ID: 694570
Sample Name: 2fiDcmkaZY.exe
Cookbook: default.jbs
Time: 00:00:54
Date: 01/09/2022
Version: 35.0.0 Citrine

Table of Contents

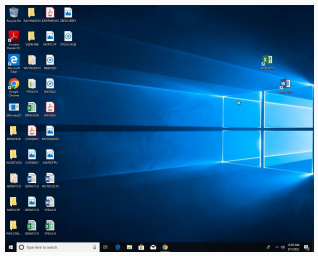
Windows Analysis Report

2fiDcmkaZY.exe

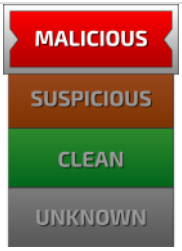
Overview

General Information

Sample Name:	2fiDcmkaZY.exe
Analysis ID:	694570
MD5:	a8ac57500de5da..
SHA1:	202baa4b862222.
SHA256:	fcc7cc8f57d5a2a..
Tags:	exe
Infos:	



Detection



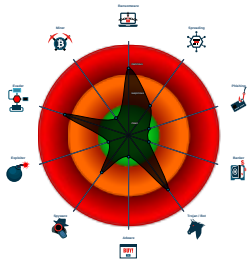
Gandcrab

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**
- 2fiDcmkaZY.exe (PID: 6752 cmdline: "C:\Users\user\Desktop\2fiDcmkaZY.exe" MD5: A8AC57500DE5DADF8C4DB19959DDF2EC)
  - nslookup.exe (PID: 6896 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6972 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7032 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7084 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 7092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7144 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 7152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5388 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6392 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 2992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 3096 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5940 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6024 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5872 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6568 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: 6636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5964 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6308 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6952 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6848 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7044 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 7040 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)

- conhost.exe (PID: 7036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 7104 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 7148 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 4556 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 5844 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 5976 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6564 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 5860 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6608 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6032 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6440 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 6460 cmdline: nslookup emsisoft.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- tdicrr.exe (PID: 1476 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe" MD5: D2E112FDFFC314778285E837BC0BED47)
- tdicrr.exe (PID: 5864 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe" MD5: D2E112FDFFC314778285E837BC0BED47)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
2fiDcmkaZY.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
2fiDcmkaZY.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
2fiDcmkaZY.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\tdicrr.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\tdicrr.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
0000000D.00000000.343462206.0000000000C79000.00000008.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0000000D.00000002.346586335.0000000000C79000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000014.00000002.363374033.0000000000C79000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000000.304343043.0000000000A69000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000014.00000000.360474661.0000000000C79000.00000008.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.0.tdicrr.exe.c70000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
13.0.tdicrr.exe.c70000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
13.0.tdicrr.exe.c70000.0.unpack	Gandcrab	Gandcrab Payload	kevoreilly	• 0xf70c:$string1: GDCB-DECRYPT.txt • 0xf77a:$string1: GDCB-DECRYPT.txt • 0xf460:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
20.0.tdicrr.exe.c70000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xf716:$: DECRYPT.txt • 0xf784:$: DECRYPT.txt
20.0.tdicrr.exe.c70000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 13 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.860180532829500 09/01/22-00:02:50.502751
SID:	2829500
Source Port:	60180
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.854371532026737 09/01/22-00:04:03.802921
SID:	2026737
Source Port:	54371
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.858474532829498 09/01/22-00:02:46.409357
SID:	2829498
Source Port:	58474
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.856690532026737 09/01/22-00:02:34.794476
SID:	2026737

Source Port:	56690
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852975532829500 09/01/22-00:03:40.177431
SID:	2829500
Source Port:	52975
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859224532829500 09/01/22-00:02:18.976716
SID:	2829500
Source Port:	59224
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853975532829500 09/01/22-00:02:39.645914
SID:	2829500
Source Port:	53975
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861348532829498 09/01/22-00:02:38.530362
SID:	2829498
Source Port:	61348
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860024532829498 09/01/22-00:02:55.250291
SID:	2829498
Source Port:	60024
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853827532026737 09/01/22-00:03:02.774286
SID:	2026737
Source Port:	53827
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860910532026737 09/01/22-00:03:28.310952
SID:	2026737
Source Port:	60910
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863730532829498 09/01/22-00:03:33.977550
SID:	2829498
Source Port:	63730
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860183532829498 09/01/22-00:03:48.283959
SID:	2829498
Source Port:	60183
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854587532829498 09/01/22-00:03:23.124735
SID:	2829498
Source Port:	54587
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850904532829500 09/01/22-00:02:58.051616
SID:	2829500
Source Port:	50904
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855070532026737 09/01/22-00:02:20.361607
SID:	2026737
Source Port:	55070
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850089532829500 09/01/22-00:03:18.466985
SID:	2829500
Source Port:	50089
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859587532829498 09/01/22-00:04:04.114751
SID:	2829498
Source Port:	59587
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855597532026737 09/01/22-00:04:09.936181
SID:	2026737
Source Port:	55597

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865325532026737 09/01/22-00:02:04.877624
SID:	2026737
Source Port:	65325
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862662532026737 09/01/22-00:02:25.469721
SID:	2026737
Source Port:	62662
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865120532829498 09/01/22-00:04:10.763289
SID:	2829498
Source Port:	65120
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861296532829498 09/01/22-00:03:15.496749
SID:	2829498
Source Port:	61296
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857484532026737 09/01/22-00:03:30.517521
SID:	2026737
Source Port:	57484
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858446532829498 09/01/22-00:03:43.925486
SID:	2829498
Source Port:	58446
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864315532829498 09/01/22-00:03:59.415810
SID:	2829498
Source Port:	64315
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865333532829498 09/01/22-00:03:39.670910
SID:	2829498
Source Port:	65333
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852193532026737 09/01/22-00:03:21.210468
SID:	2026737
Source Port:	52193
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852103532829500 09/01/22-00:03:27.689357
SID:	2829500
Source Port:	52103
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865119532829498 09/01/22-00:04:10.743391
SID:	2829498
Source Port:	65119
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850566532829500 09/01/22-00:04:04.976212
SID:	2829500
Source Port:	50566
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863448532829500 09/01/22-00:02:12.612834
SID:	2829500
Source Port:	63448
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862059532829500 09/01/22-00:03:32.850991
SID:	2829500
Source Port:	62059
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858476532829498 09/01/22-00:02:46.511401
SID:	2829498
Source Port:	58476

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862938532026737 09/01/22-00:03:42.736982
SID:	2026737
Source Port:	62938
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860181532829498 09/01/22-00:03:48.237956
SID:	2829498
Source Port:	60181
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858626532829498 09/01/22-00:03:28.872267
SID:	2829498
Source Port:	58626
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865328532026737 09/01/22-00:02:04.942715
SID:	2026737
Source Port:	65328
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864497532026737 09/01/22-00:03:56.326355
SID:	2026737
Source Port:	64497
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860286532026737 09/01/22-00:02:53.057441
SID:	2026737
Source Port:	60286
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853559532026737 09/01/22-00:03:13.202744
SID:	2026737
Source Port:	53559
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850446532829498 09/01/22-00:03:53.963216
SID:	2829498
Source Port:	50446
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856116532026737 09/01/22-00:04:05.801650
SID:	2026737
Source Port:	56116
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849729532829498 09/01/22-00:02:01.433122
SID:	2829498
Source Port:	49729
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863451532829500 09/01/22-00:02:12.684530
SID:	2829500
Source Port:	63451
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858535532829500 09/01/22-00:02:23.142881
SID:	2829500
Source Port:	58535
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850448532829498 09/01/22-00:03:54.015145
SID:	2829498
Source Port:	50448
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864499532026737 09/01/22-00:03:56.365974
SID:	2026737
Source Port:	64499
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851489532829498 09/01/22-00:02:06.151880
SID:	2829498
Source Port:	51489

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

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865117532829498 09/01/22-00:04:10.704503
SID:	2829498
Source Port:	65117
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852191532026737 09/01/22-00:03:21.167674
SID:	2026737
Source Port:	52191
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856119532026737 09/01/22-00:04:05.881610
SID:	2026737
Source Port:	56119
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856689532026737 09/01/22-00:02:34.772206
SID:	2026737
Source Port:	56689
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858584532829498 09/01/22-00:02:31.231912
SID:	2829498
Source Port:	58584
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849963532026737 09/01/22-00:03:35.711880
SID:	2026737
Source Port:	49963
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860182532829500 09/01/22-00:02:50.545957
SID:	2829500
Source Port:	60182
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854589532829498 09/01/22-00:03:23.168676
SID:	2829498
Source Port:	54589
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865515532829500 09/01/22-00:02:32.912023
SID:	2829500
Source Port:	65515
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855072532026737 09/01/22-00:02:20.399331
SID:	2026737
Source Port:	55072
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858443532829498 09/01/22-00:03:43.862727
SID:	2829498
Source Port:	58443
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854590532829498 09/01/22-00:03:23.192418
SID:	2829498
Source Port:	54590
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849581532829500 09/01/22-00:03:11.014979
SID:	2829500
Source Port:	49581
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856754532026737 09/01/22-00:02:14.833183
SID:	2026737
Source Port:	56754
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849773532829498 09/01/22-00:03:05.323153
SID:	2829498
Source Port:	49773

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

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858444532829498 09/01/22-00:03:43.882038
SID:	2829498
Source Port:	58444
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853558532026737 09/01/22-00:03:13.174170
SID:	2026737
Source Port:	53558
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852105532829500 09/01/22-00:03:27.730338
SID:	2829500
Source Port:	52105
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849727532829498 09/01/22-00:02:01.394041
SID:	2829498
Source Port:	49727
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859301532829500 09/01/22-00:04:07.531976
SID:	2829500
Source Port:	59301
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858537532829500 09/01/22-00:02:23.186317
SID:	2829500
Source Port:	58537
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852101532829498 09/01/22-00:03:32.288887
SID:	2829498
Source Port:	52101
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853430532026737 09/01/22-00:03:47.092445
SID:	2026737
Source Port:	53430
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855595532026737 09/01/22-00:04:09.898241
SID:	2026737
Source Port:	55595
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852978532829500 09/01/22-00:03:40.236027
SID:	2829500
Source Port:	52978
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860912532026737 09/01/22-00:03:28.349098
SID:	2026737
Source Port:	60912
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851487532829498 09/01/22-00:02:06.112309
SID:	2829498
Source Port:	51487
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858628532829498 09/01/22-00:03:28.916264
SID:	2829498
Source Port:	58628
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851486532829498 09/01/22-00:02:06.080173
SID:	2829498
Source Port:	51486
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856118532026737 09/01/22-00:04:05.861618
SID:	2026737
Source Port:	56118

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849583532829500 09/01/22-00:03:11.058420
SID:	2829500
Source Port:	49583
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850565532829500 09/01/22-00:04:04.955935
SID:	2829500
Source Port:	50565
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859300532829500 09/01/22-00:04:07.513788
SID:	2829500
Source Port:	59300
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856692532026737 09/01/22-00:02:34.840093
SID:	2026737
Source Port:	56692
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860911532026737 09/01/22-00:03:28.331020
SID:	2026737
Source Port:	60911
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849584532829500 09/01/22-00:03:11.078564
SID:	2829500
Source Port:	49584
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853431532026737 09/01/22-00:03:47.111713
SID:	2026737
Source Port:	53431
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858874532829500 09/01/22-00:03:38.011985
SID:	2829500
Source Port:	58874
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850082532829500 09/01/22-00:03:34.671276
SID:	2829500
Source Port:	50082
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862062532829500 09/01/22-00:03:32.918939
SID:	2829500
Source Port:	62062
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855596532026737 09/01/22-00:04:09.918088
SID:	2026737
Source Port:	55596
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849962532026737 09/01/22-00:03:35.689392
SID:	2026737
Source Port:	49962
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858583532829498 09/01/22-00:02:31.210676
SID:	2829498
Source Port:	58583
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863941532026737 09/01/22-00:03:52.370596
SID:	2026737
Source Port:	63941
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855611532829498 09/01/22-00:03:36.403141
SID:	2829498
Source Port:	55611

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

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855614532829498 09/01/22-00:03:36.468326
SID:	2829498
Source Port:	55614
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861346532829498 09/01/22-00:02:38.490397
SID:	2829498
Source Port:	61346
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850091532829500 09/01/22-00:03:18.513860
SID:	2829500
Source Port:	50091
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860298532026737 09/01/22-00:03:33.383268
SID:	2026737
Source Port:	60298
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852896532026737 09/01/22-00:03:39.114275
SID:	2026737
Source Port:	52896
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864313532829498 09/01/22-00:03:58.875073
SID:	2829498
Source Port:	64313
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849726532829498 09/01/22-00:02:01.372827
SID:	2829498
Source Port:	49726
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860288532026737 09/01/22-00:02:53.105768
SID:	2026737
Source Port:	60288
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851726532829500 09/01/22-00:03:55.342624
SID:	2829500
Source Port:	51726
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850079532829500 09/01/22-00:03:34.606965
SID:	2829500
Source Port:	50079
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856753532026737 09/01/22-00:02:14.812380
SID:	2026737
Source Port:	56753
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862663532026737 09/01/22-00:02:25.489629
SID:	2026737
Source Port:	62663
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861019532829498 09/01/22-00:04:06.677904
SID:	2829498
Source Port:	61019
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861455532829500 09/01/22-00:02:03.672879
SID:	2829500
Source Port:	61455
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853977532829500 09/01/22-00:02:39.698321
SID:	2829500
Source Port:	53977

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865496532829500 09/01/22-00:03:29.520510
SID:	2829500
Source Port:	65496
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856685532829498 09/01/22-00:02:21.613022
SID:	2829498
Source Port:	56685
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864937532026737 09/01/22-00:02:42.055156
SID:	2026737
Source Port:	64937
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854369532026737 09/01/22-00:04:03.762307
SID:	2026737
Source Port:	54369
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865516532829500 09/01/22-00:02:32.934243
SID:	2829500
Source Port:	65516
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849266532829500 09/01/22-00:04:00.982711
SID:	2829500
Source Port:	49266
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858534532829500 09/01/22-00:02:23.120247
SID:	2829500
Source Port:	58534
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859585532829498 09/01/22-00:04:04.074500
SID:	2829498
Source Port:	59585
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850447532829498 09/01/22-00:03:53.986780
SID:	2829498
Source Port:	50447
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850906532829500 09/01/22-00:02:58.094801
SID:	2829500
Source Port:	50906
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852190532026737 09/01/22-00:03:21.145887
SID:	2026737
Source Port:	52190
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858877532829500 09/01/22-00:03:38.072921
SID:	2829500
Source Port:	58877
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861298532829498 09/01/22-00:03:15.537246
SID:	2829498
Source Port:	61298
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863449532829500 09/01/22-00:02:12.647016
SID:	2829500
Source Port:	63449
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853825532026737 09/01/22-00:03:02.730691
SID:	2026737
Source Port:	53825

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862937532026737 09/01/22-00:03:42.718178
SID:	2026737
Source Port:	62937
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864498532026737 09/01/22-00:03:56.346913
SID:	2026737
Source Port:	64498
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864314532829498 09/01/22-00:03:59.395837
SID:	2829498
Source Port:	64314
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855730532829500 09/01/22-00:03:44.550258
SID:	2829500
Source Port:	55730
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865118532829498 09/01/22-00:04:10.725130
SID:	2829498
Source Port:	65118
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856686532829498 09/01/22-00:02:21.631696
SID:	2829498
Source Port:	56686
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862661532026737 09/01/22-00:02:25.448208
SID:	2026737
Source Port:	62661
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850905532829500 09/01/22-00:02:58.072382
SID:	2829500
Source Port:	50905
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860023532829498 09/01/22-00:02:55.231073
SID:	2829498
Source Port:	60023
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849964532026737 09/01/22-00:03:35.733293
SID:	2026737
Source Port:	49964
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865332532829498 09/01/22-00:03:39.649023
SID:	2829498
Source Port:	65332
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860182532829498 09/01/22-00:03:48.263650
SID:	2829498
Source Port:	60182
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863731532829498 09/01/22-00:03:33.997566
SID:	2829498
Source Port:	63731
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858625532829498 09/01/22-00:03:28.850497
SID:	2829498
Source Port:	58625
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852102532829500 09/01/22-00:03:27.668953
SID:	2829500
Source Port:	52102

