.451406002 CEST	56359	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.475533962 CEST	53	56359	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.477447033 CEST	56360	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.497633934 CEST	53	56360	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.505570889 CEST	56361	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.529026031 CEST	53	56361	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.529988050 CEST	56362	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.549556971 CEST	53	56362	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.551243067 CEST	56363	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.571007013 CEST	53	56363	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.907250881 CEST	51362	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.960828066 CEST	53	51362	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.974622965 CEST	51363	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:13.993717909 CEST	53	51363	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:13.994431019 CEST	51364	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:14.013231039 CEST	53	51364	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:14.017877102 CEST	51365	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:14.037378073 CEST	53	51365	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:14.041220903 CEST	51366	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:14.058753014 CEST	53	51366	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:14.061249018 CEST	51367	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:14.081089973 CEST	53	51367	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:14.448813915 CEST	49332	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:14.978720903 CEST	53	49332	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:14.985992908 CEST	49333	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:15.004993916 CEST	53	49333	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:15.005623102 CEST	49334	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:15.023289919 CEST	53	49334	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:15.024115086 CEST	49335	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:15.043770075 CEST	53	49335	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:15.044470072 CEST	49336	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:15.064199924 CEST	53	49336	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:15.074779987 CEST	49337	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:15.094535112 CEST	53	49337	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:15.435657024 CEST	58157	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:16.435070992 CEST	58157	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.137248039 CEST	53	58157	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.148379087 CEST	58158	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.167509079 CEST	53	58158	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.168323040 CEST	58159	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.187731981 CEST	53	58159	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.191071033 CEST	58160	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.208631039 CEST	53	58160	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.209347010 CEST	58161	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.226890087 CEST	53	58161	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.227550983 CEST	58162	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:17.246968031 CEST	53	58162	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.562474012 CEST	53	58157	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:17.566294909 CEST	57786	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.605894089 CEST	53	57786	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:18.609033108 CEST	57786	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.620011091 CEST	52844	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.639391899 CEST	53	52844	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:18.663878918 CEST	52845	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.684160948 CEST	53	52845	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:18.728477955 CEST	52846	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.746282101 CEST	53	52846	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:18.746733904 CEST	52847	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.766663074 CEST	53	52847	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:18.768532991 CEST	52848	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:18.786726952 CEST	53	52848	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.230156898 CEST	64961	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.720679045 CEST	53	57786	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.806276083 CEST	53	64961	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.817965031 CEST	64962	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.837085962 CEST	53	64962	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.837605953 CEST	64963	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.857325077 CEST	53	64963	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.857963085 CEST	64964	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.877415895 CEST	53	64964	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.877923012 CEST	64965	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.897783041 CEST	53	64965	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:19.899743080 CEST	64966	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:19.919105053 CEST	53	64966	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:20.262279034 CEST	56295	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:21.269645929 CEST	56295	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:22.271178961 CEST	56295	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.331629038 CEST	53	56295	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.340985060 CEST	56296	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.359858990 CEST	53	56296	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.360506058 CEST	56297	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.380099058 CEST	53	56297	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.380544901 CEST	56298	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.397959948 CEST	53	56298	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.403218031 CEST	56299	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.422846079 CEST	53	56299	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.423249006 CEST	56300	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.442930937 CEST	53	56300	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:22.764307022 CEST	64647	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:22.894814968 CEST	53	56295	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.301311970 CEST	53	64647	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.309506893 CEST	64648	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:23.326419115 CEST	53	64648	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.329807043 CEST	64649	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:23.349076033 CEST	53	64649	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.349894047 CEST	64650	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:23.367690086 CEST	53	64650	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.369930983 CEST	64651	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:23.389586926 CEST	53	64651	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.390727997 CEST	64652	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:23.410267115 CEST	53	64652	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:23.749346972 CEST	54503	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.301399946 CEST	53	54503	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.310062885 CEST	51888	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.329447031 CEST	53	51888	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.330288887 CEST	51889	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.350253105 CEST	53	51889	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.350750923 CEST	51890	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.370569944 CEST	53	51890	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.371077061 CEST	51891	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.390916109 CEST	53	51891	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.391366959 CEST	51892	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.411137104 CEST	53	51892	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.730248928 CEST	53041	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.806338072 CEST	53	53041	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.812444925 CEST	53042	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.831897020 CEST	53	53042	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.832633018 CEST	53043	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.850459099 CEST	53	53043	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.850862026 CEST	53044	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.870646000 CEST	53	53044	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.871066093 CEST	53045	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.890717030 CEST	53	53045	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:24.891149998 CEST	53046	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:24.910834074 CEST	53	53046	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:25.258671999 CEST	54508	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:25.904484034 CEST	53	54508	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:25.914251089 CEST	54509	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:25.932872057 CEST	53	54509	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:25.933530092 CEST	54510	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:26.317761898 CEST	53	56295	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:27.946239948 CEST	54511	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:27.967365980 CEST	53	54511	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:27.967772961 CEST	54512	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:27.988606930 CEST	53	54512	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:28.034455061 CEST	54513	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:28.055430889 CEST	53	54513	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:28.706429958 CEST	53193	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:29.724095106 CEST	53193	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:29.829662085 CEST	53	53193	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:29.908477068 CEST	53194	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:29.927891970 CEST	53	53194	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:29.933501959 CEST	53195	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:29.951251984 CEST	53	53195	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:30.011262894 CEST	53196	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:30.030755997 CEST	53	53196	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:30.133681059 CEST	53197	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:30.151573896 CEST	53	53197	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:30.152334929 CEST	53198	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:30.169919014 CEST	53	53198	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:32.441836119 CEST	60008	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.027606010 CEST	53	60008	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.051636934 CEST	60009	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.070842028 CEST	53	60009	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.071441889 CEST	60010	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.089258909 CEST	53	60010	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.089754105 CEST	60011	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.109560013 CEST	53	60011	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.110094070 CEST	60012	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.129426956 CEST	53	60012	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.131000996 CEST	60013	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.150530100 CEST	53	60013	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.499218941 CEST	54200	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.609451056 CEST	53	54200	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.616710901 CEST	54201	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.636173010 CEST	53	54201	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.636816978 CEST	54202	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.656276941 CEST	53	54202	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.657267094 CEST	54203	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.678827047 CEST	53	54203	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.679528952 CEST	54204	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.701402903 CEST	53	54204	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:33.702038050 CEST	54205	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:33.722425938 CEST	53	54205	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.088475943 CEST	50252	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.124522924 CEST	53	50252	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.141758919 CEST	50253	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.160888910 CEST	53	50253	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.167188883 CEST	50254	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.184612036 CEST	53	50254	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.185396910 CEST	50255	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.204812050 CEST	53	50255	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.205420017 CEST	50256	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.224951029 CEST	53	50256	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.225599051 CEST	50257	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.245430946 CEST	53	50257	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.730926037 CEST	64796	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.743029118 CEST	53	53193	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.796749115 CEST	53	64796	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.805094957 CEST	64797	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.824281931 CEST	53	64797	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.824858904 CEST	64798	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.844573975 CEST	53	64798	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.845123053 CEST	64799	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:34.864664078 CEST	53	64799	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.865340948 CEST	64800	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.884864092 CEST	53	64800	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:34.885485888 CEST	64801	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:34.902848959 CEST	53	64801	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.258631945 CEST	62537	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.827125072 CEST	53	62537	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.837460995 CEST	62538	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.856575966 CEST	53	62538	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.857431889 CEST	62539	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.876837969 CEST	53	62539	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.877444029 CEST	62540	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.900613070 CEST	53	62540	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.901067972 CEST	62541	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.921055079 CEST	53	62541	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:35.921513081 CEST	62542	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:35.941112041 CEST	53	62542	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:36.269373894 CEST	62036	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:37.255727053 CEST	62036	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:37.934292078 CEST	53	62036	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:37.942585945 CEST	62037	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:37.961843967 CEST	53	62037	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:37.962894917 CEST	62038	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:37.980525970 CEST	53	62038	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:37.987566948 CEST	62039	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.007184982 CEST	53	62039	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.007802010 CEST	62040	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.027669907 CEST	53	62040	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.028307915 CEST	62041	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.047924995 CEST	53	62041	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.376159906 CEST	63670	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.412417889 CEST	53	63670	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.419980049 CEST	63671	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.439403057 CEST	53	63671	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.440018892 CEST	63672	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.459865093 CEST	53	63672	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.460458040 CEST	63673	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.480101109 CEST	53	63673	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.481064081 CEST	63674	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.500571966 CEST	53	63674	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.501185894 CEST	63675	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:38.520761013 CEST	53	63675	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:38.925039053 CEST	61170	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:39.927758932 CEST	61170	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:39.928921938 CEST	53	62036	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:40.927438021 CEST	61170	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.055721998 CEST	53	61170	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.064487934 CEST	61171	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.081710100 CEST	53	61171	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.082365990 CEST	61172	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.102299929 CEST	53	61172	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.105315924 CEST	61173	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.125132084 CEST	53	61173	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.125727892 CEST	61174	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.145561934 CEST	53	61174	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.147699118 CEST	61175	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.165729046 CEST	53	61175	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.342947960 CEST	56427	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:41.456968069 CEST	53	61170	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:41.553389072 CEST	53	61170	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.981617928 CEST	53	56427	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:41.993149042 CEST	56428	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.012507915 CEST	53	56428	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.013339043 CEST	56429	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.033417940 CEST	53	56429	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.033911943 CEST	56430	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.053452969 CEST	53	56430	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.053870916 CEST	56431	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.071616888 CEST	53	56431	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.072022915 CEST	56432	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.091794014 CEST	53	56432	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.260376930 CEST	56431	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.379776001 CEST	53	56431	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.387754917 CEST	56432	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.407059908 CEST	53	56432	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.407532930 CEST	56433	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.427475929 CEST	53	56433	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.427927971 CEST	56434	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.447566032 CEST	53	56434	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.448009014 CEST	56435	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.465789080 CEST	53	56435	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.466213942 CEST	56436	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:42.486059904 CEST	53	56436	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:42.652055025 CEST	49465	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:43.646301031 CEST	49465	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.269579887 CEST	53	49465	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.278618097 CEST	49466	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.298013926 CEST	53	49466	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.300592899 CEST	49467	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.318439007 CEST	53	49467	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.319184065 CEST	49468	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.338943958 CEST	53	49468	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.340126038 CEST	49469	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.359947920 CEST	53	49469	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.362253904 CEST	49470	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.382220984 CEST	53	49470	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:44.560638905 CEST	54879	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:44.722793102 CEST	53	49465	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.552563906 CEST	54879	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.619430065 CEST	53	54879	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.626281023 CEST	54880	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.643874884 CEST	53	54880	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.644561052 CEST	54881	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.662398100 CEST	53	54881	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.662904024 CEST	54882	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.680767059 CEST	53	54882	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.681351900 CEST	54883	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.682105064 CEST	53	54879	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.701210022 CEST	53	54883	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.706056118 CEST	54884	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:45.725753069 CEST	53	54884	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:45.906866074 CEST	54296	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:46.913412094 CEST	54296	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:46.946067095 CEST	53	54296	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:46.955739975 CEST	54297	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:46.975125074 CEST	53	54297	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:46.975692987 CEST	54298	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:46.995784998 CEST	53	54298	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:46.996273041 CEST	54299	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:47.015886068 CEST	53	54299	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:47.016427994 CEST	54300	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:47.036571026 CEST	53	54300	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:47.037036896 CEST	54301	53	192.168.2.6	8.8.8.8
Aug 31, 2022 23:50:47.056572914 CEST	53	54301	8.8.8.8	192.168.2.6
Aug 31, 2022 23:50:48.583686113 CEST	53	54296	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 31, 2022 23:48:49.265063047 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:48:50.136071920 CEST	192.168.2.6	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:48:53.708611012 CEST	192.168.2.6	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:48:59.563985109 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:01.369291067 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:06.744471073 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:08.824440002 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:14.049535036 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:16.309123039 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:19.966995955 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:34.841367006 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:37.805382967 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:39.578983068 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:43.727289915 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:47.143408060 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:48.948611975 CEST	192.168.2.6	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:50.028990030 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:52.308603048 CEST	192.168.2.6	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:49:59.514467001 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:01.168688059 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:03.789285898 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:07.172538996 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:08.879571915 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:17.562561989 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:19.722575903 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:22.894917011 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:26.317929983 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:34.743129969 CEST	192.168.2.6	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:39.932499886 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 31, 2022 23:50:41.457130909 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:44.722973108 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:45.682204962 