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865495532829500 09/01/22-00:03:29.499361
SID:	2829500
Source Port:	65495
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854588532829498 09/01/22-00:03:23.146755
SID:	2829498
Source Port:	54588
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855071532026737 09/01/22-00:02:20.380296
SID:	2026737
Source Port:	55071
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853429532026737 09/01/22-00:03:47.068211
SID:	2026737
Source Port:	53429
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863942532026737 09/01/22-00:03:52.388948
SID:	2026737
Source Port:	63942
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853974532829500 09/01/22-00:02:39.626606
SID:	2829500
Source Port:	53974
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854372532026737 09/01/22-00:04:03.823257
SID:	2026737
Source Port:	54372
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849263532829500 09/01/22-00:04:00.923809
SID:	2829500
Source Port:	49263
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853432532026737 09/01/22-00:03:47.130970
SID:	2026737
Source Port:	53432
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864934532026737 09/01/22-00:02:41.995822
SID:	2026737
Source Port:	64934
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852897532026737 09/01/22-00:03:39.132619
SID:	2026737
Source Port:	52897
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862939532026737 09/01/22-00:03:42.757239
SID:	2026737
Source Port:	62939
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861295532829498 09/01/22-00:03:15.476530
SID:	2829498
Source Port:	61295
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857485532026737 09/01/22-00:03:30.537077
SID:	2026737
Source Port:	57485
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859588532829498 09/01/22-00:04:04.134905
SID:	2829498
Source Port:	59588

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859223532829500 09/01/22-00:02:18.950858
SID:	2829500
Source Port:	59223
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853828532026737 09/01/22-00:03:02.797461
SID:	2026737
Source Port:	53828
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857382532829500 09/01/22-00:03:50.398087
SID:	2829500
Source Port:	57382
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860977532829498 09/01/22-00:02:16.533431
SID:	2829498
Source Port:	60977
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861349532829498 09/01/22-00:02:38.549773
SID:	2829498
Source Port:	61349
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858475532829498 09/01/22-00:02:46.486527
SID:	2829498
Source Port:	58475
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860287532026737 09/01/22-00:02:53.081721
SID:	2026737
Source Port:	60287
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861297532829498 09/01/22-00:03:15.516933
SID:	2829498
Source Port:	61297
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850088532829500 09/01/22-00:03:18.446546
SID:	2829500
Source Port:	50088
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859586532829498 09/01/22-00:04:04.094596
SID:	2829498
Source Port:	59586
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859299532829500 09/01/22-00:04:07.496000
SID:	2829500
Source Port:	59299
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852100532829498 09/01/22-00:03:32.267998
SID:	2829498
Source Port:	52100
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860184532829498 09/01/22-00:03:48.305240
SID:	2829498
Source Port:	60184
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860980532829498 09/01/22-00:02:16.604526
SID:	2829498
Source Port:	60980
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853976532829500 09/01/22-00:02:39.666430
SID:	2829500
Source Port:	53976

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865497532829500 09/01/22-00:03:29.542703
SID:	2829500
Source Port:	65497
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857379532829500 09/01/22-00:03:50.318564
SID:	2829500
Source Port:	57379
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861454532829500 09/01/22-00:02:03.654444
SID:	2829500
Source Port:	61454
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853560532026737 09/01/22-00:03:13.225920
SID:	2026737
Source Port:	53560
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852104532829500 09/01/22-00:03:27.710044
SID:	2829500
Source Port:	52104
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858445532829498 09/01/22-00:03:43.903621
SID:	2829498
Source Port:	58445
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856756532026737 09/01/22-00:02:14.874396
SID:	2026737
Source Port:	56756
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856684532829498 09/01/22-00:02:21.592544
SID:	2829498
Source Port:	56684
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853826532026737 09/01/22-00:03:02.751283
SID:	2026737
Source Port:	53826
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858586532829498 09/01/22-00:02:31.279996
SID:	2829498
Source Port:	58586
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849771532829498 09/01/22-00:03:05.189017
SID:	2829498
Source Port:	49771
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865334532829498 09/01/22-00:03:39.691657
SID:	2829498
Source Port:	65334
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861347532829498 09/01/22-00:02:38.510793
SID:	2829498
Source Port:	61347
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860021532829498 09/01/22-00:02:55.191369
SID:	2829498
Source Port:	60021
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855729532829500 09/01/22-00:03:44.527150
SID:	2829500
Source Port:	55729

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850907532829500 09/01/22-00:02:58.117260
SID:	2829500
Source Port:	50907
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859807532829500 09/01/22-00:03:55.275052
SID:	2829500
Source Port:	59807
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861021532829498 09/01/22-00:04:06.718974
SID:	2829498
Source Port:	61021
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859225532829500 09/01/22-00:02:19.007298
SID:	2829500
Source Port:	59225
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865326532026737 09/01/22-00:02:04.899187
SID:	2026737
Source Port:	65326
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860297532026737 09/01/22-00:03:33.363249
SID:	2026737
Source Port:	60297
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863733532829498 09/01/22-00:03:34.037884
SID:	2829498
Source Port:	63733
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849774532829498 09/01/22-00:03:05.512260
SID:	2829498
Source Port:	49774
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860289532026737 09/01/22-00:02:53.129672
SID:	2026737
Source Port:	60289
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.853557532026737 09/01/22-00:03:13.152000
SID:	2026737
Source Port:	53557
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858876532829500 09/01/22-00:03:38.053463
SID:	2829500
Source Port:	58876
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850081532829500 09/01/22-00:03:34.650981
SID:	2829500
Source Port:	50081
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852976532829500 09/01/22-00:03:40.199013
SID:	2829500
Source Port:	52976
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862664532026737 09/01/22-00:02:25.509064
SID:	2026737
Source Port:	62664
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864312532829498 09/01/22-00:03:58.856410
SID:	2829498
Source Port:	64312

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857487532026737 09/01/22-00:03:30.582629
SID:	2026737
Source Port:	57487
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856117532026737 09/01/22-00:04:05.841041
SID:	2026737
Source Port:	56117
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865517532829500 09/01/22-00:02:32.956296
SID:	2829500
Source Port:	65517
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852895532026737 09/01/22-00:03:39.091614
SID:	2026737
Source Port:	52895
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851724532829500 09/01/22-00:03:55.294608
SID:	2829500
Source Port:	51724
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860299532026737 09/01/22-00:03:33.401260
SID:	2026737
Source Port:	60299
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852098532829498 09/01/22-00:03:32.229187
SID:	2829498
Source Port:	52098
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849961532026737 09/01/22-00:03:35.669538
SID:	2026737
Source Port:	49961
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849265532829500 09/01/22-00:04:00.962398
SID:	2829500
Source Port:	49265
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860979532829498 09/01/22-00:02:16.584622
SID:	2829498
Source Port:	60979
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858477532829498 09/01/22-00:02:46.531265
SID:	2829498
Source Port:	58477
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857380532829500 09/01/22-00:03:50.340625
SID:	2829500
Source Port:	57380
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855613532829498 09/01/22-00:03:36.446288
SID:	2829498
Source Port:	55613
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862936532026737 09/01/22-00:03:42.697375
SID:	2026737
Source Port:	62936
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861020532829498 09/01/22-00:04:06.699436
SID:	2829498
Source Port:	61020

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861456532829500 09/01/22-00:02:03.693126
SID:	2829500
Source Port:	61456
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865498532829500 09/01/22-00:03:29.567003
SID:	2829500
Source Port:	65498
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850080532829500 09/01/22-00:03:34.627091
SID:	2829500
Source Port:	50080
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864936532026737 09/01/22-00:02:42.036797
SID:	2026737
Source Port:	64936
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859222532829500 09/01/22-00:02:18.931529
SID:	2829500
Source Port:	59222
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855612532829498 09/01/22-00:03:36.425992
SID:	2829498
Source Port:	55612
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857381532829500 09/01/22-00:03:50.368405
SID:	2829500
Source Port:	57381
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858536532829500 09/01/22-00:02:23.164990
SID:	2829500
Source Port:	58536
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862060532829500 09/01/22-00:03:32.873172
SID:	2829500
Source Port:	62060
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860179532829500 09/01/22-00:02:50.481998
SID:	2829500
Source Port:	60179
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.859298532829500 09/01/22-00:04:07.476417
SID:	2829500
Source Port:	59298
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860978532829498 09/01/22-00:02:16.558773
SID:	2829498
Source Port:	60978
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864496532026737 09/01/22-00:03:56.305340
SID:	2026737
Source Port:	64496
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863940532026737 09/01/22-00:03:52.350223
SID:	2026737
Source Port:	63940
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850090532829500 09/01/22-00:03:18.489552
SID:	2829500
Source Port:	50090

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850564532829500 09/01/22-00:04:04.937269
SID:	2829500
Source Port:	50564
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861018532829498 09/01/22-00:04:06.657229
SID:	2829498
Source Port:	61018
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849264532829500 09/01/22-00:04:00.944094
SID:	2829500
Source Port:	49264
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849772532829498 09/01/22-00:03:05.233383
SID:	2829498
Source Port:	49772
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865518532829500 09/01/22-00:02:32.980619
SID:	2829500
Source Port:	65518
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851725532829500 09/01/22-00:03:55.314556
SID:	2829500
Source Port:	51725
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.862061532829500 09/01/22-00:03:32.897217
SID:	2829500
Source Port:	62061
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852192532026737 09/01/22-00:03:21.187862
SID:	2026737
Source Port:	52192
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.864935532026737 09/01/22-00:02:42.016020
SID:	2026737
Source Port:	64935
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858875532829500 09/01/22-00:03:38.032851
SID:	2829500
Source Port:	58875
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863732532829498 09/01/22-00:03:34.017665
SID:	2829498
Source Port:	63732
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.861457532829500 09/01/22-00:02:03.713490
SID:	2829500
Source Port:	61457
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850449532829498 09/01/22-00:03:54.035960
SID:	2829498
Source Port:	50449
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856691532026737 09/01/22-00:02:34.816978
SID:	2026737
Source Port:	56691
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855731532829500 09/01/22-00:03:44.568358
SID:	2829500
Source Port:	55731

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849582532829500 09/01/22-00:03:11.038348
SID:	2829500
Source Port:	49582
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856687532829498 09/01/22-00:02:21.652316
SID:	2829498
Source Port:	56687
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.854370532026737 09/01/22-00:04:03.782854
SID:	2026737
Source Port:	54370
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852099532829498 09/01/22-00:03:32.248418
SID:	2829498
Source Port:	52099
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.857486532026737 09/01/22-00:03:30.561309
SID:	2026737
Source Port:	57486
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860022532829498 09/01/22-00:02:55.212194
SID:	2829498
Source Port:	60022
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852894532026737 09/01/22-00:03:39.072653
SID:	2026737
Source Port:	52894
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858627532829498 09/01/22-00:03:28.892335
SID:	2829498
Source Port:	58627
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.849728532829498 09/01/22-00:02:01.412620
SID:	2829498
Source Port:	49728
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860913532026737 09/01/22-00:03:28.369056
SID:	2026737
Source Port:	60913
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855073532026737 09/01/22-00:02:20.420031
SID:	2026737
Source Port:	55073
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855594532026737 09/01/22-00:04:09.880111
SID:	2026737
Source Port:	55594
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.856755532026737 09/01/22-00:02:14.854023
SID:	2026737
Source Port:	56755
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860181532829500 09/01/22-00:02:50.523251
SID:	2829500
Source Port:	60181
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.852977532829500 09/01/22-00:03:40.217833
SID:	2829500
Source Port:	52977

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

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863450532829500 09/01/22-00:02:12.666416
SID:	2829500
Source Port:	63450
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865335532829498 09/01/22-00:03:39.713005
SID:	2829498
Source Port:	65335
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.858585532829498 09/01/22-00:02:31.250178
SID:	2829498
Source Port:	58585
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.851488532829498 09/01/22-00:02:06.132219
SID:	2829498
Source Port:	51488
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.855728532829500 09/01/22-00:03:44.508575
SID:	2829500
Source Port:	55728
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.863943532026737 09/01/22-00:03:52.415647
SID:	2026737
Source Port:	63943
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.860296532026737 09/01/22-00:03:33.345251
SID:	2026737
Source Port:	60296
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.865327532026737 09/01/22-00:02:04.922757
SID:	2026737
Source Port:	65327
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 3 - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.58.8.8.850567532829500 09/01/22-00:04:04.998120
SID:	2829500
Source Port:	50567
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)

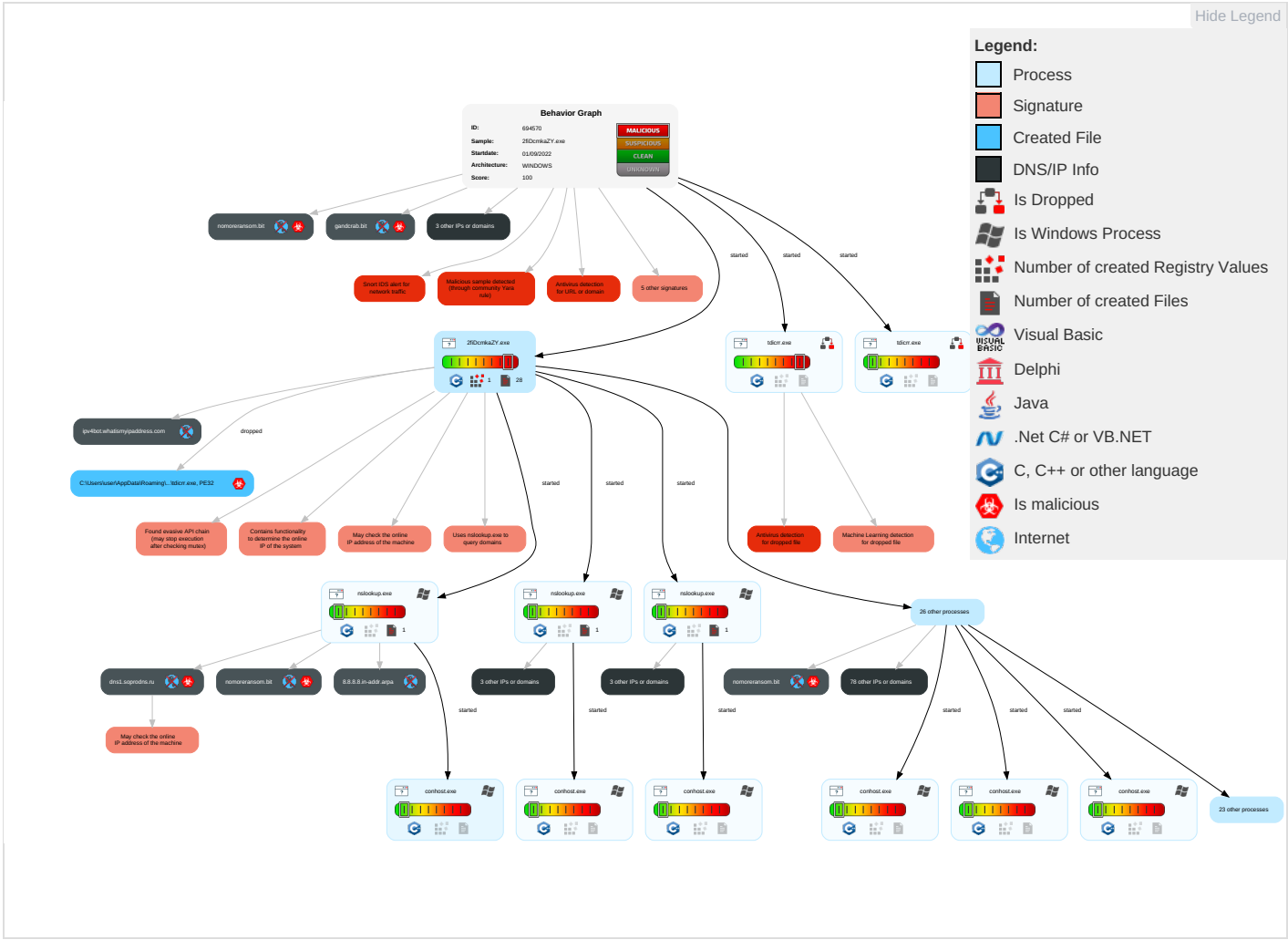
Malware Analysis System Evasion

- 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
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