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:50:48.583869934 CEST	192.168.2.6	8.8.8.8	d033	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:48:44.116539001 CEST	192.168.2.6	8.8.8.8	0x77b2	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:45.117125034 CEST	192.168.2.6	8.8.8.8	0x79e2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:46.120923042 CEST	192.168.2.6	8.8.8.8	0x79e2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.148174047 CEST	192.168.2.6	8.8.8.8	0x79e2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.446198940 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:47.468455076 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.488892078 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:48:47.509377956 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.529671907 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:48:48.691446066 CEST	192.168.2.6	8.8.8.8	0xa153	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:49.961707115 CEST	192.168.2.6	8.8.8.8	0xa153	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.144049883 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:50.163892984 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.247066021 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:48:50.267487049 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.285778999 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:48:54.912518978 CEST	192.168.2.6	8.8.8.8	0x507e	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:54.986932039 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:55.006742954 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:55.025305033 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:48:55.046077967 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:55.066318035 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:48:56.292723894 CEST	192.168.2.6	8.8.8.8	0x37a1	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:57.294055939 CEST	192.168.2.6	8.8.8.8	0x37a1	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:57.923278093 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:57.941241026 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:57.961649895 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:48:57.979980946 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:58.002645016 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:48:59.203073978 CEST	192.168.2.6	8.8.8.8	0x327f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.248944044 CEST	192.168.2.6	8.8.8.8	0x327f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.827044010 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:00.850075960 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.891035080 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:00.911463022 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.931788921 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:02.198327065 CEST	192.168.2.6	8.8.8.8	0x799	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.264911890 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:02.284759998 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.302880049 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:02.321191072 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.339569092 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:03.829682112 CEST	192.168.2.6	8.8.8.8	0xebfc	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:03.922105074 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:03.940196037 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:03.959032059 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:03.979773998 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:04.012398005 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:05.030595064 CEST	192.168.2.6	8.8.8.8	0x3312	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.028855085 CEST	192.168.2.6	8.8.8.8	0x3312	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.098314047 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:06.118498087 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.139177084 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:06.157622099 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.177939892 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:07.180340052 CEST	192.168.2.6	8.8.8.8	0x2ef	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.172979116 CEST	192.168.2.6	8.8.8.8	0x2ef	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.337205887 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:08.357395887 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.378525019 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:08.399945974 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.420766115 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:11.635112047 CEST	192.168.2.6	8.8.8.8	0x9ae2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:12.929991007 CEST	192.168.2.6	8.8.8.8	0x9ae2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:49:13.344588995 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:13.365736008 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.387386084 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:13.407922029 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.428276062 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:14.604439974 CEST	192.168.2.6	8.8.8.8	0xf69c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.610282898 CEST	192.168.2.6	8.8.8.8	0xf69c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.762787104 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:15.787075996 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.820662022 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:15.846000910 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.872216940 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:17.166126013 CEST	192.168.2.6	8.8.8.8	0xaba4	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.297399998 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:17.315310955 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.336642981 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:17.355597019 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.376161098 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:18.439655066 CEST	192.168.2.6	8.8.8.8	0x3c13	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.436444044 CEST	192.168.2.6	8.8.8.8	0x3c13	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.605516911 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:19.625741959 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.646852970 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:19.667081118 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.687489033 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:20.744438887 CEST	192.168.2.6	8.8.8.8	0x1b2c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.364559889 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:21.389710903 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.410257101 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:21.437589884 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.461711884 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:22.729974031 CEST	192.168.2.6	8.8.8.8	0xf422	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.828344107 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:22.846611977 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.865636110 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:49:22.885858059 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.906522989 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:24.181659937 CEST	192.168.2.6	8.8.8.8	0x944e	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.843636036 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:24.863671064 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.882021904 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:24.900788069 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.926548004 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:26.173096895 CEST	192.168.2.6	8.8.8.8	0x6a3c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:26.742422104 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:26.766419888 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:26.794256926 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:26.819000959 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:26.845475912 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:32.760355949 CEST	192.168.2.6	8.8.8.8	0x778b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:33.801712990 CEST	192.168.2.6	8.8.8.8	0x778b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:33.948062897 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:33.965954065 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:33.986495972 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:34.009679079 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:34.029794931 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:35.228359938 CEST	192.168.2.6	8.8.8.8	0xa02c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:36.246831894 CEST	192.168.2.6	8.8.8.8	0xa02c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.234587908 CEST	192.168.2.6	8.8.8.8	0xa02c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.414644003 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:37.435153961 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.460208893 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:37.493947983 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.527287960 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:38.629677057 CEST	192.168.2.6	8.8.8.8	0x9841	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.190716982 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:39.210927963 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.232388020 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:39.251383066 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.272142887 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:49:40.533377886 CEST	192.168.2.6	8.8.8.8	0xb43c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:41.548500061 CEST	192.168.2.6	8.8.8.8	0xb43c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.563077927 CEST	192.168.2.6	8.8.8.8	0xb43c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.830462933 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:42.850589037 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.870748997 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:42.892258883 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.910756111 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:43.926912069 CEST	192.168.2.6	8.8.8.8	0xa38b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:44.985625029 CEST	192.168.2.6	8.8.8.8	0xa38b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:45.985445023 CEST	192.168.2.6	8.8.8.8	0xa38b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.167262077 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:46.187199116 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.207613945 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:46.227968931 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.246339083 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:47.290848970 CEST	192.168.2.6	8.8.8.8	0x888a	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:48.499587059 CEST	192.168.2.6	8.8.8.8	0x888a	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:49.956358910 CEST	192.168.2.6	8.8.8.8	0x888a	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.054864883 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:50.073091984 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.142801046 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:50.167078018 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.186178923 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:52.769992113 CEST	192.168.2.6	8.8.8.8	0xe105	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.309271097 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:53.336150885 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.354264975 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:53.372548103 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.390899897 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:53.746059895 CEST	192.168.2.6	8.8.8.8	0x2c41	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.293313026 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:54.327765942 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.349513054 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:49:54.371674061 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:49:54.397249937 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:54.752284050 CEST	192.168.2.6	8.8.8.8	0x2fb6	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.810272932 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:54.828233004 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.851675987 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:54.873826027 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.897558928 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:55.329066992 CEST	192.168.2.6	8.8.8.8	0xe3e7	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:56.358541012 CEST	192.168.2.6	8.8.8.8	0xe3e7	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.000348091 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:57.020057917 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.038532972 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:57.058875084 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.078872919 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:49:57.445333958 CEST	192.168.2.6	8.8.8.8	0x54e0	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.516345978 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:57.536552906 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.561312914 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:57.581695080 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.601932049 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:49:57.951314926 CEST	192.168.2.6	8.8.8.8	0x3737	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:58.940262079 CEST	192.168.2.6	8.8.8.8	0x3737	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.045651913 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:59.065542936 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.087832928 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:59.107861042 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.128176928 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:49:59.493012905 CEST	192.168.2.6	8.8.8.8	0x6ea0	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:00.513597965 CEST	192.168.2.6	8.8.8.8	0x6ea0	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.178349018 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:01.196441889 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.216655016 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:01.237344027 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.261420965 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:01.616338968 CEST	192.168.2.6	8.8.8.8	0xe543	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:02.627542019 CEST	192.168.2.6	8.8.8.8	0xe543	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.219702959 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:03.241400003 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.259742975 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:03.325418949 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.343590975 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:03.807167053 CEST	192.168.2.6	8.8.8.8	0x51e7	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.859025002 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:03.877265930 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.897270918 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:03.917309046 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.935067892 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:04.372958899 CEST	192.168.2.6	8.8.8.8	0xf3aa	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.468360901 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:04.486609936 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.504698038 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:04.523119926 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.543015003 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:05.013535976 CEST	192.168.2.6	8.8.8.8	0xa538	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.002994061 CEST	192.168.2.6	8.8.8.8	0xa538	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.159151077 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:06.176892996 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.195981979 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:06.216034889 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.235821962 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:06.749398947 CEST	192.168.2.6	8.8.8.8	0xd5a5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.752329111 CEST	192.168.2.6	8.8.8.8	0xd5a5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.872886896 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:07.911994934 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.952331066 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:08.063038111 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:08.085752010 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:09.104058981 CEST	192.168.2.6	8.8.8.8	0x9165	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:10.170181990 CEST	192.168.2.6	8.8.8.8	0x9165	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.685503960 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:11.740057945 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.785305023 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:11.805562019 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.917623043 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:12.346817970 CEST	192.168.2.6	8.8.8.8	0x3d0f	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.390027046 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:12.408514977 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.431169033 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:12.453787088 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.473746061 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:12.822731972 CEST	192.168.2.6	8.8.8.8	0xead9	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.451406002 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:13.477447033 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.505570889 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:13.529988050 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.551243067 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:13.907250881 CEST	192.168.2.6	8.8.8.8	0x71e7	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.974622965 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:13.994431019 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:14.017877102 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:14.041220903 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:14.061249018 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:14.448813915 CEST	192.168.2.6	8.8.8.8	0xe1fb	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:14.985992908 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:15.005623102 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:15.024115086 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:15.044470072 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:15.074779987 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:15.435657024 CEST	192.168.2.6	8.8.8.8	0x45ab	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:16.435070992 CEST	192.168.2.6	8.8.8.8	0x45ab	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.148379087 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:17.168323040 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.191071033 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:17.209347010 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.227550983 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:17.566294909 CEST	192.168.2.6	8.8.8.8	0xe55c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.609033108 CEST	192.168.2.6	8.8.8.8	0xe55c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.620011091 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:18.663878918 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.728477955 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:18.746733904 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.768532991 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:19.230156898 CEST	192.168.2.6	8.8.8.8	0x17fb	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.817965031 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:19.837605953 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.857963085 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:19.877923012 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.899743080 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:20.262279034 CEST	192.168.2.6	8.8.8.8	0xdd32	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:21.269645929 CEST	192.168.2.6	8.8.8.8	0xdd32	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.271178961 CEST	192.168.2.6	8.8.8.8	0xdd32	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.340985060 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:22.360506058 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.380544901 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:22.403218031 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.423249006 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:22.764307022 CEST	192.168.2.6	8.8.8.8	0x2339	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.309506893 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:23.329807043 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.349894047 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:23.369930983 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.390727997 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:23.749346972 CEST	192.168.2.6	8.8.8.8	0xb987	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.310062885 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:24.330288887 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.350750923 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:24.371077061 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.391366959 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:24.730248928 CEST	192.168.2.6	8.8.8.8	0x3a0	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.812444925 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:24.832633018 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.850862026 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:24.871066093 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.891149998 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:25.258671999 CEST	192.168.2.6	8.8.8.8	0x2446	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:25.914251089 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:25.933530092 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:27.946239948 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:27.967772961 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:28.034455061 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:28.706429958 CEST	192.168.2.6	8.8.8.8	0xc06b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:29.724095106 CEST	192.168.2.6	8.8.8.8	0xc06b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:29.908477068 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:29.933501959 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:30.011262894 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:30.133681059 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:30.152334929 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:32.441836119 CEST	192.168.2.6	8.8.8.8	0xcae5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.051636934 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:33.071441889 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.089754105 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:33.110094070 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.131000996 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:33.499218941 CEST	192.168.2.6	8.8.8.8	0x7e06	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.616710901 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:33.636816978 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.657267094 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:33.679528952 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.702038050 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:34.088475943 CEST	192.168.2.6	8.8.8.8	0x94db	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.141758919 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:34.167188883 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.185396910 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:34.205420017 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.225599051 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:34.730926037 CEST	192.168.2.6	8.8.8.8	0x2898	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.805094957 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:34.824858904 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.845123053 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:34.865340948 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.885485888 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:35.258631945 CEST	192.168.2.6	8.8.8.8	0x35c5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.837460995 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:35.857431889 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.877444029 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:35.901067972 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.921513081 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:36.269373894 CEST	192.168.2.6	8.8.8.8	0x2a1b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:37.255727053 CEST	192.168.2.6	8.8.8.8	0x2a1b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:37.942585945 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:37.962894917 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:37.987566948 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:38.007802010 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.028307915 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:50:38.376159906 CEST	192.168.2.6	8.8.8.8	0x95d8	