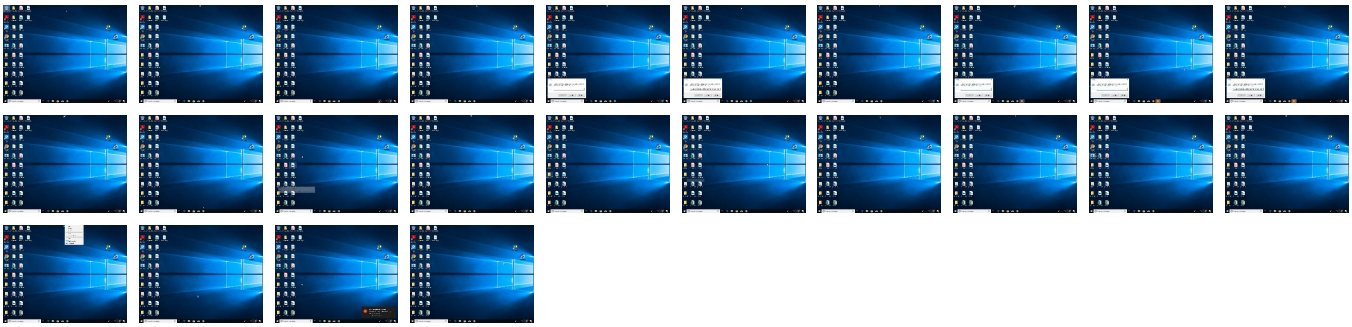
Behavior Graph



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
2fiDcmkaZY.exe	100%	ReversingLabs	Win32.Ransomware.GandCrab	
2fiDcmkaZY.exe	100%	Avira	TR/FileCoder.oytet	
2fiDcmkaZY.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.tdicrr.exe.c70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
20.2.tdicrr.exe.c70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
13.0.tdicrr.exe.c70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
0.2.2fiDcmkaZY.exe.a60000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.tdicrr.exe.c70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
0.0.2fiDcmkaZY.exe.a60000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbghvjyqy7jclk.onion.casa/2d028d577a0eb038	100%	Avira URL Cloud	malware	
http://gdcbghvjyqy7jclk.onion/2d028d577a0eb038	0%	Avira URL Cloud	safe	
http://gdcbghvjyqy7jclk.onion.top/2d028d577a0eb038	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.casa/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: malware	unknown
http://gdcbghvjyqy7jclk.onion.plus/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	false		high
http://gdcbghvjyqy7jclk.onion.rip/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	false		high
http://gdcbghvjyqy7jclk.onion/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.torproject.org/	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	false		high
http://gdcbghvjyqy7jclk.onion.top/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	true	• Avira URL Cloud: phishing	unknown
http://gdcbghvjyqy7jclk.onion.guide/2d028d577a0eb038	2fiDcmkaZY.exe, 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	2fiDcmkaZY.exe, 00000000.00000002.599059548.000000000120A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/n	2fiDcmkaZY.exe, 00000000.00000002.599059548.000000000120A000.00000004.00000020.00020000.00000000.sdmp	false		high

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:	694570
Start date and time:	2022-09-01 00:00:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2fiDcmkaZY.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:	70
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@128/2@436/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 78.1%) • Quality average: 67.4% • Quality standard deviation: 38.8%
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.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.
- VT rate limit hit for: 2fiDcmkaZY.exe

Simulations

Behavior and APIs

Time	Type	Description
00:01:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce tbmdhshhgoz "C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe"
00:02:00	API Interceptor	66x Sleep call for process: 2fiDcmkaZY.exe modified
00:02:09	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce tbmdhshhgoz "C:\Users\user\AppData\Roaming\Microsoft\tdicrr.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\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\2fiDcmkaZY.exe

File Type:	data
Category:	dropped
Size (bytes):	2219
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	9B515CE290886100F8C5F7C3AD0CB6A0
SHA1:	CF57023D314B0BAD4BCC41D552A31EC88FA56395
SHA-256:	186674F8434D142FE3E22F9A51A70FBE1F5161984D6A4B9EDE27B997C28D66EB
SHA-512:	5C7838FAEAC049C90E7AB1CED964CA7ED7F753894FBB7B270D5989631CCB3F40AE50F9579EC691DBB25A996F6ACCD66F2749952D3AEE793A3A83C54CF6BAA90F
Malicious:	false
Preview:	....

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

Process:	C:\Users\user\Desktop\2fiDcmkaZY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	75264
Entropy (8bit):	6.459228563179094
Encrypted:	false
SSDEEP:	1536:G55u555555555pmgSeGDjtQhnwmmB0ybMqqU+2bbbAV2/S2mr3IdE8mne0Avu5rJ:sMSjOnrmBTMqqDL2/mr3IdE8we0Avu5h
MD5:	D2E112FDFFC314778285E837BC0BED47
SHA1:	80902F2799D88F88DD99312023EF7086EE476566
SHA-256:	A49438E4A242B678CCFC5E8AB0B1A1082F107B2D043C245BC968954511AEF830
SHA-512:	CF8870AC369723A36D6363E6F28E24B443AADE41A464B3181AC73FDE654E0BEB137312F6819E8A82D3175B8DEF0FB466B61E04DC01C82C111E9DBB11CE2CB169
Malicious:	**true**
Yara Hits:	• Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: Joe Security • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: kevoreilly
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This +...tXm cannot be run in DOS mode....$.....AU@..4...4...4..Ce...4..Ce...4...f...4...4...4...L...4.../4...f...4...f...4...f...4..Rich.4.....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):	6.459199222303618
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2fiDcmkaZY.exe
File size:	75264
MD5:	a8ac57500de5dadf8c4db19959ddf2ec
SHA1:	202baa4b862222951619adc032fd2883562113b2
SHA256:	fcc7cc8f57d5a2a525d8026e81f69318262ca4e9036a726e26b1e3406f6f52d5
SHA512:	52ac5555cd39250903965ef6b30dbafcbe73e5f33b7d07a443cc3678e77ee3ce0736e2a70881f23c2002318b9dfba59d482cd724e5f8fdcf8084b2f6e6f826e8
SSDEEP:	1536:055u555555555pmgSeGDjtQhnwmmB0ybMqqU+2bbbAV2/S2mr3IdE8mne0Avu5rJ:mMSjOnrmBTMqqDL2/mr3IdE8we0Avu5h
TLSH:	4373391429D08233F6E3F977F5B47DE548397E9817883AEF10A254FA28251D24D39B8E
File Content Preview:	MZ.....@.....!..L.!This ...l!sm cannot be run in DOS mode....$.....AU@..4...4...4..Ce...4..Ce...4...f...4...4...4...L...4.../..4...f...4...f...4...f...4..Rich.4.....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 00007F4374BA6EFDh
push 00000000h
call dword ptr [00409168h]
pop ebp
ret
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]
xorps xmm0, xmm0
push 00000000h
push eax
mov esi, ecx

Instruction
movdqu dqword ptr [ebp-10h], xmm0
call 00007F4374BAB157h
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 00007F4374BA715Dh
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]