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.419980049 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:38.440018892 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.460458040 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:38.481064081 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.501185894 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:38.925039053 CEST	192.168.2.6	8.8.8.8	0xbe58	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:39.927758932 CEST	192.168.2.6	8.8.8.8	0xbe58	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:40.927438021 CEST	192.168.2.6	8.8.8.8	0xbe58	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.064487934 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:41.082365990 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.105315924 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:41.125727892 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.147699118 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:41.342947960 CEST	192.168.2.6	8.8.8.8	0x7e01	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.993149042 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:42.013339043 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.033911943 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:42.053870916 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.072022915 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:42.260376930 CEST	192.168.2.6	8.8.8.8	0xc002	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.387754917 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:42.407532930 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.427927971 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:42.448009014 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.466213942 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:42.652055025 CEST	192.168.2.6	8.8.8.8	0x796	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:43.646301031 CEST	192.168.2.6	8.8.8.8	0x796	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.278618097 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:44.300592899 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.319184065 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:44.340126038 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.362253904 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:50:44.560638905 CEST	192.168.2.6	8.8.8.8	0xe7ea	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.552563906 CEST	192.168.2.6	8.8.8.8	0xe7ea	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.626281023 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:45.644561052 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.662904024 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:45.681351900 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.706056118 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:50:45.906866074 CEST	192.168.2.6	8.8.8.8	0x2664	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:46.913412094 CEST	192.168.2.6	8.8.8.8	0x2664	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:46.955739975 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:46.975692987 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:46.996273041 CEST	192.168.2.6	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Aug 31, 2022 23:50:47.016427994 CEST	192.168.2.6	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:47.037036896 CEST	192.168.2.6	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:48:47.429773092 CEST	8.8.8.8	192.168.2.6	0x79e2	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.465388060 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:48:47.488225937 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.508804083 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:47.529036045 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:47.549340963 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:49.264957905 CEST	8.8.8.8	192.168.2.6	0x79e2	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:49.988116026 CEST	8.8.8.8	192.168.2.6	0xa153	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.135879040 CEST	8.8.8.8	192.168.2.6	0x79e2	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.163110971 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:50.183588028 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.266885042 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:50.285155058 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:50.305613995 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:53.708446980 CEST	8.8.8.8	192.168.2.6	0xa153	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:54.940237045 CEST	8.8.8.8	192.168.2.6	0x507e	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:55.005909920 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:55.024481058 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:55.044683933 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:55.065548897 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:55.085766077 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:57.871090889 CEST	8.8.8.8	192.168.2.6	0x37a1	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:57.940429926 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:48:57.961014986 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:57.979434013 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:57.997720003 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:58.020783901 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:48:59.563860893 CEST	8.8.8.8	192.168.2.6	0x37a1	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.778501987 CEST	8.8.8.8	192.168.2.6	0x327f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.846194029 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:00.870034933 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.910629988 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:00.930983067 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:00.951646090 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:01.369014978 CEST	8.8.8.8	192.168.2.6	0x327f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.226392031 CEST	8.8.8.8	192.168.2.6	0x799	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.283921003 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:49:02.302268028 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.320642948 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:02.338948965 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:02.359249115 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:03.865678072 CEST	8.8.8.8	192.168.2.6	0xebfc	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:03.939187050 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:03.958033085 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:03.978843927 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:03.997428894 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:04.032171965 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:06.064717054 CEST	8.8.8.8	192.168.2.6	0x3312	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.117698908 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:06.138461113 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.157145977 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:06.177340984 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:06.195765972 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:06.744250059 CEST	8.8.8.8	192.168.2.6	0x3312	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.292459011 CEST	8.8.8.8	192.168.2.6	0x2ef	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.356190920 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:08.376708031 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.397835970 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:08.418164968 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:08.440345049 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:08.824318886 CEST	8.8.8.8	192.168.2.6	0x2ef	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.306567907 CEST	8.8.8.8	192.168.2.6	0x9ae2	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.364543915 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:13.386758089 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.407160044 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:13.427547932 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:13.445738077 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:14.049354076 CEST	8.8.8.8	192.168.2.6	0x9ae2	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.732141018 CEST	8.8.8.8	192.168.2.6	0xf69c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.786143064 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:15.810261011 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.845424891 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:49:15.871382952 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:15.897437096 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:16.308988094 CEST	8.8.8.8	192.168.2.6	0xf69c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.240441084 CEST	8.8.8.8	192.168.2.6	0xaba4	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.314428091 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:17.335490942 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.354706049 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:17.375117064 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:17.394150019 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:19.552881956 CEST	8.8.8.8	192.168.2.6	0x3c13	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.624495029 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:19.646193027 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.666341066 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:19.686774969 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:19.706923962 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:19.966856956 CEST	8.8.8.8	192.168.2.6	0x3c13	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.322283030 CEST	8.8.8.8	192.168.2.6	0x1b2c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.388284922 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:21.409245014 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.428335905 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:21.460988045 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:21.481684923 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:22.802742958 CEST	8.8.8.8	192.168.2.6	0xf422	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.845546007 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:22.864109993 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.885181904 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:22.905694008 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:22.924313068 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:24.794177055 CEST	8.8.8.8	192.168.2.6	0x944e	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.862725973 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:24.881535053 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.900017977 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:24.918819904 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:24.944628000 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:26.704699039 CEST	8.8.8.8	192.168.2.6	0x6a3c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:49:26.762280941 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:26.786171913 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:26.815588951 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:26.840948105 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:26.868755102 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:33.918472052 CEST	8.8.8.8	192.168.2.6	0x778b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:33.965091944 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:33.985773087 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:34.008980036 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:34.029289961 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:34.047578096 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:34.840379000 CEST	8.8.8.8	192.168.2.6	0x778b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.368525028 CEST	8.8.8.8	192.168.2.6	0xa02c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.434192896 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:37.455080986 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.479908943 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:37.513475895 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:37.546905994 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:37.804033995 CEST	8.8.8.8	192.168.2.6	0xa02c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.158519983 CEST	8.8.8.8	192.168.2.6	0x9841	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.209886074 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:39.228986025 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.250422955 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:39.270978928 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:39.291903973 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:39.578844070 CEST	8.8.8.8	192.168.2.6	0xa02c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.803582907 CEST	8.8.8.8	192.168.2.6	0xb43c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.849625111 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:42.870042086 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.890347004 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:42.910130978 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:42.930283070 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:43.727183104 CEST	8.8.8.8	192.168.2.6	0xb43c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:44.304563046 CEST	8.8.8.8	192.168.2.6	0xb43c	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.151169062 CEST	8.8.8.8	192.168.2.6	0xa38b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:49:46.186392069 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:46.206867933 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.227328062 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:46.245661020 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:46.263768911 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:47.143296003 CEST	8.8.8.8	192.168.2.6	0xa38b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:48.946257114 CEST	8.8.8.8	192.168.2.6	0xa38b	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:49.671741962 CEST	8.8.8.8	192.168.2.6	0x888a	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.028801918 CEST	8.8.8.8	192.168.2.6	0x888a	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.072125912 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:50.094736099 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.160806894 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:50.185210943 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:50.206547022 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:52.308414936 CEST	8.8.8.8	192.168.2.6	0x888a	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.300184965 CEST	8.8.8.8	192.168.2.6	0xe105	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.328352928 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:53.353754044 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.372015953 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:53.390347004 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:53.411127090 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:54.282331944 CEST	8.8.8.8	192.168.2.6	0x2c41	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.312721014 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:54.346045017 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.369218111 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:54.389324903 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.415669918 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:54.786828041 CEST	8.8.8.8	192.168.2.6	0x2fb6	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.827580929 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:54.848042965 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.871623039 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:54.893619061 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:54.917089939 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:56.991584063 CEST	8.8.8.8	192.168.2.6	0xe3e7	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.019478083 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:49:57.038048983 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.058454990 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:57.078458071 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.096430063 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:57.489593983 CEST	8.8.8.8	192.168.2.6	0x54e0	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.535823107 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:57.556433916 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.581238985 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:57.601391077 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:57.621717930 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:59.038297892 CEST	8.8.8.8	192.168.2.6	0x3737	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.064886093 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:49:59.085707903 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.107444048 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:59.127703905 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:49:59.148261070 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:49:59.514354944 CEST	8.8.8.8	192.168.2.6	0x3737	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.090209007 CEST	8.8.8.8	192.168.2.6	0x6ea0	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.166991949 CEST	8.8.8.8	192.168.2.6	0x6ea0	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.195605040 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:01.216135979 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.236490965 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:01.255160093 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:01.281599998 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:01.376256943 CEST	8.8.8.8	192.168.2.6	0xe3e7	Server failure (2)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.165421963 CEST	8.8.8.8	192.168.2.6	0xe543	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.239063978 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:03.259295940 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.279720068 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:03.343146086 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.361332893 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:03.789190054 CEST	8.8.8.8	192.168.2.6	0xe543	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.843403101 CEST	8.8.8.8	192.168.2.6	0x51e7	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.876193047 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:03.896852016 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:03.916883945 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:03.934696913 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:03.954763889 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:04.441500902 CEST	8.8.8.8	192.168.2.6	0xf3aa	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.485769033 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:04.504255056 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.522697926 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:04.542658091 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:04.562457085 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:06.137584925 CEST	8.8.8.8	192.168.2.6	0xa538	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.176224947 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:06.194561005 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.215605021 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:06.235455036 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:06.255532980 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:07.172410965 CEST	8.8.8.8	192.168.2.6	0xa538	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.863023043 CEST	8.8.8.8	192.168.2.6	0xd5a5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.908613920 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:07.947222948 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:07.987987041 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:08.082803011 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:08.104629993 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:08.879440069 CEST	8.8.8.8	192.168.2.6	0xd5a5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:10.707927942 CEST	8.8.8.8	192.168.2.6	0x9165	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:10.771631002 CEST	8.8.8.8	192.168.2.6	0x9165	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.704840899 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:11.759860039 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.805135965 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:11.825198889 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:11.937248945 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:12.383526087 CEST	8.8.8.8	192.168.2.6	0x3d0f	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.407648087 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:12.429454088 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.453207016 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:12.473371029 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:12.493643045 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:13.443161964 CEST	8.8.8.8	192.168.2.6	0xead9	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.475533962 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:13.497633934 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.529026031 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:13.549556971 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.571007013 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:13.960828066 CEST	8.8.8.8	192.168.2.6	0x71e7	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:13.993717909 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:14.013231039 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:14.037378073 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:14.058753014 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:14.081089973 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:14.978720903 CEST	8.8.8.8	192.168.2.6	0xe1fb	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:15.004993916 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:15.023289919 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:15.043770075 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:15.064199924 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:15.094535112 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:17.137248039 CEST	8.8.8.8	192.168.2.6	0x45ab	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.167509079 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:17.187731981 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.208631039 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:17.226890087 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:17.246968031 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:17.562474012 CEST	8.8.8.8	192.168.2.6	0x45ab	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.605894089 CEST	8.8.8.8	192.168.2.6	0xe55c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.639391899 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:18.684160948 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.746282101 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:18.766663074 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:18.786726952 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:19.720679045 CEST	8.8.8.8	192.168.2.6	0xe55c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.806276083 CEST	8.8.8.8	192.168.2.6	0x17fb	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.837085962 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:19.857325077 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.877415895 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:19.897783041 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:19.919105053 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:22.331629038 CEST	8.8.8.8	192.168.2.6	0xdd32	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.359858990 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:22.380099058 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.397959948 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:22.422846079 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:22.442930937 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:22.894814968 CEST	8.8.8.8	192.168.2.6	0xdd32	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.301311970 CEST	8.8.8.8	192.168.2.6	0x2339	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.326419115 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:23.349076033 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.367690086 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:23.389586926 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:23.410267115 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:24.301399946 CEST	8.8.8.8	192.168.2.6	0xb987	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.329447031 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:24.350253105 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.370569944 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:24.390916109 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.411137104 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:24.806338072 CEST	8.8.8.8	192.168.2.6	0x3a0	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.831897020 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:24.850459099 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.870646000 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:24.890717030 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:24.910834074 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:25.904484034 CEST	8.8.8.8	192.168.2.6	0x2446	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:25.932872057 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:26.317761898 CEST	8.8.8.8	192.168.2.6	0xdd32	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:27.967365980 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:27.988606930 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:28.055430889 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)