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

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

DLL	Import
GDI32.dll	TextOutW
ADVAPI32.dll	CryptExportKey, AllocateAndInitializeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, FreeSid
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
192.168.2.58.8.8.8601805 32829500 09/01/22-00:02:50.502751	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60180	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8543715 32026737 09/01/22-00:04:03.802921	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54371	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584745 32829498 09/01/22-00:02:46.409357	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58474	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566905 32026737 09/01/22-00:02:34.794476	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56690	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8529755 32829500 09/01/22-00:03:40.177431	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52975	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592245 32829500 09/01/22-00:02:18.976716	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59224	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8539755 32829500 09/01/22-00:02:39.645914	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53975	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8613485 32829498 09/01/22-00:02:38.530362	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61348	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8600245 32829498 09/01/22-00:02:55.250291	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60024	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8538275 32026737 09/01/22-00:03:02.774286	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53827	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609105 32026737 09/01/22-00:03:28.310952	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60910	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8637305 32829498 09/01/22-00:03:33.977550	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	63730	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601835 32829498 09/01/22-00:03:48.283959	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60183	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8545875 32829498 09/01/22-00:03:23.124735	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54587	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8509045 32829500 09/01/22-00:02:58.051616	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50904	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8550705 32026737 09/01/22-00:02:20.361607	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55070	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500895 32829500 09/01/22-00:03:18.466985	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50089	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8595875 32829498 09/01/22-00:04:04.114751	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59587	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8555975 32026737 09/01/22-00:04:09.936181	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55597	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653255 32026737 09/01/22-00:02:04.877624	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65325	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8626625 32026737 09/01/22-00:02:25.469721	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62662	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8651205 32829498 09/01/22-00:04:10.763289	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65120	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8612965 32829498 09/01/22-00:03:15.496749	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61296	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8574845 32026737 09/01/22-00:03:30.517521	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57484	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584465 32829498 09/01/22-00:03:43.925486	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58446	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8643155 32829498 09/01/22-00:03:59.415810	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64315	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653335 32829498 09/01/22-00:03:39.670910	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65333	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521935 32026737 09/01/22-00:03:21.210468	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52193	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521035 32829500 09/01/22-00:03:27.689357	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52103	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8651195 32829498 09/01/22-00:04:10.743391	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65119	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8505665 32829500 09/01/22-00:04:04.976212	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50566	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8634485 32829500 09/01/22-00:02:12.612834	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63448	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8620595 32829500 09/01/22-00:03:32.850991	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62059	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584765 32829498 09/01/22-00:02:46.511401	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58476	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8629385 32026737 09/01/22-00:03:42.736982	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62938	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601815 32829498 09/01/22-00:03:48.237956	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60181	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8586265 32829498 09/01/22-00:03:28.872267	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58626	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653285 32026737 09/01/22-00:02:04.942715	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65328	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8644975 32026737 09/01/22-00:03:56.326355	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64497	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602865 32026737 09/01/22-00:02:53.057441	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60286	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8535595 32026737 09/01/22-00:03:13.202744	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53559	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8504465 32829498 09/01/22-00:03:53.963216	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50446	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8561165 32026737 09/01/22-00:04:05.801650	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56116	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497295 32829498 09/01/22-00:02:01.433122	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49729	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8634515 32829500 09/01/22-00:02:12.684530	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63451	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585355 32829500 09/01/22-00:02:23.142881	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58535	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8504485 32829498 09/01/22-00:03:54.015145	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50448	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8644995 32026737 09/01/22-00:03:56.365974	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64499	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8514895 32829498 09/01/22-00:02:06.151880	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51489	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8651175 32829498 09/01/22-00:04:10.704503	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65117	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521915 32026737 09/01/22-00:03:21.167674	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52191	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8561195 32026737 09/01/22-00:04:05.881610	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56119	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566895 32026737 09/01/22-00:02:34.772206	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56689	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585845 32829498 09/01/22-00:02:31.231912	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58584	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8499635 32026737 09/01/22-00:03:35.711880	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49963	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601825 32829500 09/01/22-00:02:50.545957	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60182	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8545895 32829498 09/01/22-00:03:23.168676	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54589	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8655155 32829500 09/01/22-00:02:32.912023	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65515	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8550725 32026737 09/01/22-00:02:20.399331	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55072	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584435 32829498 09/01/22-00:03:43.862727	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58443	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8545905 32829498 09/01/22-00:03:23.192418	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54590	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8495815 32829500 09/01/22-00:03:11.014979	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49581	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8567545 32026737 09/01/22-00:02:14.833183	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56754	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497735 32829498 09/01/22-00:03:05.323153	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49773	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584445 32829498 09/01/22-00:03:43.882038	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58444	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8535585 32026737 09/01/22-00:03:13.174170	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53558	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521055 32829500 09/01/22-00:03:27.730338	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52105	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497275 32829498 09/01/22-00:02:01.394041	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49727	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8593015 32829500 09/01/22-00:04:07.531976	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59301	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585375 32829500 09/01/22-00:02:23.186317	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58537	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521015 32829498 09/01/22-00:03:32.288887	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52101	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8534305 32026737 09/01/22-00:03:47.092445	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53430	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8555955 32026737 09/01/22-00:04:09.898241	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55595	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8529785 32829500 09/01/22-00:03:40.236027	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52978	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609125 32026737 09/01/22-00:03:28.349098	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60912	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8514875 32829498 09/01/22-00:02:06.112309	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51487	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8586285 32829498 09/01/22-00:03:28.916264	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58628	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8514865 32829498 09/01/22-00:02:06.080173	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51486	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8561185 32026737 09/01/22-00:04:05.861618	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56118	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8495835 32829500 09/01/22-00:03:11.058420	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49583	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8505655 32829500 09/01/22-00:04:04.955935	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50565	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8593005 32829500 09/01/22-00:04:07.513788	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59300	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566925 32026737 09/01/22-00:02:34.840093	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56692	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609115 32026737 09/01/22-00:03:28.331020	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60911	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8495845 32829500 09/01/22-00:03:11.078564	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49584	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8534315 32026737 09/01/22-00:03:47.111713	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53431	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8588745 32829500 09/01/22-00:03:38.011985	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58874	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500825 32829500 09/01/22-00:03:34.671276	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50082	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8620625 32829500 09/01/22-00:03:32.918939	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62062	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8555965 32026737 09/01/22-00:04:09.918088	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55596	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8499625 32026737 09/01/22-00:03:35.689392	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49962	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585835 32829498 09/01/22-00:02:31.210676	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58583	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8639415 32026737 09/01/22-00:03:52.370596	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63941	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8556115 32829498 09/01/22-00:03:36.403141	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55611	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8556145 32829498 09/01/22-00:03:36.468326	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55614	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8613465 32829498 09/01/22-00:02:38.490397	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61346	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500915 32829500 09/01/22-00:03:18.513860	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50091	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602985 32026737 09/01/22-00:03:33.383268	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60298	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8528965 32026737 09/01/22-00:03:39.114275	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52896	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8643135 32829498 09/01/22-00:03:58.875073	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64313	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497265 32829498 09/01/22-00:02:01.372827	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49726	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602885 32026737 09/01/22-00:02:53.105768	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60288	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8517265 32829500 09/01/22-00:03:55.342624	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51726	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500795 32829500 09/01/22-00:03:34.606965	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50079	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8567535 32026737 09/01/22-00:02:14.812380	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56753	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8626635 32026737 09/01/22-00:02:25.489629	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62663	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8610195 32829498 09/01/22-00:04:06.677904	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61019	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8614555 32829500 09/01/22-00:02:03.672879	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61455	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8539775 32829500 09/01/22-00:02:39.698321	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53977	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8654965 32829500 09/01/22-00:03:29.520510	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65496	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566855 32829498 09/01/22-00:02:21.613022	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56685	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8649375 32026737 09/01/22-00:02:42.055156	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64937	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8543695 32026737 09/01/22-00:04:03.762307	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54369	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8655165 32829500 09/01/22-00:02:32.934243	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65516	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8492665 32829500 09/01/22-00:04:00.982711	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49266	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8585345 32829500 09/01/22-00:02:23.120247	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58534	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8595855 32829498 09/01/22-00:04:04.074500	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59585	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8504475 32829498 09/01/22-00:03:53.986780	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50447	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8509065 32829500 09/01/22-00:02:58.094801	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50906	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521905 32026737 09/01/22-00:03:21.145887	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52190	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8588775 32829500 09/01/22-00:03:38.072921	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58877	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8612985 32829498 09/01/22-00:03:15.537246	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61298	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8634495 32829500 09/01/22-00:02:12.647016	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63449	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8538255 32026737 09/01/22-00:03:02.730691	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53825	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8629375 32026737 09/01/22-00:03:42.718178	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62937	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8644985 32026737 09/01/22-00:03:56.346913	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64498	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8643145 32829498 09/01/22-00:03:59.395837	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64314	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8557305 32829500 09/01/22-00:03:44.550258	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	55730	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8651185 32829498 09/01/22-00:04:10.725130	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65118	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566865 32829498 09/01/22-00:02:21.631696	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56686	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8626615 32026737 09/01/22-00:02:25.448208	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62661	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8509055 32829500 09/01/22-00:02:58.072382	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50905	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8600235 32829498 09/01/22-00:02:55.231073	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60023	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8499645 32026737 09/01/22-00:03:35.733293	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49964	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653325 32829498 09/01/22-00:03:39.649023	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65332	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601825 32829498 09/01/22-00:03:48.263650	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60182	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8637315 32829498 09/01/22-00:03:33.997566	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	63731	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8586255 32829498 09/01/22-00:03:28.850497	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58625	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521025 32829500 09/01/22-00:03:27.668953	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52102	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8654955 32829500 09/01/22-00:03:29.499361	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65495	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8545885 32829498 09/01/22-00:03:23.146755	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	54588	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8550715 32026737 09/01/22-00:02:20.380296	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55071	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8534295 32026737 09/01/22-00:03:47.068211	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53429	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8639425 32026737 09/01/22-00:03:52.388948	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63942	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8539745 32829500 09/01/22-00:02:39.626606	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53974	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8543725 32026737 09/01/22-00:04:03.823257	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54372	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8492635 32829500 09/01/22-00:04:00.923809	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49263	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8534325 32026737 09/01/22-00:03:47.130970	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53432	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8649345 32026737 09/01/22-00:02:41.995822	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64934	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8528975 32026737 09/01/22-00:03:39.132619	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52897	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8629395 32026737 09/01/22-00:03:42.757239	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62939	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8612955 32829498 09/01/22-00:03:15.476530	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61295	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8574855 32026737 09/01/22-00:03:30.537077	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57485	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8595885 32829498 09/01/22-00:04:04.134905	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59588	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592235 32829500 09/01/22-00:02:18.950858	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59223	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8538285 32026737 09/01/22-00:03:02.797461	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53828	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8573825 32829500 09/01/22-00:03:50.398087	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	57382	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609775 32829498 09/01/22-00:02:16.533431	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60977	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8613495 32829498 09/01/22-00:02:38.549773	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61349	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584755 32829498 09/01/22-00:02:46.486527	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58475	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602875 32026737 09/01/22-00:02:53.081721	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60287	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8612975 32829498 09/01/22-00:03:15.516933	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61297	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500885 32829500 09/01/22-00:03:18.446546	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50088	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8595865 32829498 09/01/22-00:04:04.094596	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	59586	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592995 32829500 09/01/22-00:04:07.496000	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59299	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8521005 32829498 09/01/22-00:03:32.267998	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52100	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601845 32829498 09/01/22-00:03:48.305240	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60184	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609805 32829498 09/01/22-00:02:16.604526	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60980	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8539765 32829500 09/01/22-00:02:39.666430	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	53976	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8654975 32829500 09/01/22-00:03:29.542703	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65497	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8573795 32829500 09/01/22-00:03:50.318564	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	57379	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8614545 32829500 09/01/22-00:02:03.654444	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61454	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8535605 32026737 09/01/22-00:03:13.225920	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53560	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521045 32829500 09/01/22-00:03:27.710044	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52104	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584455 32829498 09/01/22-00:03:43.903621	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58445	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8567565 32026737 09/01/22-00:02:14.874396	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56756	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566845 32829498 09/01/22-00:02:21.592544	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56684	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8538265 32026737 09/01/22-00:03:02.751283	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53826	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585865 32829498 09/01/22-00:02:31.279996	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58586	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497715 32829498 09/01/22-00:03:05.189017	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49771	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653345 32829498 09/01/22-00:03:39.691657	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65334	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8613475 32829498 09/01/22-00:02:38.510793	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61347	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8600215 32829498 09/01/22-00:02:55.191369	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60021	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8557295 32829500 09/01/22-00:03:44.527150	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	55729	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8509075 32829500 09/01/22-00:02:58.117260	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50907	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8598075 32829500 09/01/22-00:03:55.275052	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59807	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8610215 32829498 09/01/22-00:04:06.718974	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61021	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592255 32829500 09/01/22-00:02:19.007298	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59225	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653265 32026737 09/01/22-00:02:04.899187	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65326	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602975 32026737 09/01/22-00:03:33.363249	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60297	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8637335 32829498 09/01/22-00:03:34.037884	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	63733	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497745 32829498 09/01/22-00:03:05.512260	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49774	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602895 32026737 09/01/22-00:02:53.129672	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60289	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8535575 32026737 09/01/22-00:03:13.152000	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53557	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8588765 32829500 09/01/22-00:03:38.053463	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58876	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500815 32829500 09/01/22-00:03:34.650981	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50081	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8529765 32829500 09/01/22-00:03:40.199013	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52976	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8626645 32026737 09/01/22-00:02:25.509064	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62664	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8643125 32829498 09/01/22-00:03:58.856410	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	64312	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8574875 32026737 09/01/22-00:03:30.582629	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57487	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8561175 32026737 09/01/22-00:04:05.841041	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56117	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8655175 32829500 09/01/22-00:02:32.956296	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65517	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8528955 32026737 09/01/22-00:03:39.091614	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52895	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8517245 32829500 09/01/22-00:03:55.294608	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51724	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8602995 32026737 09/01/22-00:03:33.401260	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60299	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8520985 32829498 09/01/22-00:03:32.229187	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52098	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8499615 32026737 09/01/22-00:03:35.669538	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49961	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8492655 32829500 09/01/22-00:04:00.962398	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49265	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609795 32829498 09/01/22-00:02:16.584622	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60979	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8584775 32829498 09/01/22-00:02:46.531265	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58477	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8573805 32829500 09/01/22-00:03:50.340625	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	57380	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8556135 32829498 09/01/22-00:03:36.446288	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55613	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8629365 32026737 09/01/22-00:03:42.697375	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	62936	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8610205 32829498 09/01/22-00:04:06.699436	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61020	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8614565 32829500 09/01/22-00:02:03.693126	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61456	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8654985 32829500 09/01/22-00:03:29.567003	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65498	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500805 32829500 09/01/22-00:03:34.627091	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50080	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8649365 32026737 09/01/22-00:02:42.036797	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64936	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592225 32829500 09/01/22-00:02:18.931529	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59222	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8556125 32829498 09/01/22-00:03:36.425992	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	55612	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8573815 32829500 09/01/22-00:03:50.368405	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	57381	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585365 32829500 09/01/22-00:02:23.164990	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58536	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8620605 32829500 09/01/22-00:03:32.873172	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62060	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601795 32829500 09/01/22-00:02:50.481998	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60179	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8592985 32829500 09/01/22-00:04:07.476417	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	59298	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609785 32829498 09/01/22-00:02:16.558773	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60978	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8644965 32026737 09/01/22-00:03:56.305340	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64496	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8639405 32026737 09/01/22-00:03:52.350223	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63940	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8500905 32829500 09/01/22-00:03:18.489552	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50090	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8505645 32829500 09/01/22-00:04:04.937269	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50564	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8610185 32829498 09/01/22-00:04:06.657229	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61018	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8492645 32829500 09/01/22-00:04:00.944094	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49264	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497725 32829498 09/01/22-00:03:05.233383	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49772	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8655185 32829500 09/01/22-00:02:32.980619	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	65518	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8517255 32829500 09/01/22-00:03:55.314556	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	51725	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8620615 32829500 09/01/22-00:03:32.897217	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	62061	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8521925 32026737 09/01/22-00:03:21.187862	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52192	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8649355 32026737 09/01/22-00:02:42.016020	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64935	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8588755 32829500 09/01/22-00:03:38.032851	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	58875	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8637325 32829498 09/01/22-00:03:34.017665	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	63732	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8614575 32829500 09/01/22-00:02:03.713490	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	61457	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8504495 32829498 09/01/22-00:03:54.035960	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50449	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566915 32026737 09/01/22-00:02:34.816978	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56691	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8557315 32829500 09/01/22-00:03:44.568358	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	55731	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8495825 32829500 09/01/22-00:03:11.038348	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	49582	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8566875 32829498 09/01/22-00:02:21.652316	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56687	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8543705 32026737 09/01/22-00:04:03.782854	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54370	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8520995 32829498 09/01/22-00:03:32.248418	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52099	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8574865 32026737 09/01/22-00:03:30.561309	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	57486	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8600225 32829498 09/01/22-00:02:55.212194	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60022	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8528945 32026737 09/01/22-00:03:39.072653	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	52894	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8586275 32829498 09/01/22-00:03:28.892335	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58627	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8497285 32829498 09/01/22-00:02:01.412620	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	49728	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8609135 32026737 09/01/22-00:03:28.369056	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60913	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8550735 32026737 09/01/22-00:02:20.420031	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55073	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8555945 32026737 09/01/22-00:04:09.880111	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	55594	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8567555 32026737 09/01/22-00:02:14.854023	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56755	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8601815 32829500 09/01/22-00:02:50.523251	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	60181	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8529775 32829500 09/01/22-00:03:40.217833	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	52977	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8634505 32829500 09/01/22-00:02:12.666416	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	63450	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653355 32829498 09/01/22-00:03:39.713005	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65335	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8585855 32829498 09/01/22-00:02:31.250178	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58585	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8514885 32829498 09/01/22-00:02:06.132219	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51488	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8557285 32829500 09/01/22-00:03:44.508575	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	55728	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8639435 32026737 09/01/22-00:03:52.415647	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63943	53	192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8602965 32026737 09/01/22-00:03:33.345251	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60296	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8653275 32026737 09/01/22-00:02:04.922757	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65327	53	192.168.2.5	8.8.8.8
192.168.2.58.8.8.8505675 32829500 09/01/22-00:04:04.998120	UDP	2829500	ETPRO TROJAN GandCrab DNS Lookup 3	50567	53	192.168.2.5	8.8.8.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:01:59.911590099 CEST	49177	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:01:59.931437016 CEST	53	49177	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.239926100 CEST	49724	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.334580898 CEST	53	49724	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.352194071 CEST	49725	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.372085094 CEST	53	49725	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.372827053 CEST	49726	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.393094063 CEST	53	49726	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.394041061 CEST	49727	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.412072897 CEST	53	49727	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.412620068 CEST	49728	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.432477951 CEST	53	49728	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:01.433121920 CEST	49729	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:01.453190088 CEST	53	49729	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:02.555277109 CEST	61452	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.563941002 CEST	61452	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.608334064 CEST	53	61452	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.633827925 CEST	53	61452	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.633877039 CEST	61453	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.653230906 CEST	53	61453	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.654443979 CEST	61454	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.672249079 CEST	53	61454	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.672878981 CEST	61455	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.692581892 CEST	53	61455	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.693125963 CEST	61456	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.712928057 CEST	53	61456	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:03.713490009 CEST	61457	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:03.733714104 CEST	53	61457	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.721681118 CEST	65323	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.834590912 CEST	53	65323	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.856112003 CEST	65324	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.876791954 CEST	53	65324	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.877624035 CEST	65325	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.898612976 CEST	53	65325	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.899187088 CEST	65326	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.920192003 CEST	53	65326	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.922756910 CEST	65327	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.941993952 CEST	53	65327	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:04.942714930 CEST	65328	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:04.961915970 CEST	53	65328	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:06.005309105 CEST	51484	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.042258024 CEST	53	51484	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:06.059837103 CEST	51485	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.078336954 CEST	53	51485	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:06.080173016 CEST	51486	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.101386070 CEST	53	51486	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:06.112308979 CEST	51487	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.131583929 CEST	53	51487	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:06.132219076 CEST	51488	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.151202917 CEST	53	51488	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:06.151880026 CEST	51489	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:06.173470020 CEST	53	51489	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:11.007499933 CEST	63446	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.022016048 CEST	63446	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.567970991 CEST	53	63446	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:12.591213942 CEST	63447	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.610974073 CEST	53	63447	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:12.612833977 CEST	63448	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.632694960 CEST	53	63448	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:12.647016048 CEST	63449	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.665808916 CEST	53	63449	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:12.666415930 CEST	63450	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.684042931 CEST	53	63450	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:12.684530020 CEST	63451	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:12.704040051 CEST	53	63451	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:13.709269047 CEST	56751	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.739041090 CEST	56751	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.775738955 CEST	53	56751	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:14.792093039 CEST	56752	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.811539888 CEST	53	56752	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:14.812380075 CEST	56753	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.832356930 CEST	53	56753	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:14.833183050 CEST	56754	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.853168011 CEST	53	56754	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:14.854022980 CEST	56755	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.873765945 CEST	53	56755	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:14.874396086 CEST	56756	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:14.894181013 CEST	53	56756	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:15.249150038 CEST	53	56751	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:15.933274984 CEST	55039	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.027390957 CEST	53	63446	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.471765041 CEST	53	55039	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.490912914 CEST	60976	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.512093067 CEST	53	60976	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.533431053 CEST	60977	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.554326057 CEST	53	60977	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.558773041 CEST	60978	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.580204964 CEST	53	60978	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.584621906 CEST	60979	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.603900909 CEST	53	60979	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:16.604526043 CEST	60980	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:16.625678062 CEST	53	60980	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:18.327372074 CEST	59220	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:18.866029978 CEST	53	59220	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:18.912621975 CEST	59221	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:18.930771112 CEST	53	59221	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:18.931529045 CEST	59222	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:18.950180054 CEST	53	59222	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:18.950858116 CEST	59223	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:18.971628904 CEST	53	59223	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:18.976716042 CEST	59224	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:18.997745991 CEST	53	59224	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:19.007297993 CEST	59225	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:19.028003931 CEST	53	59225	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.212028027 CEST	55068	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:20.281924009 CEST	53	55068	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.343282938 CEST	55069	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:20.360511065 CEST	53	55069	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.361607075 CEST	55070	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:20.379569054 CEST	53	55070	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.380295992 CEST	55071	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:20.398627043 CEST	53	55071	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.399331093 CEST	55072	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:20.419385910 CEST	53	55072	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:20.420031071 CEST	55073	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:20.438457966 CEST	53	55073	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.510334015 CEST	56682	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.547008991 CEST	53	56682	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.570235014 CEST	56683	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.589804888 CEST	53	56683	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.592544079 CEST	56684	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.612307072 CEST	53	56684	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.613022089 CEST	56685	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.631066084 CEST	53	56685	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.631695986 CEST	56686	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.651690006 CEST	53	56686	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:21.652316093 CEST	56687	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:21.670263052 CEST	53	56687	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:22.988415956 CEST	58532	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.073178053 CEST	53	58532	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:23.090640068 CEST	58533	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.108946085 CEST	53	58533	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:23.120246887 CEST	58534	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.139523029 CEST	53	58534	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:23.142880917 CEST	58535	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.164510012 CEST	53	58535	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:23.164989948 CEST	58536	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.185849905 CEST	53	58536	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:23.186316967 CEST	58537	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:23.208182096 CEST	53	58537	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:24.293374062 CEST	62659	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.285326958 CEST	62659	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.395417929 CEST	53	62659	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:25.416001081 CEST	62660	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.436459064 CEST	53	62660	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:25.448208094 CEST	62661	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.469156981 CEST	53	62661	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:25.469721079 CEST	62662	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.489044905 CEST	53	62662	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:25.489629030 CEST	62663	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.508452892 CEST	53	62663	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:25.509063959 CEST	62664	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:25.530004978 CEST	53	62664	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:28.241271019 CEST	53	62659	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:30.590687990 CEST	58581	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.166659117 CEST	53	58581	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:31.191478968 CEST	58582	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.209889889 CEST	53	58582	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:31.210675955 CEST	58583	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.231199026 CEST	53	58583	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:31.231911898 CEST	58584	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.249490976 CEST	53	58584	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:31.250178099 CEST	58585	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.269680977 CEST	53	58585	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:31.279995918 CEST	58586	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:31.300205946 CEST	53	58586	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:32.336535931 CEST	56263	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:32.866913080 CEST	53	56263	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:32.885988951 CEST	65514	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:32.905796051 CEST	53	65514	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:32.912023067 CEST	65515	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:32.933625937 CEST	53	65515	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:32.934242964 CEST	65516	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:32.955260038 CEST	53	65516	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:32.956295967 CEST	65517	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:32.979974985 CEST	53	65517	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:32.980618954 CEST	65518	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:33.001955032 CEST	53	65518	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.142494917 CEST	56687	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.717264891 CEST	53	56687	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.743534088 CEST	56688	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.764400959 CEST	53	56688	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.772206068 CEST	56689	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.793865919 CEST	53	56689	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.794476032 CEST	56690	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.816371918 CEST	53	56690	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.816977978 CEST	56691	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.839456081 CEST	53	56691	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:34.840092897 CEST	56692	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:34.859596014 CEST	53	56692	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:35.871191025 CEST	64419	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:36.910881996 CEST	64419	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:37.964308977 CEST	64419	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.451112986 CEST	53	64419	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.469635963 CEST	61345	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.489614010 CEST	53	61345	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.490396976 CEST	61346	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.510234118 CEST	53	61346	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.510792971 CEST	61347	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.529823065 CEST	53	61347	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.530361891 CEST	61348	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.544522047 CEST	53	64419	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.549093008 CEST	53	61348	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:38.549772978 CEST	61349	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:38.569746971 CEST	53	61349	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.005251884 CEST	53	64419	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.543435097 CEST	53972	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.580847025 CEST	53	53972	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.608720064 CEST	53973	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.625894070 CEST	53	53973	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.626605988 CEST	53974	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.645344973 CEST	53	53974	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.645914078 CEST	53975	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.665539026 CEST	53	53975	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.666429996 CEST	53976	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.686157942 CEST	53	53976	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:39.698321104 CEST	53977	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:39.718056917 CEST	53	53977	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:41.365394115 CEST	64932	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:41.948688984 CEST	53	64932	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:41.974438906 CEST	64933	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:41.993784904 CEST	53	64933	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:41.995821953 CEST	64934	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:42.015419006 CEST	53	64934	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:42.016020060 CEST	64935	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:42.035979033 CEST	53	64935	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:42.036797047 CEST	64936	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:42.054507971 CEST	53	64936	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:42.055155993 CEST	64937	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:42.075145006 CEST	53	64937	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:43.388982058 CEST	58472	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:44.405422926 CEST	58472	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:45.428538084 CEST	58472	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.031758070 CEST	53	58472	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.391263008 CEST	58473	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.408472061 CEST	53	58473	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.409357071 CEST	58474	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.428978920 CEST	53	58474	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.486526966 CEST	58475	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.506362915 CEST	53	58475	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.511400938 CEST	58476	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.529474020 CEST	53	58476	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.531265020 CEST	58477	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:46.550900936 CEST	53	58477	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:46.627775908 CEST	53	58472	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:47.232079029 CEST	53	58472	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.357605934 CEST	60177	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.431725979 CEST	53	60177	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.462135077 CEST	60178	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.481153965 CEST	53	60178	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.481997967 CEST	60179	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.502183914 CEST	53	60179	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.502751112 CEST	60180	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.522468090 CEST	53	60180	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.523251057 CEST	60181	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.545125961 CEST	53	60181	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:50.545957088 CEST	60182	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:50.565229893 CEST	53	60182	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:51.939711094 CEST	60284	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:52.973716974 CEST	60284	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.012386084 CEST	53	60284	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:53.031869888 CEST	60285	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.051094055 CEST	53	60285	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:53.057440996 CEST	60286	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.081031084 CEST	53	60286	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:53.081721067 CEST	60287	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.105006933 CEST	53	60287	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:53.105767965 CEST	60288	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.129003048 CEST	53	60288	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:53.129672050 CEST	60289	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:53.152440071 CEST	53	60289	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:54.129081964 CEST	60019	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.115514040 CEST	60019	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.143107891 CEST	53	60019	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:55.169272900 CEST	60020	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.190500021 CEST	53	60020	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:55.191369057 CEST	60021	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.211363077 CEST	53	60021	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:55.212193966 CEST	60022	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.230350971 CEST	53	60022	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:55.231072903 CEST	60023	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.249286890 CEST	53	60023	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:55.250291109 CEST	60024	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:55.269426107 CEST	53	60024	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:55.303771973 CEST	53	60019	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:56.391621113 CEST	50902	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:56.963818073 CEST	53	60284	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:57.439699888 CEST	50902	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.006582975 CEST	53	50902	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.030960083 CEST	50903	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.050683022 CEST	53	50903	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.051615953 CEST	50904	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.055273056 CEST	53	50902	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.071692944 CEST	53	50904	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.072381973 CEST	50905	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.092132092 CEST	53	50905	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.094800949 CEST	50906	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.112858057 CEST	53	50906	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:58.117259979 CEST	50907	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:02:58.137913942 CEST	53	50907	8.8.8.8	192.168.2.5
Sep 1, 2022 00:02:59.546935081 CEST	53823	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:00.539176941 CEST	53823	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:01.593920946 CEST	53823	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.673258066 CEST	53	53823	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:02.707921982 CEST	53824	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.728626013 CEST	53	53824	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:02.730690956 CEST	53825	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.749336004 CEST	53	53825	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:02.751282930 CEST	53826	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.772249937 CEST	53	53826	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:02.774286032 CEST	53827	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.794682980 CEST	53	53827	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:02.797461033 CEST	53828	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:02.818588018 CEST	53	53828	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:03.269387960 CEST	53	53823	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:04.074176073 CEST	49769	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:04.564574957 CEST	53	53823	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.102104902 CEST	49769	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.140230894 CEST	53	49769	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.167689085 CEST	49770	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.186117887 CEST	53	49770	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.189017057 CEST	49771	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.209920883 CEST	53	49771	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.233382940 CEST	49772	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.252963066 CEST	53	49772	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.323153019 CEST	49773	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.340817928 CEST	53	49773	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:05.512259960 CEST	49774	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:05.533775091 CEST	53	49774	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:09.094862938 CEST	53	49769	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:10.430033922 CEST	49579	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:10.970557928 CEST	53	49579	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:10.994596958 CEST	49580	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:11.013236046 CEST	53	49580	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:11.014978886 CEST	49581	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:11.036653042 CEST	53	49581	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:11.038347960 CEST	49582	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:11.057737112 CEST	53	49582	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:11.058419943 CEST	49583	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:11.077819109 CEST	53	49583	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:11.078563929 CEST	49584	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:11.099826097 CEST	53	49584	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:12.533488035 CEST	53555	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:13.112035036 CEST	53	53555	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:13.129920006 CEST	53556	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:13.151115894 CEST	53	53556	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:13.151999950 CEST	53557	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:13.173320055 CEST	53	53557	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:13.174170017 CEST	53558	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:13.196038961 CEST	53	53558	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:13.202744007 CEST	53559	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:13.224518061 CEST	53	53559	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:13.225919962 CEST	53560	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:13.246552944 CEST	53	53560	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:14.898765087 CEST	61293	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.436304092 CEST	53	61293	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:15.455348969 CEST	61294	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.474445105 CEST	53	61294	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:15.476530075 CEST	61295	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.496115923 CEST	53	61295	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:15.496748924 CEST	61296	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.516382933 CEST	53	61296	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:15.516932964 CEST	61297	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.536484003 CEST	53	61297	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:15.537245989 CEST	61298	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:15.554661036 CEST	53	61298	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:17.268368959 CEST	50086	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.259387016 CEST	50086	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.395138979 CEST	53	50086	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:18.425247908 CEST	50087	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.445703030 CEST	53	50087	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:18.446546078 CEST	50088	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.466348886 CEST	53	50088	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:18.466984987 CEST	50089	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.488691092 CEST	53	50089	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:18.489552021 CEST	50090	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.510843992 CEST	53	50090	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:18.513859987 CEST	50091	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:18.533323050 CEST	53	50091	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:19.081789970 CEST	52188	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:19.943706036 CEST	53	50086	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:20.074146986 CEST	52188	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.087065935 CEST	52188	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.117666960 CEST	53	52188	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.124485970 CEST	52189	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.145231009 CEST	53	52189	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.145886898 CEST	52190	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.167120934 CEST	53	52190	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.167674065 CEST	52191	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.187253952 CEST	53	52191	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.187861919 CEST	52192	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.209659100 CEST	53	52192	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.210468054 CEST	52193	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:21.230139017 CEST	53	52193	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:21.243673086 CEST	53	52188	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:22.047276020 CEST	54585	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:22.152108908 CEST	53	52188	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.055248976 CEST	54585	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:23.089651108 CEST	53	54585	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.098977089 CEST	54586	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:23.118304968 CEST	53	54586	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.124735117 CEST	54587	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:23.144418001 CEST	53	54587	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.146754980 CEST	54588	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:23.165380955 CEST	53	54588	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.168675900 CEST	54589	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:23.188942909 CEST	53	54589	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:23.192418098 CEST	54590	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:23.213639021 CEST	53	54590	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:25.939043045 CEST	52100	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.282510996 CEST	52100	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.609777927 CEST	53	52100	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.648454905 CEST	52101	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.668226004 CEST	53	52101	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.668952942 CEST	52102	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.688935995 CEST	53	52102	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.689357042 CEST	52103	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.709584951 CEST	53	52103	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.710043907 CEST	52104	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.729931116 CEST	53	52104	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.730338097 CEST	52105	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:27.748384953 CEST	53	52105	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:27.819541931 CEST	53	52100	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.075316906 CEST	53	54585	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.205267906 CEST	60908	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.274440050 CEST	53	60908	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.293237925 CEST	60909	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.310379982 CEST	53	60909	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.310951948 CEST	60910	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.330352068 CEST	53	60910	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.331020117 CEST	60911	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.348592997 CEST	53	60911	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.349097967 CEST	60912	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.368571997 CEST	53	60912	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.369055986 CEST	60913	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.388623953 CEST	53	60913	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.783333063 CEST	58623	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.819798946 CEST	53	58623	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.828504086 CEST	58624	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.849626064 CEST	53	58624	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.850497007 CEST	58625	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.871601105 CEST	53	58625	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.872267008 CEST	58626	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.891577005 CEST	53	58626	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.892334938 CEST	58627	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.915539980 CEST	53	58627	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:28.916264057 CEST	58628	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:28.937171936 CEST	53	58628	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.413041115 CEST	65493	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.466361046 CEST	53	65493	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.475575924 CEST	65494	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.496511936 CEST	53	65494	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.499361038 CEST	65495	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.516742945 CEST	53	65495	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.520509958 CEST	65496	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.542265892 CEST	53	65496	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.542702913 CEST	65497	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.564232111 CEST	53	65497	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.567003012 CEST	65498	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:29.586312056 CEST	53	65498	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:29.950607061 CEST	57482	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:30.487483025 CEST	53	57482	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:30.496217012 CEST	57483	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:30.516846895 CEST	53	57483	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:30.517520905 CEST	57484	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:30.536672115 CEST	53	57484	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:30.537076950 CEST	57485	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:30.559077978 CEST	53	57485	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:30.561309099 CEST	57486	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:30.580718040 CEST	53	57486	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:30.582628965 CEST	57487	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:30.603596926 CEST	53	57487	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:31.118854046 CEST	52096	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.118266106 CEST	52096	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.197714090 CEST	53	52096	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.206779957 CEST	52097	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.226025105 CEST	53	52097	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.229187012 CEST	52098	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.247734070 CEST	53	52098	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.248418093 CEST	52099	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.259257078 CEST	53	52096	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.267229080 CEST	53	52099	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.267997980 CEST	52100	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.288376093 CEST	53	52100	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.288887024 CEST	52101	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.309899092 CEST	53	52101	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.741540909 CEST	62057	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.809542894 CEST	53	62057	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.826855898 CEST	62058	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.847543955 CEST	53	62058	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.850991011 CEST	62059	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.872570038 CEST	53	62059	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.873172045 CEST	62060	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.894160032 CEST	53	62060	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.897217035 CEST	62061	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.918351889 CEST	53	62061	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:32.918939114 CEST	62062	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:32.940099001 CEST	53	62062	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.285465002 CEST	60294	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.313813925 CEST	53	60294	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.323398113 CEST	60295	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.340472937 CEST	53	60295	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.345251083 CEST	60296	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.362754107 CEST	53	60296	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.363249063 CEST	60297	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.382714987 CEST	53	60297	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.383268118 CEST	60298	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.400686026 CEST	53	60298	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.401259899 CEST	60299	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.420860052 CEST	53	60299	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.877412081 CEST	63728	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.947339058 CEST	53	63728	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.957496881 CEST	63729	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.976629972 CEST	53	63729	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.977550030 CEST	63730	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:33.997020960 CEST	53	63730	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:33.997565985 CEST	63731	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.017164946 CEST	53	63731	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.017664909 CEST	63732	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.037424088 CEST	53	63732	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:34.037883997 CEST	63733	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.055460930 CEST	53	63733	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.510437965 CEST	50077	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.579391003 CEST	53	50077	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.589109898 CEST	50078	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.606172085 CEST	53	50078	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.606965065 CEST	50079	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.626548052 CEST	53	50079	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.627090931 CEST	50080	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.645029068 CEST	53	50080	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.650980949 CEST	50081	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.670808077 CEST	53	50081	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:34.671276093 CEST	50082	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:34.691076040 CEST	53	50082	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.101633072 CEST	49959	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.637387991 CEST	53	49959	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.647269011 CEST	49960	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.667938948 CEST	53	49960	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.669538021 CEST	49961	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.688895941 CEST	53	49961	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.689392090 CEST	49962	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.711240053 CEST	53	49962	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.711879969 CEST	49963	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.732723951 CEST	53	49963	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:35.733293056 CEST	49964	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:35.755530119 CEST	53	49964	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.301939011 CEST	55609	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.375839949 CEST	53	55609	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.383898020 CEST	55610	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.402359009 CEST	53	55610	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.403141022 CEST	55611	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.424987078 CEST	53	55611	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.425992012 CEST	55612	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.445525885 CEST	53	55612	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.446288109 CEST	55613	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.467850924 CEST	53	55613	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.468326092 CEST	55614	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:36.489662886 CEST	53	55614	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:36.851623058 CEST	58872	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:37.856156111 CEST	58872	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:37.983706951 CEST	53	58872	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:37.990816116 CEST	58873	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.011287928 CEST	53	58873	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:38.011985064 CEST	58874	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.032377958 CEST	53	58874	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:38.032850981 CEST	58875	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.052937031 CEST	53	58875	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:38.053462982 CEST	58876	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.072388887 CEST	53	58876	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:38.072921038 CEST	58877	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.090707064 CEST	53	58877	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:38.425242901 CEST	52892	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:38.996529102 CEST	53	52892	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.052143097 CEST	52893	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.071681023 CEST	53	52893	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.072653055 CEST	52894	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.091151953 CEST	53	52894	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.091614008 CEST	52895	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.110236883 CEST	53	52895	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:39.114274979 CEST	52896	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.132061005 CEST	53	52896	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.132618904 CEST	52897	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.151518106 CEST	53	52897	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.482498884 CEST	53	58872	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.587059021 CEST	65330	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.615535975 CEST	53	65330	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.627641916 CEST	65331	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.646815062 CEST	53	65331	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.649023056 CEST	65332	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.666840076 CEST	53	65332	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.670909882 CEST	65333	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.691112995 CEST	53	65333	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.691657066 CEST	65334	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.711394072 CEST	53	65334	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:39.713005066 CEST	65335	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:39.733046055 CEST	53	65335	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.106767893 CEST	52973	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.144674063 CEST	53	52973	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.155935049 CEST	52974	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.176877022 CEST	53	52974	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.177431107 CEST	52975	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.198590040 CEST	53	52975	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.199012995 CEST	52976	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.217324018 CEST	53	52976	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.217833042 CEST	52977	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.235502958 CEST	53	52977	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.236027002 CEST	52978	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:40.253726959 CEST	53	52978	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:40.812171936 CEST	50005	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:41.821934938 CEST	50005	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.581233025 CEST	53	50005	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:42.678219080 CEST	62935	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.695910931 CEST	53	62935	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:42.697375059 CEST	62936	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.717495918 CEST	53	62936	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:42.718178034 CEST	62937	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.736381054 CEST	53	62937	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:42.736982107 CEST	62938	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.756829023 CEST	53	62938	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:42.757239103 CEST	62939	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:42.774645090 CEST	53	62939	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.304724932 CEST	59862	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.834578991 CEST	53	59862	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.843754053 CEST	58442	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.862184048 CEST	53	58442	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.862726927 CEST	58443	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.881683111 CEST	53	58443	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.882038116 CEST	58444	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.903206110 CEST	53	58444	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.903620958 CEST	58445	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.924917936 CEST	53	58445	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:43.925486088 CEST	58446	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:43.945391893 CEST	53	58446	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.445437908 CEST	55726	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:44.472067118 CEST	53	55726	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.482812881 CEST	55727	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:44.500081062 CEST	53	55727	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.508574963 CEST	55728	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:44.526537895 CEST	53	55728	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.527149916 CEST	55729	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:44.546730042 CEST	53	55729	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.550257921 CEST	55730	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:44.567960024 CEST	53	55730	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.568357944 CEST	55731	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:44.588005066 CEST	53	55731	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:44.976836920 CEST	61928	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:45.831124067 CEST	53	50005	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:45.962614059 CEST	61928	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:46.981189013 CEST	61928	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.038166046 CEST	53	61928	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.047594070 CEST	53428	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.067724943 CEST	53	53428	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.068211079 CEST	53429	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.089193106 CEST	53	53429	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.092444897 CEST	53430	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.111303091 CEST	53	53430	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.111712933 CEST	53431	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.130348921 CEST	53	53431	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.130970001 CEST	53432	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:47.152026892 CEST	53	53432	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.509731054 CEST	53	61928	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:47.627257109 CEST	60179	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.198370934 CEST	53	60179	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.218760967 CEST	60180	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.237399101 CEST	53	60180	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.237956047 CEST	60181	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.258917093 CEST	53	60181	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.263649940 CEST	60182	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.283209085 CEST	53	60182	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.283958912 CEST	60183	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.304694891 CEST	53	60183	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.305239916 CEST	60184	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:48.325745106 CEST	53	60184	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:48.691673040 CEST	57377	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:49.241806030 CEST	53	61928	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:49.697010994 CEST	57377	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.281771898 CEST	53	57377	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.300674915 CEST	57378	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.307605028 CEST	53	57377	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.317943096 CEST	53	57378	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.318563938 CEST	57379	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.338493109 CEST	53	57379	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.340625048 CEST	57380	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.358608961 CEST	53	57380	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.368405104 CEST	57381	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.388493061 CEST	53	57381	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.398087025 CEST	57382	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:50.416033030 CEST	53	57382	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:50.775196075 CEST	63938	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:51.779573917 CEST	63938	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.316684961 CEST	53	63938	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:52.325777054 CEST	63939	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.345062017 CEST	53	63939	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:52.350223064 CEST	63940	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.370079041 CEST	53	63940	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:52.370595932 CEST	63941	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.388272047 CEST	53	63941	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:03:52.388947964 CEST	63942	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.412725925 CEST	53	63942	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:52.415647030 CEST	63943	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:52.435429096 CEST	53	63943	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:52.890666008 CEST	50444	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:53.896193027 CEST	50444	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:53.933697939 CEST	53	50444	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:53.943182945 CEST	50445	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:53.962321997 CEST	53	50445	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:53.963216066 CEST	50446	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:53.984399080 CEST	53	50446	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:53.986779928 CEST	50447	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:54.007458925 CEST	53	50447	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:54.015145063 CEST	50448	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:54.026586056 CEST	53	50444	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:54.035367012 CEST	53	50448	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:54.035959959 CEST	50449	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:54.055593014 CEST	53	50449	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:54.669785023 CEST	59805	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.239881992 CEST	53	59805	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.253882885 CEST	59806	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.274434090 CEST	53	59806	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.275052071 CEST	59807	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.294156075 CEST	53	59807	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.294608116 CEST	51724	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.313684940 CEST	53	51724	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.314555883 CEST	51725	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.336025953 CEST	53	51725	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.342623949 CEST	51726	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.364104986 CEST	53	51726	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:55.731010914 CEST	64494	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:55.794974089 CEST	53	63938	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.268456936 CEST	53	64494	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.282052040 CEST	64495	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:56.301691055 CEST	53	64495	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.305340052 CEST	64496	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:56.325932980 CEST	53	64496	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.326354980 CEST	64497	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:56.346476078 CEST	53	64497	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.346913099 CEST	64498	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:56.365498066 CEST	53	64498	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.365973949 CEST	64499	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:56.386655092 CEST	53	64499	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:56.795289993 CEST	64310	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:57.797553062 CEST	64310	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:58.797333002 CEST	64310	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:58.825668097 CEST	53	64310	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:58.836684942 CEST	64311	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:58.855791092 CEST	53	64311	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:58.856410027 CEST	64312	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:58.874407053 CEST	53	64312	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:58.875072956 CEST	64313	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:58.893013000 CEST	53	64313	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:59.395837069 CEST	64314	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:59.415303946 CEST	53	64314	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:59.415810108 CEST	64315	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:03:59.437519073 CEST	53	64315	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:59.477504015 CEST	53	64310	8.8.8.8	192.168.2.5
Sep 1, 2022 00:03:59.624346018 CEST	49261	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:04:00.200125933 CEST	53	49261	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.706511974 CEST	53	64310	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.905369997 CEST	49262	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:00.922754049 CEST	53	49262	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.923809052 CEST	49263	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:00.943747044 CEST	53	49263	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.944093943 CEST	49264	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:00.962049007 CEST	53	49264	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.962398052 CEST	49265	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:00.982321024 CEST	53	49265	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:00.982711077 CEST	49266	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:01.002304077 CEST	53	49266	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:01.164730072 CEST	54367	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:02.157042980 CEST	54367	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.156949043 CEST	54367	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.734221935 CEST	53	54367	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:03.742338896 CEST	54368	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.761651039 CEST	53	54368	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:03.762306929 CEST	54369	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.782330036 CEST	53	54369	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:03.782854080 CEST	54370	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.802499056 CEST	53	54370	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:03.802921057 CEST	54371	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.822778940 CEST	53	54371	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:03.823256969 CEST	54372	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:03.842823982 CEST	53	54372	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.020246983 CEST	59583	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.048010111 CEST	53	59583	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.054968119 CEST	59584	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.074004889 CEST	53	59584	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.074500084 CEST	59585	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.094161987 CEST	53	59585	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.094595909 CEST	59586	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.114377975 CEST	53	59586	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.114751101 CEST	59587	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.134500980 CEST	53	59587	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.134905100 CEST	59588	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.154583931 CEST	53	59588	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.195255041 CEST	53	54367	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.339045048 CEST	50562	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.913227081 CEST	53	50562	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.919328928 CEST	50563	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.936587095 CEST	53	50563	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.937268972 CEST	50564	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.955105066 CEST	53	50564	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.955935001 CEST	50565	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.975845098 CEST	53	50565	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.976212025 CEST	50566	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:04.996162891 CEST	53	50566	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:04.998120070 CEST	50567	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.017935991 CEST	53	50567	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.204899073 CEST	56114	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.764825106 CEST	53	54367	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.773658037 CEST	53	56114	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.781946898 CEST	56115	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.801095963 CEST	53	56115	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.801650047 CEST	56116	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.840457916 CEST	53	56116	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.841041088 CEST	56117	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:04:05.861089945 CEST	53	56117	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.861618042 CEST	56118	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.881166935 CEST	53	56118	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:05.881609917 CEST	56119	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:05.901103973 CEST	53	56119	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.088465929 CEST	61016	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.630609989 CEST	53	61016	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.636603117 CEST	61017	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.656243086 CEST	53	61017	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.657228947 CEST	61018	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.677496910 CEST	53	61018	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.677903891 CEST	61019	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.698992968 CEST	53	61019	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.699435949 CEST	61020	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.718585014 CEST	53	61020	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.718974113 CEST	61021	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:06.737366915 CEST	53	61021	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:06.913439989 CEST	59296	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.451251030 CEST	53	59296	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.458348036 CEST	59297	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.475867033 CEST	53	59297	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.476417065 CEST	59298	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.495662928 CEST	53	59298	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.496000051 CEST	59299	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.513513088 CEST	53	59299	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.513787985 CEST	59300	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.531666040 CEST	53	59300	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.531975985 CEST	59301	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:07.552181005 CEST	53	59301	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:07.723758936 CEST	55592	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:08.720289946 CEST	55592	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.720633984 CEST	55592	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.852585077 CEST	53	55592	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.860241890 CEST	55593	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.861260891 CEST	53	55592	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.879578114 CEST	53	55593	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.880110979 CEST	55594	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.897767067 CEST	53	55594	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.898241043 CEST	55595	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.917709112 CEST	53	55595	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.918087959 CEST	55596	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.935751915 CEST	53	55596	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:09.936181068 CEST	55597	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:09.956202984 CEST	53	55597	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.134829044 CEST	65115	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.284883022 CEST	53	55592	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.678015947 CEST	53	65115	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.686275959 CEST	65116	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.703870058 CEST	53	65116	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.704503059 CEST	65117	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.724714041 CEST	53	65117	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.725130081 CEST	65118	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.742995024 CEST	53	65118	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.743391037 CEST	65119	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.762958050 CEST	53	65119	8.8.8.8	192.168.2.5
Sep 1, 2022 00:04:10.763288975 CEST	65120	53	192.168.2.5	8.8.8.8
Sep 1, 2022 00:04:10.784327984 CEST	53	65120	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Sep 1, 2022 00:02:03.633960009 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:15.249326944 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:28.241391897 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:38.546083927 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:46.627891064 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:55.305211067 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:56.963974953 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:02:58.055891037 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:03.269479036 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:04.564671040 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:09.094980001 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:19.943866014 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:21.243824959 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:22.152236938 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:27.819679022 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:32.259469986 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:39.482671976 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:45.831290960 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:47.510422945 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:49.242109060 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:50.310148954 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:54.026720047 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:55.795069933 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:03:59.477780104 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:04:00.706722975 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:04:04.195362091 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:04:05.764991999 CEST	192.168.2.5	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:04:09.861358881 CEST	192.168.2.5	8.8.8.8	d032	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:01:59.911590099 CEST	192.168.2.5	8.8.8.8	0xb66e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.239926100 CEST	192.168.2.5	8.8.8.8	0xe0a0	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.352194071 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:01.372827053 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:02:01.394041061 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:01.412620068 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.433121920 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:02.555277109 CEST	192.168.2.5	8.8.8.8	0xdfb2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.563941002 CEST	192.168.2.5	8.8.8.8	0xdfb2	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.633877039 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:03.654443979 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.672878981 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:03.693125963 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.713490009 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:04.721681118 CEST	192.168.2.5	8.8.8.8	0x3cd5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.856112003 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:04.877624035 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.899187088 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:04.922756910 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.942714930 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:06.005309105 CEST	192.168.2.5	8.8.8.8	0x27fd	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.059837103 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:06.080173016 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.112308979 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:06.132219076 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.151880026 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:11.007499933 CEST	192.168.2.5	8.8.8.8	0x5f2a	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.022016048 CEST	192.168.2.5	8.8.8.8	0x5f2a	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.591213942 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:12.612833977 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.647016048 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:12.666415930 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.684530020 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:13.709269047 CEST	192.168.2.5	8.8.8.8	0xe32f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.739041090 CEST	192.168.2.5	8.8.8.8	0xe32f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.792093039 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:14.812380075 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.833183050 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:14.854022980 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:02:14.874396086 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:15.933274984 CEST	192.168.2.5	8.8.8.8	0x2c2f	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.490912914 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:16.533431053 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.558773041 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:16.584621906 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.604526043 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:18.327372074 CEST	192.168.2.5	8.8.8.8	0xb4ae	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:18.912621975 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:18.931529045 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:18.950858116 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:18.976716042 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:19.007297993 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:20.212028027 CEST	192.168.2.5	8.8.8.8	0x65f7	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:20.343282938 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:20.361607075 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:20.380295992 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:20.399331093 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:20.420031071 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:21.510334015 CEST	192.168.2.5	8.8.8.8	0x17a5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.570235014 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:21.592544079 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.613022089 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:21.631695986 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.652316093 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:22.988415956 CEST	192.168.2.5	8.8.8.8	0xf0f	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.090640068 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:23.120246887 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.142880917 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:23.164989948 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.186316967 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:24.293374062 CEST	192.168.2.5	8.8.8.8	0x1940	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.285326958 CEST	192.168.2.5	8.8.8.8	0x1940	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.416001081 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:25.448208094 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:02:25.469721079 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:25.489629030 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.509063959 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:30.590687990 CEST	192.168.2.5	8.8.8.8	0x1450	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.191478968 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:31.210675955 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.231911898 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:31.250178099 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.279995918 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:32.336535931 CEST	192.168.2.5	8.8.8.8	0x6c66	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:32.885988951 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:32.912023067 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:32.934242964 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:32.956295967 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:32.980618954 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:34.142494917 CEST	192.168.2.5	8.8.8.8	0xda28	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:34.743534088 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:34.772206068 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:34.794476032 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:34.816977978 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:34.840092897 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:35.871191025 CEST	192.168.2.5	8.8.8.8	0xfb8d	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:36.910881996 CEST	192.168.2.5	8.8.8.8	0xfb8d	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:37.964308977 CEST	192.168.2.5	8.8.8.8	0xfb8d	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.469635963 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:38.490396976 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.510792971 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:38.530361891 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.549772978 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:02:39.543435097 CEST	192.168.2.5	8.8.8.8	0x374e	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.608720064 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:39.626605988 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.645914078 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:39.666429996 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.698321104 CEST	192.168.2.5	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
Sep 1, 2022 00:02:41.365394115 CEST	192.168.2.5	8.8.8.8	0xbde8	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:41.974438906 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:41.995821953 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:42.016020060 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:42.036797047 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:42.055155993 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:43.388982058 CEST	192.168.2.5	8.8.8.8	0x6fbd	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:44.405422926 CEST	192.168.2.5	8.8.8.8	0x6fbd	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:45.428538084 CEST	192.168.2.5	8.8.8.8	0x6fbd	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.391263008 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:46.409357071 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.486526966 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:46.511400938 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.531265020 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:50.357605934 CEST	192.168.2.5	8.8.8.8	0xafd1	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.462135077 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:50.481997967 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.502751112 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:50.523251057 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.545957088 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:51.939711094 CEST	192.168.2.5	8.8.8.8	0xbfd8	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:52.973716974 CEST	192.168.2.5	8.8.8.8	0xbfd8	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.031869888 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:53.057440996 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.081721067 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:53.105767965 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.129672050 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:02:54.129081964 CEST	192.168.2.5	8.8.8.8	0xbfee	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.115514040 CEST	192.168.2.5	8.8.8.8	0xbfee	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.169272900 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:55.191369057 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.212193966 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:55.231072903 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.250291109 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:02:56.391621113 CEST	192.168.2.5	8.8.8.8	0xa3e5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:02:57.439699888 CEST	192.168.2.5	8.8.8.8	0xa3e5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.030960083 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:58.051615953 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.072381973 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:58.094800949 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.117259979 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:02:59.546935081 CEST	192.168.2.5	8.8.8.8	0x8bd5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:00.539176941 CEST	192.168.2.5	8.8.8.8	0x8bd5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:01.593920946 CEST	192.168.2.5	8.8.8.8	0x8bd5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.707921982 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:02.730690956 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.751282930 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:02.774286032 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.797461033 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:04.074176073 CEST	192.168.2.5	8.8.8.8	0xdae1	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.102104902 CEST	192.168.2.5	8.8.8.8	0xdae1	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.167689085 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:05.189017057 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.233382940 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:05.323153019 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.512259960 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:10.430033922 CEST	192.168.2.5	8.8.8.8	0x82a2	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:10.994596958 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:11.014978886 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:11.038347960 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:11.058419943 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:11.078563929 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:12.533488035 CEST	192.168.2.5	8.8.8.8	0x4482	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.129920006 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:13.151999950 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.174170017 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:13.202744007 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.225919962 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:14.898765087 CEST	192.168.2.5	8.8.8.8	0xe274	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.455348969 CEST	192.168.2.5	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
Sep 1, 2022 00:03:15.476530075 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.496748924 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:15.516932964 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.537245989 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:17.268368959 CEST	192.168.2.5	8.8.8.8	0x55e4	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.259387016 CEST	192.168.2.5	8.8.8.8	0x55e4	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.425247908 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:18.446546078 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.466984987 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:18.489552021 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.513859987 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:19.081789970 CEST	192.168.2.5	8.8.8.8	0x8b47	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:20.074146986 CEST	192.168.2.5	8.8.8.8	0x8b47	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.087065935 CEST	192.168.2.5	8.8.8.8	0x8b47	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.124485970 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:21.145886898 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.167674065 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:21.187861919 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.210468054 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:22.047276020 CEST	192.168.2.5	8.8.8.8	0x560f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.055248976 CEST	192.168.2.5	8.8.8.8	0x560f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.098977089 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:23.124735117 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.146754980 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:23.168675900 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.192418098 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:25.939043045 CEST	192.168.2.5	8.8.8.8	0x82c5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.282510996 CEST	192.168.2.5	8.8.8.8	0x82c5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.648454905 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:27.668952942 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.689357042 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:27.710043907 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.730338097 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:28.205267906 CEST	192.168.2.5	8.8.8.8	0xf281	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.293237925 CEST	192.168.2.5	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
Sep 1, 2022 00:03:28.310951948 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.331020117 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:28.349097967 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.369055986 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:28.783333063 CEST	192.168.2.5	8.8.8.8	0xdac3	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.828504086 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:28.850497007 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.872267008 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:28.892334938 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.916264057 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:29.413041115 CEST	192.168.2.5	8.8.8.8	0x163a	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.475575924 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:29.499361038 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.520509958 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:29.542702913 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.567003012 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:29.950607061 CEST	192.168.2.5	8.8.8.8	0xadc5	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.496217012 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:30.517520905 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.537076950 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:30.561309099 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.582628965 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:31.118854046 CEST	192.168.2.5	8.8.8.8	0xe338	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.118266106 CEST	192.168.2.5	8.8.8.8	0xe338	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.206779957 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:32.229187012 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.248418093 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:32.267997980 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.288887024 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:32.741540909 CEST	192.168.2.5	8.8.8.8	0xa108	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.826855898 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:32.850991011 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.873172045 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:32.897217035 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.918939114 CEST	192.168.2.5	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
Sep 1, 2022 00:03:33.285465002 CEST	192.168.2.5	8.8.8.8	0xe874	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.323398113 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:33.345251083 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.363249063 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:33.383268118 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.401259899 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:33.877412081 CEST	192.168.2.5	8.8.8.8	0xca6e	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.957496881 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:33.977550030 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.997565985 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:34.017664909 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.037883997 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:34.510437965 CEST	192.168.2.5	8.8.8.8	0x3d5a	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.589109898 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:34.606965065 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.627090931 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:34.650980949 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.671276093 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:35.101633072 CEST	192.168.2.5	8.8.8.8	0xa2a9	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.647269011 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:35.669538021 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.689392090 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:35.711879969 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.733293056 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:36.301939011 CEST	192.168.2.5	8.8.8.8	0xd67b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.383898020 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:36.403141022 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.425992012 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:36.446288109 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.468326092 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:36.851623058 CEST	192.168.2.5	8.8.8.8	0xba9f	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:37.856156111 CEST	192.168.2.5	8.8.8.8	0xba9f	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:37.990816116 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:38.011985064 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:38.032850981 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:03:38.053462982 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:38.072921038 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:38.425242901 CEST	192.168.2.5	8.8.8.8	0x5fe7	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.052143097 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:39.072653055 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.091614008 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:39.114274979 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.132618904 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:39.587059021 CEST	192.168.2.5	8.8.8.8	0x82c2	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.627641916 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:39.649023056 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.670909882 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:39.691657066 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.713005066 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:40.106767893 CEST	192.168.2.5	8.8.8.8	0x2edf	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.155935049 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:40.177431107 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.199012995 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:40.217833042 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.236027002 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:40.812171936 CEST	192.168.2.5	8.8.8.8	0x8cc	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:41.821934938 CEST	192.168.2.5	8.8.8.8	0x8cc	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.678219080 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:42.697375059 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.718178034 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:42.736982107 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.757239103 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:43.304724932 CEST	192.168.2.5	8.8.8.8	0x2679	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.843754053 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:43.862726927 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.882038116 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:43.903620958 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.925486088 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:44.445437908 CEST	192.168.2.5	8.8.8.8	0x4cff	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.482812881 CEST	192.168.2.5	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
Sep 1, 2022 00:03:44.508574963 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.527149916 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:44.550257921 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.568357944 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:44.976836920 CEST	192.168.2.5	8.8.8.8	0x6ec8	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:45.962614059 CEST	192.168.2.5	8.8.8.8	0x6ec8	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:46.981189013 CEST	192.168.2.5	8.8.8.8	0x6ec8	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.047594070 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:47.068211079 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.092444897 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:47.111712933 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.130970001 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:47.627257109 CEST	192.168.2.5	8.8.8.8	0x8128	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.218760967 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:48.237956047 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.263649940 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:48.283958912 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.305239916 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:03:48.691673040 CEST	192.168.2.5	8.8.8.8	0xab90	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:49.697010994 CEST	192.168.2.5	8.8.8.8	0xab90	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.300674915 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:50.318563938 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.340625048 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:50.368405104 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.398087025 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:50.775196075 CEST	192.168.2.5	8.8.8.8	0x7c25	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:51.779573917 CEST	192.168.2.5	8.8.8.8	0x7c25	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.325777054 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:52.350223064 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.370595932 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:52.388947964 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.415647030 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:52.890666008 CEST	192.168.2.5	8.8.8.8	0x5962	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:53.896193027 CEST	192.168.2.5	8.8.8.8	0x5962	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:53.943182945 CEST	192.168.2.5	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
Sep 1, 2022 00:03:53.963216066 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:53.986779928 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:54.015145063 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:54.035959959 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:54.669785023 CEST	192.168.2.5	8.8.8.8	0xc5e7	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.253882885 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:55.275052071 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.294608116 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:55.314555883 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.342623949 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:03:55.731010914 CEST	192.168.2.5	8.8.8.8	0x2f3	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.282052040 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:56.305340052 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.326354980 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:56.346913099 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.365973949 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:03:56.795289993 CEST	192.168.2.5	8.8.8.8	0xe61c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:57.797553062 CEST	192.168.2.5	8.8.8.8	0xe61c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:58.797333002 CEST	192.168.2.5	8.8.8.8	0xe61c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:58.836684942 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:58.856410027 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:58.875072956 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:59.395837069 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:59.415810108 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:03:59.624346018 CEST	192.168.2.5	8.8.8.8	0xdb8b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.905369997 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:00.923809052 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.944093943 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:00.962398052 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.982711077 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:01.164730072 CEST	192.168.2.5	8.8.8.8	0xc850	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:02.157042980 CEST	192.168.2.5	8.8.8.8	0xc850	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.156949043 CEST	192.168.2.5	8.8.8.8	0xc850	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.742338896 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:03.762306929 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:04:03.782854080 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:03.802921057 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.823256969 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:04.020246983 CEST	192.168.2.5	8.8.8.8	0x9e81	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.054968119 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:04.074500084 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.094595909 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:04:04.114751101 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.134905100 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:04:04.339045048 CEST	192.168.2.5	8.8.8.8	0xed4b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.919328928 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:04.937268972 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.955935001 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:04.976212025 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.998120070 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:05.204899073 CEST	192.168.2.5	8.8.8.8	0x647b	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.781946898 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:05.801650047 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.841041088 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:05.861618042 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.881609917 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:06.088465929 CEST	192.168.2.5	8.8.8.8	0xedf0	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.636603117 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:06.657228947 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.677903891 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:04:06.699435949 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.718974113 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Sep 1, 2022 00:04:06.913439989 CEST	192.168.2.5	8.8.8.8	0x3852	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.458348036 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:07.476417065 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.496000051 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:07.513787985 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	emsisoft.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.531975985 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	emsisoft.bit	28	IN (0x0001)
Sep 1, 2022 00:04:07.723758936 CEST	192.168.2.5	8.8.8.8	0x26ba	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:08.720289946 CEST	192.168.2.5	8.8.8.8	0x26ba	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:04:09.720633984 CEST	192.168.2.5	8.8.8.8	0x26ba	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.860241890 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:09.880110979 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.898241043 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:09.918087959 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.936181068 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:04:10.134829044 CEST	192.168.2.5	8.8.8.8	0x31f5	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.686275959 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:10.704503059 CEST	192.168.2.5	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.725130081 CEST	192.168.2.5	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:04:10.743391037 CEST	192.168.2.5	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.763288975 CEST	192.168.2.5	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:02:01.334580898 CEST	8.8.8.8	192.168.2.5	0xe0a0	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.372085094 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:01.393094063 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.412072897 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:01.432477951 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:01.453190088 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:03.608334064 CEST	8.8.8.8	192.168.2.5	0xdfb2	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.633827925 CEST	8.8.8.8	192.168.2.5	0xdfb2	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.653230906 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:03.672249079 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.692581892 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:03.712928057 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:03.733714104 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:04.834590912 CEST	8.8.8.8	192.168.2.5	0x3cd5	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.876791954 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:04.898612976 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.920192003 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:04.941993952 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:04.961915970 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:06.042258024 CEST	8.8.8.8	192.168.2.5	0x27fd	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.078336954 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:02:06.101386070 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.131583929 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:06.151202917 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:06.173470020 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:12.567970991 CEST	8.8.8.8	192.168.2.5	0x5f2a	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.610974073 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:12.632694960 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.665808916 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:12.684042931 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:12.704040051 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:14.775738955 CEST	8.8.8.8	192.168.2.5	0xe32f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.811539888 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:14.832356930 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.853168011 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:14.873765945 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:14.894181013 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:15.249150038 CEST	8.8.8.8	192.168.2.5	0xe32f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.027390957 CEST	8.8.8.8	192.168.2.5	0x5f2a	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.471765041 CEST	8.8.8.8	192.168.2.5	0x2c2f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.512093067 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:16.554326057 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.580204964 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:16.603900909 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:16.625678062 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:18.866029978 CEST	8.8.8.8	192.168.2.5	0xb4ae	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:18.930771112 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:18.950180054 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:18.971628904 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:18.997745991 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:19.028003931 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:20.281924009 CEST	8.8.8.8	192.168.2.5	0x65f7	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:20.360511065 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:20.379569054 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:20.398627043 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:20.419385910 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:02:20.438457966 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:21.547008991 CEST	8.8.8.8	192.168.2.5	0x17a5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.589804888 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:21.612307072 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.631066084 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:21.651690006 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:21.670263052 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:23.073178053 CEST	8.8.8.8	192.168.2.5	0xf0f	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.108946085 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:23.139523029 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.164510012 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:23.185849905 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:23.208182096 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:25.395417929 CEST	8.8.8.8	192.168.2.5	0x1940	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.436459064 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:25.469156981 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.489044905 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:25.508452892 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:25.530004978 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:28.241271019 CEST	8.8.8.8	192.168.2.5	0x1940	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.166659117 CEST	8.8.8.8	192.168.2.5	0x1450	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.209889889 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:31.231199026 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.249490976 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:31.269680977 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:31.300205946 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:32.866913080 CEST	8.8.8.8	192.168.2.5	0x6c66	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:32.905796051 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:32.933625937 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:32.955260038 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:32.979974985 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:33.001955032 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:34.717264891 CEST	8.8.8.8	192.168.2.5	0xda28	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:34.764400959 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:34.793865919 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:02:34.816371918 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:34.839456081 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:34.859596014 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:38.451112986 CEST	8.8.8.8	192.168.2.5	0xfb8d	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.489614010 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:38.510234118 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.529823065 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:38.544522047 CEST	8.8.8.8	192.168.2.5	0xfb8d	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.549093008 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:38.569746971 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:39.005251884 CEST	8.8.8.8	192.168.2.5	0xfb8d	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.580847025 CEST	8.8.8.8	192.168.2.5	0x374e	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.625894070 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:39.645344973 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.665539026 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:39.686157942 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:39.718056917 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:41.948688984 CEST	8.8.8.8	192.168.2.5	0xbde8	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:41.993784904 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:42.015419006 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:42.035979033 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:42.054507971 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:42.075145006 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:46.031758070 CEST	8.8.8.8	192.168.2.5	0x6fbd	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.408472061 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:46.428978920 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.506362915 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:46.529474020 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:46.550900936 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:46.627775908 CEST	8.8.8.8	192.168.2.5	0x6fbd	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:47.232079029 CEST	8.8.8.8	192.168.2.5	0x6fbd	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.431725979 CEST	8.8.8.8	192.168.2.5	0xafd1	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.481153965 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:50.502183914 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.522468090 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:02:50.545125961 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:50.565229893 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:53.012386084 CEST	8.8.8.8	192.168.2.5	0xbfd8	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.051094055 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:53.081031084 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.105006933 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:53.129003048 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:53.152440071 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:55.143107891 CEST	8.8.8.8	192.168.2.5	0xbfee	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.190500021 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:55.211363077 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.230350971 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:55.249286890 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:55.269426107 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:55.303771973 CEST	8.8.8.8	192.168.2.5	0xbfee	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:56.963818073 CEST	8.8.8.8	192.168.2.5	0xbfd8	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.006582975 CEST	8.8.8.8	192.168.2.5	0xa3e5	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.050683022 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:02:58.055273056 CEST	8.8.8.8	192.168.2.5	0xa3e5	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.071692944 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.092132092 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:02:58.112858057 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:02:58.137913942 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:02.673258066 CEST	8.8.8.8	192.168.2.5	0x8bd5	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.728626013 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:02.749336004 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.772249937 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:02.794682980 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:02.818588018 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:03.269387960 CEST	8.8.8.8	192.168.2.5	0x8bd5	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:04.564574957 CEST	8.8.8.8	192.168.2.5	0x8bd5	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.140230894 CEST	8.8.8.8	192.168.2.5	0xdae1	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.186117887 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:05.209920883 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.252963066 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:03:05.340817928 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:05.533775091 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:09.094862938 CEST	8.8.8.8	192.168.2.5	0xdae1	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:10.970557928 CEST	8.8.8.8	192.168.2.5	0x82a2	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:11.013236046 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:11.036653042 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:11.057737112 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:11.077819109 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:11.099826097 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:13.112035036 CEST	8.8.8.8	192.168.2.5	0x4482	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.151115894 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:13.173320055 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.196038961 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:13.224518061 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:13.246552944 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:15.436304092 CEST	8.8.8.8	192.168.2.5	0xe274	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.474445105 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:15.496115923 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.516382933 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:15.536484003 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:15.554661036 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:18.395138979 CEST	8.8.8.8	192.168.2.5	0x55e4	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.445703030 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:18.466348886 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.488691092 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:18.510843992 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:18.533323050 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:19.943706036 CEST	8.8.8.8	192.168.2.5	0x55e4	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.117666960 CEST	8.8.8.8	192.168.2.5	0x8b47	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.145231009 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:21.167120934 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.187253952 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:21.209659100 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:21.230139017 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:21.243673086 CEST	8.8.8.8	192.168.2.5	0x8b47	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
Sep 1, 2022 00:03:22.152108908 CEST	8.8.8.8	192.168.2.5	0x8b47	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.089651108 CEST	8.8.8.8	192.168.2.5	0x560f	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.118304968 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:23.144418001 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.165380955 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:23.188942909 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:23.213639021 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:27.609777927 CEST	8.8.8.8	192.168.2.5	0x82c5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.668226004 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:27.688935995 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.709584951 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:27.729931116 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:27.748384953 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:27.819541931 CEST	8.8.8.8	192.168.2.5	0x82c5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.075316906 CEST	8.8.8.8	192.168.2.5	0x560f	Server failure (2)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.274440050 CEST	8.8.8.8	192.168.2.5	0xf281	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.310379982 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:28.330352068 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.348592997 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:28.368571997 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.388623953 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:28.819798946 CEST	8.8.8.8	192.168.2.5	0xdac3	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.849626064 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:28.871601105 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.891577005 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:28.915539980 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:28.937171936 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:29.466361046 CEST	8.8.8.8	192.168.2.5	0x163a	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.496511936 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:29.516742945 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.542265892 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:29.564232111 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:29.586312056 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:30.487483025 CEST	8.8.8.8	192.168.2.5	0xadc5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.516846895 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:03:30.536672115 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.559077978 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:30.580718040 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:30.603596926 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:32.197714090 CEST	8.8.8.8	192.168.2.5	0xe338	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.226025105 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:32.247734070 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.259257078 CEST	8.8.8.8	192.168.2.5	0xe338	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.267229080 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:32.288376093 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.309899092 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:32.809542894 CEST	8.8.8.8	192.168.2.5	0xa108	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.847543955 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:32.872570038 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.894160032 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:32.918351889 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:32.940099001 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:33.313813925 CEST	8.8.8.8	192.168.2.5	0xe874	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.340472937 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:33.362754107 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.382714987 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:33.400686026 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.420860052 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:33.947339058 CEST	8.8.8.8	192.168.2.5	0xca6e	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:33.976629972 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:33.997020960 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.017164946 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:34.037424088 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.055460930 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:34.579391003 CEST	8.8.8.8	192.168.2.5	0x3d5a	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.606172085 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:34.626548052 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.645029068 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:34.670808077 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:34.691076040 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:03:35.637387991 CEST	8.8.8.8	192.168.2.5	0xa2a9	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.667938948 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:35.688895941 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.711240053 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:35.732723951 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:35.755530119 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:36.375839949 CEST	8.8.8.8	192.168.2.5	0xd67b	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.402359009 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:36.424987078 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.445525885 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:36.467850924 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:36.489662886 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:37.983706951 CEST	8.8.8.8	192.168.2.5	0xba9f	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:38.011287928 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:38.032377958 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:38.052937031 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:38.072388887 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:38.090707064 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:38.996529102 CEST	8.8.8.8	192.168.2.5	0x5fe7	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.071681023 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:39.091151953 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.110236883 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:39.132061005 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.151518106 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:39.482498884 CEST	8.8.8.8	192.168.2.5	0xba9f	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.615535975 CEST	8.8.8.8	192.168.2.5	0x82c2	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.646815062 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:39.666840076 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.691112995 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:39.711394072 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:39.733046055 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:40.144674063 CEST	8.8.8.8	192.168.2.5	0x2edf	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.176877022 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:40.198590040 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.217324018 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:03:40.235502958 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:40.253726959 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:42.581233025 CEST	8.8.8.8	192.168.2.5	0x8cc	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.695910931 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:42.717495918 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.736381054 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:42.756829023 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:42.774645090 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:43.834578991 CEST	8.8.8.8	192.168.2.5	0x2679	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.862184048 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:43.881683111 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.903206110 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:43.924917936 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:43.945391893 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:44.472067118 CEST	8.8.8.8	192.168.2.5	0x4cff	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.500081062 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:44.526537895 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.546730042 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:44.567960024 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:44.588005066 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:45.831124067 CEST	8.8.8.8	192.168.2.5	0x8cc	Server failure (2)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.038166046 CEST	8.8.8.8	192.168.2.5	0x6ec8	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.067724943 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:47.089193106 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.111303091 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:47.130348921 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:47.152026892 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:47.509731054 CEST	8.8.8.8	192.168.2.5	0x6ec8	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.198370934 CEST	8.8.8.8	192.168.2.5	0x8128	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.237399101 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:48.258917093 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.283209085 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:48.304694891 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:48.325745106 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:49.241806030 CEST	8.8.8.8	192.168.2.5	0x6ec8	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
Sep 1, 2022 00:03:50.281771898 CEST	8.8.8.8	192.168.2.5	0xab90	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.307605028 CEST	8.8.8.8	192.168.2.5	0xab90	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.317943096 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:50.338493109 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.358608961 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:50.388493061 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:50.416033030 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:52.316684961 CEST	8.8.8.8	192.168.2.5	0x7c25	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.345062017 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:52.370079041 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.388272047 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:52.412725925 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:52.435429096 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:53.933697939 CEST	8.8.8.8	192.168.2.5	0x5962	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:53.962321997 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:53.984399080 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:54.007458925 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:54.026586056 CEST	8.8.8.8	192.168.2.5	0x5962	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:54.035367012 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:54.055593014 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:55.239881992 CEST	8.8.8.8	192.168.2.5	0xc5e7	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.274434090 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:55.294156075 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.313684940 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:55.336025953 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:55.364104986 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:55.794974089 CEST	8.8.8.8	192.168.2.5	0x7c25	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.268456936 CEST	8.8.8.8	192.168.2.5	0x2f3	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.301691055 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:03:56.325932980 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.346476078 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:56.365498066 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:56.386655092 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:58.825668097 CEST	8.8.8.8	192.168.2.5	0xe61c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:58.855791092 CEST	8.8.8.8	192.168.2.5	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
Sep 1, 2022 00:03:58.874407053 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:58.893013000 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:59.415303946 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:03:59.437519073 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:03:59.477504015 CEST	8.8.8.8	192.168.2.5	0xe61c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.200125933 CEST	8.8.8.8	192.168.2.5	0xdb8b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.706511974 CEST	8.8.8.8	192.168.2.5	0xe61c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.922754049 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:00.943747044 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:00.962049007 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:00.982321024 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:01.002304077 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:03.734221935 CEST	8.8.8.8	192.168.2.5	0xc850	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.761651039 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:03.782330036 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.802499056 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:03.822778940 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:03.842823982 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:04.048010111 CEST	8.8.8.8	192.168.2.5	0x9e81	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.074004889 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:04.094161987 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.114377975 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:04.134500980 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.154583931 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:04.195255041 CEST	8.8.8.8	192.168.2.5	0xc850	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.913227081 CEST	8.8.8.8	192.168.2.5	0xed4b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.936587095 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:04.955105066 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:04.975845098 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:04.996162891 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.017935991 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:05.764825106 CEST	8.8.8.8	192.168.2.5	0xc850	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.773658037 CEST	8.8.8.8	192.168.2.5	0x647b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.801095963 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:05.840457916 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:04:05.861089945 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:05.881166935 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:05.901103973 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:06.630609989 CEST	8.8.8.8	192.168.2.5	0xedf0	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.656243086 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:06.677496910 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.698992968 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:06.718585014 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:06.737366915 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:07.451251030 CEST	8.8.8.8	192.168.2.5	0x3852	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.475867033 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:07.495662928 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.513513088 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:07.531666040 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	emsisoft.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:07.552181005 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	emsisoft.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:09.852585077 CEST	8.8.8.8	192.168.2.5	0x26ba	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.861260891 CEST	8.8.8.8	192.168.2.5	0x26ba	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.879578114 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:09.897767067 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.917709112 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:09.935751915 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:09.956202984 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:10.284883022 CEST	8.8.8.8	192.168.2.5	0x26ba	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.678015947 CEST	8.8.8.8	192.168.2.5	0x31f5	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.703870058 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:04:10.724714041 CEST	8.8.8.8	192.168.2.5	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.742995024 CEST	8.8.8.8	192.168.2.5	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:04:10.762958050 CEST	8.8.8.8	192.168.2.5	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:04:10.784327984 CEST	8.8.8.8	192.168.2.5	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 2fiDcmkaZY.exe PID: **6752**, Parent PID: **4696**

General

Target ID:	0
Start time:	00:01:51
Start date:	01/09/2022
Path:	C:\Users\user\Desktop\2fiDcmkaZY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2fiDcmkaZY.exe"
Imagebase:	0xa60000
File size:	75264 bytes
MD5 hash:	A8AC57500DE5DADF8C4DB19959DDF2EC
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: 00000000.00000000.304343043.0000000000A69000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.598939067.0000000000A69000.00000004.00000001.01000000.00000003.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	tbmdhshhgoz	unicode	"C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe"	success or wait	1	A62AAA	RegSetValueExW

Analysis Process: nslookup.exe PID: **6896**, Parent PID: **6752**

General

Target ID:	2
Start time:	00:01:59
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6920**, Parent PID: **6896**

General

Target ID:	3
Start time:	00:02:00
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6972**, Parent PID: **6752**

General

Target ID:	4
Start time:	00:02:00
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6980**, Parent PID: **6972**

General

Target ID:	5
Start time:	00:02:01
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **7032**, Parent PID: **6752**

General

Target ID:	6
Start time:	00:02:03
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **7040**, Parent PID: **7032**

General

Target ID:	7
Start time:	00:02:03
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **7084**, Parent PID: **6752**

General

Target ID:	8
Start time:	00:02:04
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **7092**, Parent PID: **7084**

General

Target ID:	9
Start time:	00:02:04
Start date:	01/09/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **7144**, Parent PID: **6752**

General

Target ID:	10
Start time:	00:02:06
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **7152**, Parent PID: **7144**

General

Target ID:	11
Start time:	00:02:07
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tdicrr.exe PID: **1476**, Parent PID: **3324**

General

Target ID:	13
Start time:	00:02:09

Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe"
Imagebase:	0xc70000
File size:	75264 bytes
MD5 hash:	D2E112FDFFC314778285E837BC0BED47
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: 0000000D.00000000.343462206.0000000000C79000.00000008.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000D.00000002.346586335.0000000000C79000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: Joe Security • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe, Author: kevoreilly
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: nslookup.exe PID: **5388**, Parent PID: **6752**

General

Target ID:	14
Start time:	00:02:12
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5320**, Parent PID: **5388**

General

Target ID:	15
Start time:	00:02:12
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6752**

General

Target ID:	16
Start time:	00:02:14
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **2992**, Parent PID: **6392**

General

Target ID:	17
Start time:	00:02:14
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **3096**, Parent PID: **6752**

General

Target ID:	18
Start time:	00:02:16
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5808**, Parent PID: **3096**

General

Target ID:	19
Start time:	00:02:16
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tdicrr.exe PID: **5864**, Parent PID: **3324**

General

Target ID:	20
Start time:	00:02:17
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\tdicrr.exe"
Imagebase:	0xc70000
File size:	75264 bytes
MD5 hash:	D2E112FDFFC314778285E837BC0BED47
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: 00000014.00000002.363374033.0000000000C79000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000014.00000000.360474661.0000000000C79000.00000008.00000001.01000000.00000004.sdmp, Author: Joe Security

Analysis Process: nslookup.exe PID: **5940**, Parent PID: **6752**

General

Target ID:	21
Start time:	00:02:18
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: 5836, Parent PID: 5940

General	
Target ID:	22
Start time:	00:02:18
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 6024, Parent PID: 6752

General	
Target ID:	23
Start time:	00:02:19
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: 6036, Parent PID: 6024

General	
Target ID:	24
Start time:	00:02:20
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000

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: **5872**, Parent PID: **6752**

General

Target ID:	26
Start time:	00:02:21
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6568**, Parent PID: **5872**

General

Target ID:	27
Start time:	00:02:21
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6752**

General

Target ID:	28
Start time:	00:02:22
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6636**, Parent PID: **6632**

General

Target ID:	29
Start time:	00:02:23
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5964**, Parent PID: **6752**

General

Target ID:	31
Start time:	00:02:25
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6460**, Parent PID: **5964**

General

Target ID:	32
Start time:	00:02:27

Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6308**, Parent PID: **6752**

General

Target ID:	33
Start time:	00:02:30
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6524**, Parent PID: **6308**

General

Target ID:	34
Start time:	00:02:31
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6952**, Parent PID: **6752**

General

Target ID:	35
Start time:	00:02:32
Start date:	01/09/2022

Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6964**, Parent PID: **6952**

General

Target ID:	36
Start time:	00:02:32
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6848**, Parent PID: **6752**

General

Target ID:	37
Start time:	00:02:34
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6844**, Parent PID: **6848**

General	
Target ID:	38
Start time:	00:02:34
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **7044**, Parent PID: **6752**

General	
Target ID:	39
Start time:	00:02:37
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5040**, Parent PID: **7044**

General	
Target ID:	40
Start time:	00:02:38
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 7040, Parent PID: 6752

General

Target ID:	41
Start time:	00:02:39
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: 7036, Parent PID: 7040

General

Target ID:	42
Start time:	00:02:39
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 7104, Parent PID: 6752

General

Target ID:	43
Start time:	00:02:41
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5684**, Parent PID: **7104**

General

Target ID:	45
Start time:	00:02:41
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **7148**, Parent PID: **6752**

General

Target ID:	49
Start time:	00:02:45
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **712**, Parent PID: **7148**

General

Target ID:	50
Start time:	00:02:48
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **4556**, Parent PID: **6752**

General	
Target ID:	51
Start time:	00:02:49
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6092**, Parent PID: **4556**

General	
Target ID:	52
Start time:	00:02:50
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5844**, Parent PID: **6752**

General	
Target ID:	53
Start time:	00:02:52
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5888**, Parent PID: **5844**

General

Target ID:	54
Start time:	00:02:52
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5976**, Parent PID: **6752**

General

Target ID:	55
Start time:	00:02:54
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5944**, Parent PID: **5976**

General

Target ID:	56
Start time:	00:02:55
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6564**, Parent PID: **6752**

General

Target ID:	58

Start time:	00:02:57
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6028**, Parent PID: **6564**

General	
Target ID:	59
Start time:	00:02:57
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5860**, Parent PID: **6752**

General	
Target ID:	60
Start time:	00:03:02
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **5892**, Parent PID: **5860**

General	
Target ID:	61
Start time:	00:03:02
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6608**, Parent PID: **6752**

General	
Target ID:	62
Start time:	00:03:05
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6588**, Parent PID: **6608**

General	
Target ID:	63
Start time:	00:03:08
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6032**, Parent PID: **6752**

General	
Target ID:	64
Start time:	00:03:10
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6912**, Parent PID: **6032**

General

Target ID:	65
Start time:	00:03:11
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6440**, Parent PID: **6752**

General	
Target ID:	66
Start time:	00:03:12
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6076**, Parent PID: **6440**

General	
Target ID:	67
Start time:	00:03:13
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6460**, Parent PID: **6752**

General	
Target ID:	68
Start time:	00:03:15
Start date:	01/09/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup emsisoft.bit dns1.soprodns.ru
Imagebase:	0xcd0000
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: **6788**, Parent PID: **6460**

General

Target ID:	69
Start time:	00:03:15
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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