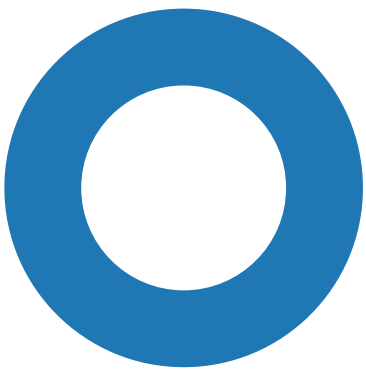
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:29.829662085 CEST	8.8.8.8	192.168.2.6	0xc06b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:29.927891970 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:29.951251984 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:30.030755997 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:30.151573896 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:30.169919014 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:33.027606010 CEST	8.8.8.8	192.168.2.6	0xcae5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.070842028 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:33.089258909 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.109560013 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:33.129426956 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.150530100 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:33.609451056 CEST	8.8.8.8	192.168.2.6	0x7e06	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.636173010 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:33.656276941 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.678827047 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:33.701402903 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:33.722425938 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:34.124522924 CEST	8.8.8.8	192.168.2.6	0x94db	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.160888910 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:34.184612036 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.204812050 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:34.224951029 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.245430946 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:34.743029118 CEST	8.8.8.8	192.168.2.6	0xc06b	Server failure (2)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.796749115 CEST	8.8.8.8	192.168.2.6	0x2898	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.824281931 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:34.844573975 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.864664078 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:34.884864092 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:34.902848959 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:35.827125072 CEST	8.8.8.8	192.168.2.6	0x35c5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.856575966 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:35.876837969 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.900613070 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:35.921055079 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:35.941112041 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:37.934292078 CEST	8.8.8.8	192.168.2.6	0x2a1b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:37.961843967 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:37.980525970 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.007184982 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:38.027669907 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.047924995 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:38.412417889 CEST	8.8.8.8	192.168.2.6	0x95d8	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.439403057 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:38.459865093 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.480101109 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:38.500571966 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:38.520761013 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:39.928921938 CEST	8.8.8.8	192.168.2.6	0x2a1b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.055721998 CEST	8.8.8.8	192.168.2.6	0xbe58	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.081710100 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:41.102299929 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.125132084 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:41.145561934 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.165729046 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:41.456968069 CEST	8.8.8.8	192.168.2.6	0xbe58	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.553389072 CEST	8.8.8.8	192.168.2.6	0xbe58	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:41.981617928 CEST	8.8.8.8	192.168.2.6	0x7e01	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.012507915 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:42.033417940 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.053452969 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:42.071616888 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.091794014 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:42.379776001 CEST	8.8.8.8	192.168.2.6	0xc002	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.407059908 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:42.427475929 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.447566032 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:42.465789080 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:42.486059904 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:50:44.269579887 CEST	8.8.8.8	192.168.2.6	0x796	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.298013926 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:44.318439007 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.338943958 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:44.359947920 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:44.382220984 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:44.722793102 CEST	8.8.8.8	192.168.2.6	0x796	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.619430065 CEST	8.8.8.8	192.168.2.6	0xe7ea	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.643874884 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:45.662398100 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.680767059 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:45.682105064 CEST	8.8.8.8	192.168.2.6	0xe7ea	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.701210022 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:45.725753069 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:46.946067095 CEST	8.8.8.8	192.168.2.6	0x2664	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:46.975125074 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:50:46.995784998 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:47.015886068 CEST	8.8.8.8	192.168.2.6	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:47.036571026 CEST	8.8.8.8	192.168.2.6	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:47.056572914 CEST	8.8.8.8	192.168.2.6	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:50:48.583686113 CEST	8.8.8.8	192.168.2.6	0x2664	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)

Statistics

Behavior



- eW1QrimJYd.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- qvvfpl.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- qvvfpl.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe

- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: eW1QrimJYd.exe PID: 4500, Parent PID: 5436

General

Target ID:	1
Start time:	23:48:35
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\eW1QrimJYd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\eW1QrimJYd.exe"
Imagebase:	0xa80000
File size:	75264 bytes
MD5 hash:	B7325E075262FFDEAA68CAE94018CADB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000001.00000002.532107831.0000000000A89000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000001.00000000.250804234.0000000000A89000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	cfbtnelfyrp	unicode	"C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe"	success or wait	1	A82AAA	RegSetValueExW

Analysis Process: nslookup.exe PID: 5720, Parent PID: 4500

General

Target ID:	5
Start time:	23:48:44

Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5276**, Parent PID: **5720**

General

Target ID:	6
Start time:	23:48:44
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nslookup.exe PID: **5916**, Parent PID: **4500**

General

Target ID:	7
Start time:	23:48:48
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5460**, Parent PID: **5916**

General

Target ID:	8
Start time:	23:48:48
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nslookup.exe PID: **5400**, Parent PID: **4500**

General

Target ID:	9
Start time:	23:48:50
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: qvvfpl.exe PID: **3252**, Parent PID: **3452**

General

Target ID:	11
Start time:	23:48:52
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe"
Imagebase:	0xd70000
File size:	75264 bytes
MD5 hash:	E5E0C9F951E9947AEA55720B7D0299F2
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000B.00000000.290444735.0000000000D79000.00000008.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000B.00000002.293487625.0000000000D79000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: Joe Security • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe, Author: kevoreilly
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: conhost.exe PID: **492**, Parent PID: **5400**

General

Target ID:	12
Start time:	23:48:54
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nslookup.exe PID: **5732**, Parent PID: **4500**

General

Target ID:	13
Start time:	23:48:55
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5964**, Parent PID: **5732**

General

Target ID:	15
Start time:	23:48:56
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **4788**, Parent PID: **4500**

General

Target ID:	20
Start time:	23:48:58
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3572**, Parent PID: **4788**

General

Target ID:	21
Start time:	23:48:58
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **5276**, Parent PID: **4500**

General

Target ID:	22

Start time:	23:49:01
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5380**, Parent PID: **5276**

General

Target ID:	23
Start time:	23:49:01
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: qvvfpl.exe PID: **68**, Parent PID: **3452**

General

Target ID:	24
Start time:	23:49:02
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\qvvfpl.exe"
Imagebase:	0xd70000
File size:	75264 bytes
MD5 hash:	E5E0C9F951E9947AEA55720B7D0299F2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000018.00000002.311448565.0000000000D79000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000018.00000000.308301094.0000000000D79000.00000008.00000001.01000000.00000006.sdmp, Author: Joe Security

Analysis Process: nslookup.exe PID: **6148**, Parent PID: **4500**

General	
Target ID:	25
Start time:	23:49:02
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6168**, Parent PID: **6148**

General	
Target ID:	26
Start time:	23:49:03
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6220**, Parent PID: **4500**

General	
Target ID:	28
Start time:	23:49:04
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6260, Parent PID: 6220

General

Target ID:	29
Start time:	23:49:04
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 6316, Parent PID: 4500

General

Target ID:	30
Start time:	23:49:06
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6324, Parent PID: 6316

General

Target ID:	31
Start time:	23:49:06
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 6372, Parent PID: 4500

General

Target ID:	32
Start time:	23:49:08
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6380, Parent PID: 6372

General

Target ID:	33
Start time:	23:49:09
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 6528, Parent PID: 4500

General

Target ID:	35
Start time:	23:49:13
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6540**, Parent PID: **6528**

General

Target ID:	36
Start time:	23:49:14
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6632**, Parent PID: **4500**

General

Target ID:	37
Start time:	23:49:16
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6640**, Parent PID: **6632**

General

Target ID:	38
Start time:	23:49:16
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6720**, Parent PID: **4500**

General

Target ID:	39
Start time:	23:49:17
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6736**, Parent PID: **6720**

General

Target ID:	40
Start time:	23:49:18
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6808**, Parent PID: **4500**

General

Target ID:	41
Start time:	23:49:20
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes

MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6820**, Parent PID: **6808**

General

Target ID:	42
Start time:	23:49:20
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6920**, Parent PID: **4500**

General

Target ID:	43
Start time:	23:49:21
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6932**, Parent PID: **6920**

General

Target ID:	44
Start time:	23:49:22

Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **7028**, Parent PID: **4500**

General

Target ID:	45
Start time:	23:49:23
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7040**, Parent PID: **7028**

General

Target ID:	46
Start time:	23:49:23
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **7100**, Parent PID: **4500**

General

Target ID:	47
Start time:	23:49:25
Start date:	31/08/2022

Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7108**, Parent PID: **7100**

General

Target ID:	48
Start time:	23:49:25
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **7156**, Parent PID: **4500**

General

Target ID:	49
Start time:	23:49:27
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7164**, Parent PID: **7156**

General	
Target ID:	50
Start time:	23:49:28
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6164**, Parent PID: **4500**

General	
Target ID:	51
Start time:	23:49:34
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6156**, Parent PID: **6164**

General	
Target ID:	52
Start time:	23:49:34
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6288**, Parent PID: **4500**

General	
Target ID:	53
Start time:	23:49:38
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6260**, Parent PID: **6288**

General	
Target ID:	54
Start time:	23:49:38
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **2852**, Parent PID: **4500**

General	
Target ID:	56
Start time:	23:49:39
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1432**, Parent PID: **2852**

General

Target ID:	57
Start time:	23:49:40
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **2408**, Parent PID: **4500**

General

Target ID:	58
Start time:	23:49:43
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6448**, Parent PID: **2408**

General

Target ID:	59
Start time:	23:49:43
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **6392**, Parent PID: **4500**

General	
Target ID:	61
Start time:	23:49:46
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xb80000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6428**, Parent PID: **6392**

General	
Target ID:	62
Start time:	23:49:47
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly