



ID: 694566
Sample Name: gI5xZdIxUs.exe
Cookbook: default.jbs
Time: 23:56:48
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report gI5xZdIxUs.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Initial Sample 6
Dropped Files 6
Memory Dumps 6
Unpacked PEs 7
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 24
AV Detection 24
Networking 24
Spam, unwanted Advertisements and Ransom Demands 24
System Summary 24
Data Obfuscation 24
Mitre Att&ck Matrix 24
Behavior Graph 25
Screenshots 26
Thumbnails 26
Antivirus, Machine Learning and Genetic Malware Detection 27
Initial Sample 27
Dropped Files 27
Unpacked PE Files 27
Domains 28
URLs 28
Domains and IPs 28
Contacted Domains 28
URLs from Memory and Binaries 28
World Map of Contacted IPs 28
General Information 28
Warnings 29
Simulations 29
Behavior and APIs 29
Joe Sandbox View / Context 29
IPs 29
Domains 29
ASNs 29
JA3 Fingerprints 30
Dropped Files 30
Created / dropped Files 30
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a 30
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe 30
Static File Info 31
General 31
File Icon 31
Static PE Info 31
General 31
Entrypoint Preview 31
Rich Headers 33
Data Directories 33
Sections 33
Resources 33
Imports 34
Exports 34
Possible Origin 34
Network Behavior 34
Snort IDS Alerts 34
UDP Packets 39
ICMP Packets 50
DNS Queries 50
DNS Answers 59
Statistics 68
Behavior 68
System Behavior 68
Analysis Process: gI5xZdIxUs.exePID: 5280, Parent PID: 5364 68
General 69

File Activities 69
Registry Activities 69
Key Value Created 69
Analysis Process: nslookup.exePID: 5960, Parent PID: 5280 69
General 69
File Activities 69
Analysis Process: conhost.exePID: 792, Parent PID: 5960 69
General 69
Analysis Process: nslookup.exePID: 4684, Parent PID: 5280 70
General 70
File Activities 70
Analysis Process: conhost.exePID: 5556, Parent PID: 4684 70
General 70
Analysis Process: isqmkp.exePID: 5464, Parent PID: 3452 71
General 71
Analysis Process: nslookup.exePID: 4596, Parent PID: 5280 71
General 71
File Activities 71
Analysis Process: conhost.exePID: 1920, Parent PID: 4596 71
General 72
Analysis Process: nslookup.exePID: 6112, Parent PID: 5280 72
General 72
File Activities 72
Analysis Process: conhost.exePID: 4624, Parent PID: 6112 72
General 72
Analysis Process: isqmkp.exePID: 1572, Parent PID: 3452 73
General 73
Analysis Process: nslookup.exePID: 1916, Parent PID: 5280 73
General 73
File Activities 73
Analysis Process: conhost.exePID: 5388, Parent PID: 1916 73
General 73
Analysis Process: nslookup.exePID: 5244, Parent PID: 5280 74
General 74
File Activities 74
Analysis Process: conhost.exePID: 4592, Parent PID: 5244 74
General 74
Analysis Process: nslookup.exePID: 6028, Parent PID: 5280 74
General 74
File Activities 75
Analysis Process: conhost.exePID: 1012, Parent PID: 6028 75
General 75
Analysis Process: nslookup.exePID: 5116, Parent PID: 5280 75
General 75
File Activities 75
Analysis Process: conhost.exePID: 5552, Parent PID: 5116 75
General 75
Analysis Process: nslookup.exePID: 680, Parent PID: 5280 76
General 76
File Activities 76
Analysis Process: conhost.exePID: 496, Parent PID: 680 76
General 76
Analysis Process: nslookup.exePID: 5124, Parent PID: 5280 76
General 76
File Activities 77
Analysis Process: conhost.exePID: 5484, Parent PID: 5124 77
General 77
Analysis Process: nslookup.exePID: 4972, Parent PID: 5280 77
General 77
File Activities 77
Analysis Process: conhost.exePID: 6096, Parent PID: 4972 77
General 78
Analysis Process: nslookup.exePID: 5604, Parent PID: 5280 78
General 78
File Activities 78
Analysis Process: conhost.exePID: 1784, Parent PID: 5604 78
General 78
Analysis Process: nslookup.exePID: 736, Parent PID: 5280 78
General 78
File Activities 79
Analysis Process: conhost.exePID: 6060, Parent PID: 736 79
General 79
Analysis Process: nslookup.exePID: 4460, Parent PID: 5280 79
General 79
File Activities 79
Analysis Process: conhost.exePID: 4560, Parent PID: 4460 80
General 80
Analysis Process: nslookup.exePID: 6052, Parent PID: 5280 80
General 80
File Activities 80
Analysis Process: conhost.exePID: 5984, Parent PID: 6052 80
General 80
Analysis Process: nslookup.exePID: 5424, Parent PID: 5280 81
General 81
File Activities 81
Analysis Process: conhost.exePID: 1000, Parent PID: 5424 81
General 81
Analysis Process: nslookup.exePID: 4364, Parent PID: 5280 81

General 81
File Activities 82
Analysis Process: conhost.exePID: 1552, Parent PID: 4364 82
General 82
Analysis Process: nslookup.exePID: 5188, Parent PID: 5280 82
General 82
File Activities 82
Analysis Process: conhost.exePID: 1960, Parent PID: 5188 82
General 82
Analysis Process: nslookup.exePID: 1164, Parent PID: 5280 83
General 83
File Activities 83
Analysis Process: conhost.exePID: 5824, Parent PID: 1164 83
General 83
Analysis Process: nslookup.exePID: 1092, Parent PID: 5280 83
General 83
File Activities 84
Analysis Process: conhost.exePID: 5844, Parent PID: 1092 84
General 84
Analysis Process: nslookup.exePID: 968, Parent PID: 5280 84
General 84
File Activities 84
Analysis Process: conhost.exePID: 5636, Parent PID: 968 84
General 84
Disassembly 85

Copyright Joe Security LLC 2022

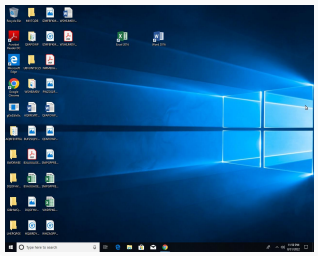
Windows Analysis Report

gI5xZdIxUs.exe

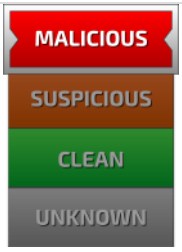
Overview

General Information

Sample Name:	gI5xZdIxUs.exe
Analysis ID:	694566
MD5:	98a12ec721c098..
SHA1:	9dfd7d1746c8ae..
SHA256:	f83457d173841c..
Tags:	exe
Infos:	



Detection



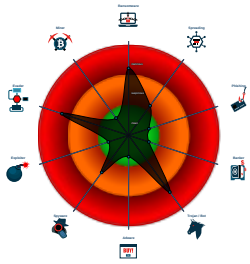
Gandcrab, ReflectiveLoader

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

Signatures

- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected ReflectiveLoader
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- 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**
- gI5xZdIxUs.exe (PID: 5280 cmdline: "C:\Users\user\Desktop\gI5xZdIxUs.exe" MD5: 98A12EC721C098842FBFD7384D5A72AE)
  - nslookup.exe (PID: 5960 cmdline: nslookup nomoreransom.coin dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4684 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4596 cmdline: nslookup gandcrab.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 1920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6112 cmdline: nslookup nomoreransom.coin dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 4624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 1916 cmdline: nslookup nomoreransom.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5244 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 4592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6028 cmdline: nslookup nomoreransom.coin dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 1012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5116 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 680 cmdline: nslookup gandcrab.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5124 cmdline: nslookup nomoreransom.coin dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4972 cmdline: nslookup nomoreransom.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5604 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 1784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 736 cmdline: nslookup nomoreransom.coin dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4460 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 4560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 6052 cmdline: nslookup gandcrab.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 5984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5424 cmdline: nslookup nomoreransom.coin dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 4364 cmdline: nslookup nomoreransom.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - conhost.exe (PID: 1552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5188 cmdline: nslookup gandcrab.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)

Copyright Joe Security LLC 2022

- conhost.exe (PID: 1960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 1164 cmdline: nslookup nomoreransom.coin dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 1092 cmdline: nslookup nomoreransom.bit dns1.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nslookup.exe (PID: 968 cmdline: nslookup gandcrab.bit dns2.soprodns.ru MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
  - conhost.exe (PID: 5636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- isqmkp.exe (PID: 5464 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe" MD5: F4758788F11A0DE8D11EB4B8C515FFBD)
- isqmkp.exe (PID: 1572 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe" MD5: F4758788F11A0DE8D11EB4B8C515FFBD)
  - **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
gI5xZdIxUs.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xed22:$x1: ReflectiveLoader
gI5xZdIxUs.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe67e:$: DECRYPT.txt • 0xe6e4:$: DECRYPT.txt
gI5xZdIxUs.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
gI5xZdIxUs.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
gI5xZdIxUs.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xed21:$s1: _ReflectiveLoader@ • 0xed22:$s2: ReflectiveLoader@
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xed22:$x1: ReflectiveLoader
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe67e:$: DECRYPT.txt • 0xe6e4:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xed21:$s1: _ReflectiveLoader@ • 0xed22:$s2: ReflectiveLoader@
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000000.322631215.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0000000E.00000002.315651936.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0000000E.00000000.307654244.000000000F9E2000.00000008.00000001.01000000.00000005.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000001.00000000.272296797.000000000FC6A000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0000000E.00000000.307645700.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.isqmkp.exe.f9d0000.0.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xed22:$x1: ReflectiveLoader
14.2.isqmkp.exe.f9d0000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe67e:$: DECRYPT.txt • 0xe6e4:$: DECRYPT.txt
14.2.isqmkp.exe.f9d0000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
14.2.isqmkp.exe.f9d0000.0.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
14.2.isqmkp.exe.f9d0000.0.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xed21:$s1: _ReflectiveLoader@ • 0xed22:$s2: ReflectiveLoader@
Click to see the 31 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.860754532829498 08/31/22-23:58:43.044195
SID:	2829498
Source Port:	60754
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.850789532829498 08/31/22-23:59:48.239260
SID:	2829498
Source Port:	50789
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.858305532829498 08/31/22-23:59:32.365598
SID:	2829498

Copyright Joe Security LLC 2022

Source Port:	58305
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865389532829498 08/31/22-23:59:40.892307
SID:	2829498
Source Port:	65389
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849203532026737 08/31/22-23:59:56.322889
SID:	2026737
Source Port:	49203
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856952532026737 08/31/22-23:58:46.555077
SID:	2026737
Source Port:	56952
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853051532829498 08/31/22-23:59:12.297576
SID:	2829498
Source Port:	53051
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853431532829498 08/31/22-23:59:18.287185
SID:	2829498
Source Port:	53431
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865022532829498 08/31/22-23:58:54.690068
SID:	2829498
Source Port:	65022
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.861420532829498 08/31/22-23:59:01.493233
SID:	2829498
Source Port:	61420
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.851994532829498 08/31/22-23:59:24.206869
SID:	2829498
Source Port:	51994
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860478532829498 08/31/22-23:59:59.939438
SID:	2829498
Source Port:	60478
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865019532829498 08/31/22-23:58:54.630989
SID:	2829498
Source Port:	65019
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850230532026737 09/01/22-00:00:07.433896
SID:	2026737
Source Port:	50230
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860093532026737 08/31/22-23:59:14.413883
SID:	2026737
Source Port:	60093
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858122532026737 08/31/22-23:59:27.247839
SID:	2026737
Source Port:	58122
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865515532026737 08/31/22-23:59:20.761806
SID:	2026737
Source Port:	65515
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852958532829498 08/31/22-23:58:07.331283
SID:	2829498
Source Port:	52958

Copyright Joe Security LLC 2022

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.854156532026737 08/31/22-23:59:42.281210
SID:	2026737
Source Port:	54156
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865110532829498 08/31/22-23:58:33.358759
SID:	2829498
Source Port:	65110
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853430532829498 08/31/22-23:59:18.269254
SID:	2829498
Source Port:	53430
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858121532026737 08/31/22-23:59:27.189978
SID:	2026737
Source Port:	58121
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865021532829498 08/31/22-23:58:54.669703
SID:	2829498
Source Port:	65021
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858306532829498 08/31/22-23:59:32.396919
SID:	2829498
Source Port:	58306
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864126532026737 08/31/22-23:59:50.649034
SID:	2026737
Source Port:	64126
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858695532026737 08/31/22-23:58:36.600606
SID:	2026737
Source Port:	58695
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.861418532829498 08/31/22-23:59:01.454658
SID:	2829498
Source Port:	61418
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865516532026737 08/31/22-23:59:20.780161
SID:	2026737
Source Port:	65516
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865111532829498 08/31/22-23:58:33.379307
SID:	2829498
Source Port:	65111
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865388532829498 08/31/22-23:59:40.874321
SID:	2829498
Source Port:	65388
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858694532026737 08/31/22-23:58:36.580328
SID:	2026737
Source Port:	58694
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.854155532026737 08/31/22-23:59:42.262891
SID:	2026737
Source Port:	54155
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852957532829498 08/31/22-23:58:07.312591
SID:	2829498
Source Port:	52957

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.849204532026737 08/31/22-23:59:56.342973
SID:	2026737
Source Port:	49204
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.860586532026737 08/31/22-23:58:15.043750
SID:	2026737
Source Port:	60586
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.850231532026737 09/01/22-00:00:07.455721
SID:	2026737
Source Port:	50231
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.852959532829498 08/31/22-23:58:07.365561
SID:	2829498
Source Port:	52959
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.862054532829498 08/31/22-23:58:21.744663
SID:	2829498
Source Port:	62054
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.859641532026737 08/31/22-23:58:24.944174
SID:	2026737
Source Port:	59641
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.859638532026737 08/31/22-23:58:24.884406
SID:	2026737
Source Port:	59638
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865198532026737 08/31/22-23:59:03.441447
SID:	2026737
Source Port:	65198
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865109532829498 08/31/22-23:58:33.338202
SID:	2829498
Source Port:	65109
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852457532829498 09/01/22-00:00:11.310934
SID:	2829498
Source Port:	52457
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860587532026737 08/31/22-23:58:15.064663
SID:	2026737
Source Port:	60587
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853470532026737 08/31/22-23:58:56.772805
SID:	2026737
Source Port:	53470
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856620532026737 09/01/22-00:00:02.142088
SID:	2026737
Source Port:	56620
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858693532026737 08/31/22-23:58:36.550637
SID:	2026737
Source Port:	58693
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858696532026737 08/31/22-23:58:36.619047
SID:	2026737
Source Port:	58696

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856954532026737 08/31/22-23:58:46.594398
SID:	2026737
Source Port:	56954
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849205532026737 08/31/22-23:59:56.360951
SID:	2026737
Source Port:	49205
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856619532026737 09/01/22-00:00:02.120945
SID:	2026737
Source Port:	56619
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.851995532829498 08/31/22-23:59:24.227191
SID:	2829498
Source Port:	51995
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.861421532829498 08/31/22-23:59:01.511754
SID:	2829498
Source Port:	61421
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852960532829498 08/31/22-23:58:07.384051
SID:	2829498
Source Port:	52960
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865390532829498 08/31/22-23:59:40.910653
SID:	2829498
Source Port:	65390
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853053532829498 08/31/22-23:59:12.348894
SID:	2829498
Source Port:	53053
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.854158532026737 08/31/22-23:59:42.322126
SID:	2026737
Source Port:	54158
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860753532829498 08/31/22-23:58:43.024087
SID:	2829498
Source Port:	60753
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857391532829498 09/01/22-00:00:05.158775
SID:	2829498
Source Port:	57391
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858303532829498 08/31/22-23:59:32.323930
SID:	2829498
Source Port:	58303
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860584532026737 08/31/22-23:58:15.004694
SID:	2026737
Source Port:	60584
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858123532026737 08/31/22-23:59:27.268863
SID:	2026737
Source Port:	58123
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860091532026737 08/31/22-23:59:14.371988
SID:	2026737
Source Port:	60091

Copyright Joe Security LLC 2022

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865200532026737 08/31/22-23:59:03.482704
SID:	2026737
Source Port:	65200
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853433532829498 08/31/22-23:59:18.325585
SID:	2829498
Source Port:	53433
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850787532829498 08/31/22-23:59:48.189200
SID:	2829498
Source Port:	50787
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860751532829498 08/31/22-23:58:42.984219
SID:	2829498
Source Port:	60751
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850786532829498 08/31/22-23:59:48.168544
SID:	2829498
Source Port:	50786
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853468532026737 08/31/22-23:58:56.731128
SID:	2026737
Source Port:	53468
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.849206532026737 08/31/22-23:59:56.381031
SID:	2026737
Source Port:	49206
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860475532829498 08/31/22-23:59:59.877731
SID:	2829498
Source Port:	60475
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863448532026737 08/31/22-23:59:36.563649
SID:	2026737
Source Port:	63448
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.851997532829498 08/31/22-23:59:24.265731
SID:	2829498
Source Port:	51997
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856618532026737 09/01/22-00:00:02.100951
SID:	2026737
Source Port:	56618
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853471532026737 08/31/22-23:58:56.793274
SID:	2026737
Source Port:	53471
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853054532829498 08/31/22-23:59:12.369224
SID:	2829498
Source Port:	53054
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852458532829498 09/01/22-00:00:11.330853
SID:	2829498
Source Port:	52458
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865513532026737 08/31/22-23:59:20.720500
SID:	2026737
Source Port:	65513

Copyright Joe Security LLC 2022

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

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860828532829498 08/31/22-23:59:53.952246
SID:	2829498
Source Port:	60828
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864124532026737 08/31/22-23:59:50.605079
SID:	2026737
Source Port:	64124
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.862052532829498 08/31/22-23:58:21.699516
SID:	2829498
Source Port:	62052
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857390532829498 09/01/22-00:00:05.138814
SID:	2829498
Source Port:	57390
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850233532026737 09/01/22-00:00:07.502496
SID:	2026737
Source Port:	50233
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860090532026737 08/31/22-23:59:14.353291
SID:	2026737
Source Port:	60090
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852459532829498 09/01/22-00:00:11.350932
SID:	2829498
Source Port:	52459
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860827532829498 08/31/22-23:59:53.930680
SID:	2829498
Source Port:	60827
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853469532026737 08/31/22-23:58:56.749513
SID:	2026737
Source Port:	53469
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850232532026737 09/01/22-00:00:07.481526
SID:	2026737
Source Port:	50232
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865387532829498 08/31/22-23:59:40.854236
SID:	2829498
Source Port:	65387
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863451532026737 08/31/22-23:59:36.620733
SID:	2026737
Source Port:	63451
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864125532026737 08/31/22-23:59:50.625202
SID:	2026737
Source Port:	64125
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860476532829498 08/31/22-23:59:59.898864
SID:	2829498
Source Port:	60476
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.854157532026737 08/31/22-23:59:42.301537
SID:	2026737
Source Port:	54157

Copyright Joe Security LLC 2022

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

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857392532829498 09/01/22-00:00:05.176878
SID:	2829498
Source Port:	57392
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852460532829498 09/01/22-00:00:11.371195
SID:	2829498
Source Port:	52460
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.857389532829498 09/01/22-00:00:05.118977
SID:	2829498
Source Port:	57389
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856043532829498 08/31/22-23:58:21.768917
SID:	2829498
Source Port:	56043
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853052532829498 08/31/22-23:59:12.328339
SID:	2829498
Source Port:	53052
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.861419532829498 08/31/22-23:59:01.474961
SID:	2829498
Source Port:	61419
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.851996532829498 08/31/22-23:59:24.245596
SID:	2829498
Source Port:	51996
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.853432532829498 08/31/22-23:59:18.305428
SID:	2829498
Source Port:	53432
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860585532026737 08/31/22-23:58:15.025136
SID:	2026737
Source Port:	60585
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863450532026737 08/31/22-23:59:36.602428
SID:	2026737
Source Port:	63450
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860477532829498 08/31/22-23:59:59.919053
SID:	2829498
Source Port:	60477
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856951532026737 08/31/22-23:58:46.526858
SID:	2026737
Source Port:	56951
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865112532829498 08/31/22-23:58:33.402809
SID:	2829498
Source Port:	65112
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865020532829498 08/31/22-23:58:54.651252
SID:	2829498
Source Port:	65020
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863449532026737 08/31/22-23:59:36.584182
SID:	2026737
Source Port:	63449

Copyright Joe Security LLC 2022

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865201532026737 08/31/22-23:59:03.503720
SID:	2026737
Source Port:	65201
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860830532829498 08/31/22-23:59:53.997132
SID:	2829498
Source Port:	60830
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859640532026737 08/31/22-23:58:24.925442
SID:	2026737
Source Port:	59640
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.864123532026737 08/31/22-23:59:50.576561
SID:	2026737
Source Port:	64123
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.850788532829498 08/31/22-23:59:48.220006
SID:	2829498
Source Port:	50788
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860092532026737 08/31/22-23:59:14.392903
SID:	2026737
Source Port:	60092
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858124532026737 08/31/22-23:59:27.287358
SID:	2026737
Source Port:	58124
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865199532026737 08/31/22-23:59:03.462712
SID:	2026737
Source Port:	65199
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859639532026737 08/31/22-23:58:24.905091
SID:	2026737
Source Port:	59639
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856953532026737 08/31/22-23:58:46.573613
SID:	2026737
Source Port:	56953
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.858304532829498 08/31/22-23:59:32.344904
SID:	2829498
Source Port:	58304
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860752532829498 08/31/22-23:58:43.003278
SID:	2829498
Source Port:	60752
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.865514532026737 08/31/22-23:59:20.740564
SID:	2026737
Source Port:	65514
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860829532829498 08/31/22-23:59:53.975918
SID:	2829498
Source Port:	60829
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN GandCrab DNS Lookup 1 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.862053532829498 08/31/22-23:58:21.721380
SID:	2829498
Source Port:	62053

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

ET TROJAN Observed GandCrab Domain (gandcrab .bit) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.38.8.8.856621532026737 09/01/22-00:00:02.160962
SID:	2026737
Source Port:	56621
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
- Multi AV Scanner detection for domain / URL
- 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
- Performs many domain queries via nslookup

Spam, unwanted Advertisements and Ransom Demands



- Yara detected Gandcrab

System Summary



- Malicious sample detected (through community Yara rule)

Data Obfuscation



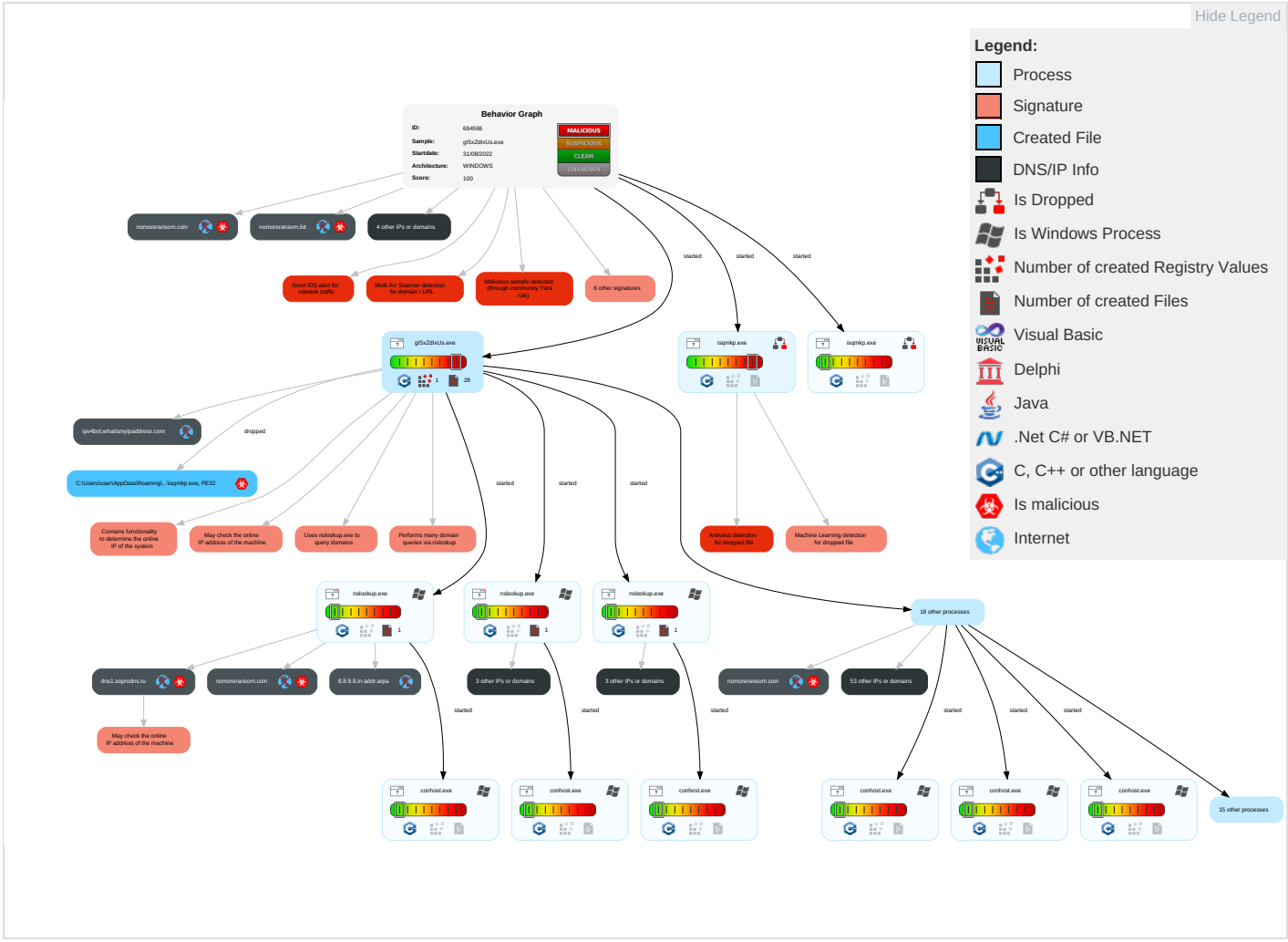
- Yara detected ReflectiveLoader

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

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	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

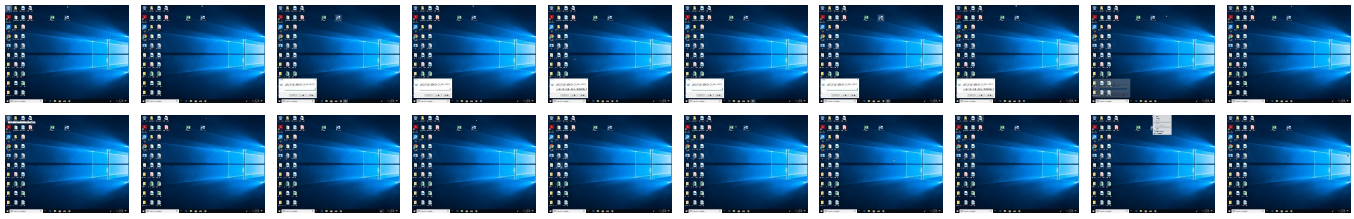
Behavior Graph



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
gI5xZdlxUs.exe	86%	Virustotal		Browse
gI5xZdlxUs.exe	74%	Metadefender		Browse
gI5xZdlxUs.exe	93%	ReversingLabs	Win32.Ransomware.GandCrab	
gI5xZdlxUs.exe	100%	Avira	TR/Dropper.Gen	
gI5xZdlxUs.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.gI5xZdlxUs.exe.fc60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.isqmkp.exe.f9d0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.2.isqmkp.exe.f9d0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.2.isqmkp.exe.f9d0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
1.0.gI5xZdIxUs.exe.fc60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.isqmkp.exe.f9d0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
nomoreransom.coin	2%	Virustotal		Browse
nomoreransom.bit	1%	Virustotal		Browse
gandcrab.bit	2%	Virustotal		Browse
dns1.soprodns.ru	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gdcbghvjyqy7jclk.onion/3a23db8448d3b2b	0%	URL Reputation	safe	
http://https://tox.chat/download.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nomoreransom.coin	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
ipv4bot.whatismyipaddress.com	unknown	unknown	false		high
nomoreransom.bit	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
gandcrab.bit	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
dns1.soprodns.ru	unknown	unknown	true	• 5%, Virustotal, Browse	unknown
dns2.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://ipv4bot.whatismyipaddress.com/a	gI5xZdIxUs.exe, 00000001.00000002.537080039.0000000000C7A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.torproject.org/	gI5xZdIxUs.exe, isqmkp.exe.1.dr	false		high
http://ipv4bot.whatismyipaddress.com/4	gI5xZdIxUs.exe, 00000001.00000002.537080039.0000000000C7A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://gdcbghvjyqy7jclk.onion/3a23db8448d3b2b	gI5xZdIxUs.exe, isqmkp.exe.1.dr	true	• URL Reputation: safe	unknown
http://ipv4bot.whatismyipaddress.com/	gI5xZdIxUs.exe, 00000001.00000002.537080039.0000000000C7A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://tox.chat/download.html	gI5xZdIxUs.exe, isqmkp.exe.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694566
Start date and time:	2022-08-31 23:56:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2022

Report type:	light
Sample file name:	gI5xZdIxUs.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:	62
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@85/2@305/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 96%) • Quality average: 83.6% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 20.82.228.9
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, store-images.s-microsoft.com, neus2c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:57:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce bwduumgtptl "C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe"
23:58:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce bwduumgtptl "C:\Users\user\AppData\Roaming\Microsoft\isqmkp.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\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\gI5xZdIxUs.exe
File Type:	data
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	F97F9E17EAFDD0105A4E11BAFDE04B40
SHA1:	BA06A7ABE986A61B71889B80A6F9B02B22D40667
SHA-256:	4783424121E6C2F870DC931B374D20C62C764EDDC5769D2F536609ADC1226ABB
SHA-512:	778C4AAB55F6F0FE44DBC9A97F53B59EC8ED2E35901F77AFEBAEA57C738AD301412760709AB909B51335DDD7676CD8F8C1410C5751F2EF5CC74282BCD6C5F50E
Malicious:	false
Preview:	....

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

Process:	C:\Users\user\Desktop\gI5xZdIxUs.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	101710
Entropy (8bit):	5.97549755837271
Encrypted:	false
SSDEEP:	1536:dZZZZZZZZZZZZpXzzzzzzzzzzzzV9rXounV98hbHnAwfMqqU+2bbbAV2/S2LkvdQ:BBounVyFHpfMqqDL2/LkvdmYvQd2a
MD5:	F4758788F11A0DE8D11EB4B8C515FFBD
SHA1:	04C1326C595D62977F53037F91B3FB863D4039BA
SHA-256:	DFCE3F5E421DEAF40DAB26ABDF67D5873968DB47B6DDE38787B90FF2CEAB3C96
SHA-512:	49C27F1DFA7C78C99C9055772D04BC89CEA41DF2DF027A400C915195FC82E8904FD89974F30CC7FD484A998DB0AE4B6F5440B5BA02FC56D2BB1ECE98117FB038
Malicious:	**true**
Yara Hits:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: kevoreilly
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This .R.Y6.m cannot be run in DOS mode....$.....Tg..:4..:4..:4..4..:4..4..:4...4..:4..:4..:4..:4..:4..:42.:4...4..:4...4..:4...4. .:4...4..:4Rich..:4.....PE..L....Z.Z.....K.....p.....@.....U...8.....`.....P..... .....text..... ..`.rdata...p.....r.....@..@.data..... .....@....CRT.....0.....@..@.rsrc.....@..... @..@.reloc.....P.....@..B.I2.....`.....@..@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.9754370991350365
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:	gI5xZdIxUs.exe
File size:	101710
MD5:	98a12ec721c098842fbfd7384d5a72ae
SHA1:	9dfd7d1746c8ae943f3dced0f85f0e3c6f5084f3
SHA256:	f83457d173841c7e944bc60b00c197ca93c864893c71902cf1b1a36decdd30a4
SHA512:	a0b74851a36115822bf619a1a767cd76f57539a87dbbd4d452f309839f903ad7d94937a46acdcbc1e41bb50e381fe0fd2394122ec1260f05722a578030973ed8
SSDEEP:	1536:YZZZZZZZZZZZZpXzzzzzzzzzzzzV9rXounV98hbHnAwfMqqU+2bbbAV2/S2LkvdQ:WBounVyFHpfMqqDL2/LkvdmYvQd2a
TLSH:	F8A3490972E1A0A3E1E20679E5756EE5456E3C103F2496EB3993378D69728F0AD3B703
File Content Preview:	MZ.....@.....!..L.!This .<].e.m cannot be run in DOS mode....$.....Tg..:4..:4..:4...4..:4...4..:4...4..:4..:4..:4...4..:4..:42.:4...4..:4...4..:4...4..:4...4..:4Rich..:4.....PE..L....Z.Z...

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x10004bf0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x5A8C5AD9 [Tue Feb 20 17:28:57 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:	6b11af918234585a966ca8fab046dc6c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 0Ch
mov dword ptr [ebp-0Ch], 00000001h
mov eax, dword ptr [ebp+0Ch]

Instruction
mov dword ptr [ebp-08h], eax
cmp dword ptr [ebp-08h], 01h
jmp 00007F0364768A56h
jmp 00007F0364768A7Ch
jmp 00007F0364768A7Ah
push 00000000h
push 00000000h
push 00000000h
push 10004950h
push 00000000h
push 00000000h
call dword ptr [1000A108h]
mov dword ptr [ebp-04h], eax
cmp dword ptr [ebp-04h], 00000000h
je 00007F0364768A5Ch
mov ecx, dword ptr [ebp-04h]
push ecx
call dword ptr [1000A10Ch]
mov eax, dword ptr [ebp-0Ch]
mov esp, ebp
pop ebp
retn 000Ch
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
movdqu dqword ptr [ebp-10h], xmm0
call 00007F036476CE07h
mov eax, dword ptr [10012A6Ch]
add esp, 0Ch
mov dword ptr [ebp-18h], eax
mov dword ptr [ebp-1Ch], eax
mov eax, dword ptr [10012A68h]
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 [1000A164h]

Instruction
test eax, eax
jne 00007F0364768A5Dh
call dword ptr [1000A064h]
pop esi
mov esp, ebp
pop ebp
ret
push dword ptr [ebp-10h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x104e0	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10538	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x200	.I2
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15000	0xac4	.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	0xa000	0x1fc	.rdata
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	0x82e8	0x8400	False	0.4593690814393939	data	6.340223357377212	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x70a6	0x7200	False	0.4923245614035088	data	6.181274430024402	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0xa80	0xc00	False	0.3160807291666667	data	3.1174892908286225	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x13000	0x4	0x200	False	0.033203125	data	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1e0	0x200	False	0.52734375	data	4.7176788329467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15000	0xac4	0xc00	False	0.7802734375	data	6.4568381269501165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.I2	0x16000	0x200	0x200	False	0.52734375	data	4.7137725829467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x16060	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, GetProcAddress, Process32FirstW, GetTempPathW, GetProcessHeap, HeapFree, HeapAlloc, lstrlenA, CreateProcessW, ExitProcess, IsProcessorFeaturePresent
USER32.dll	BeginPaint, wsprintfW, TranslateMessage, LoadCursorW, LoadIconW, MessageBoxA, GetMessageW, EndPaint, DestroyWindow, RegisterClassExW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, GetForegroundWindow, SetWindowLongW
GDI32.dll	TextOutW
ADVAPI32.dll	FreeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptExportKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, AllocateAndInitializeSid
SHELL32.dll	ShellExecuteW, SHGetSpecialFolderPathW, ShellExecuteExW
CRYPT32.dll	CryptStringToBinaryA, CryptBinaryToStringA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

Exports

Name	Ordinal	Address
_ReflectiveLoader@0	1	0x10005ec0

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
192.168.2.38.8.8.8607545 32829498 08/31/22-23:58:43.044195	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60754	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8507895 32829498 08/31/22-23:59:48.239260	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50789	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8583055 32829498 08/31/22-23:59:32.365598	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58305	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8653895 32829498 08/31/22-23:59:40.892307	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65389	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8492035 32026737 08/31/22-23:59:56.322889	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49203	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8569525 32026737 08/31/22-23:58:46.555077	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56952	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8530515 32829498 08/31/22-23:59:12.297576	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53051	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534315 32829498 08/31/22-23:59:18.287185	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53431	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8650225 32829498 08/31/22-23:58:54.690068	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65022	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8614205 32829498 08/31/22-23:59:01.493233	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61420	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8519945 32829498 08/31/22-23:59:24.206869	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51994	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8604785 32829498 08/31/22-23:59:59.939438	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60478	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8650195 32829498 08/31/22-23:58:54.630989	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65019	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8502305 32026737 09/01/22-00:00:07.433896	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50230	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8600935 32026737 08/31/22-23:59:14.413883	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60093	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8581225 32026737 08/31/22-23:59:27.247839	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58122	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8655155 32026737 08/31/22-23:59:20.761806	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65515	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8529585 32829498 08/31/22-23:58:07.331283	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52958	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8541565 32026737 08/31/22-23:59:42.281210	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54156	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651105 32829498 08/31/22-23:58:33.358759	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65110	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534305 32829498 08/31/22-23:59:18.269254	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53430	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8581215 32026737 08/31/22-23:59:27.189978	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58121	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8650215 32829498 08/31/22-23:58:54.669703	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65021	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8583065 32829498 08/31/22-23:59:32.396919	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58306	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8641265 32026737 08/31/22-23:59:50.649034	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64126	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8586955 32026737 08/31/22-23:58:36.600606	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58695	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8614185 32829498 08/31/22-23:59:01.454658	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61418	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8655165 32026737 08/31/22-23:59:20.780161	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65516	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651115 32829498 08/31/22-23:58:33.379307	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65111	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8653885 32829498 08/31/22-23:59:40.874321	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65388	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8586945 32026737 08/31/22-23:58:36.580328	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58694	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8541555 32026737 08/31/22-23:59:42.262891	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54155	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8529575 32829498 08/31/22-23:58:07.312591	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52957	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8492045 32026737 08/31/22-23:59:56.342973	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49204	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8605865 32026737 08/31/22-23:58:15.043750	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60586	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8502315 32026737 09/01/22-00:00:07.455721	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50231	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8529595 32829498 08/31/22-23:58:07.365561	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52959	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8620545 32829498 08/31/22-23:58:21.744663	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62054	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8596415 32026737 08/31/22-23:58:24.944174	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	59641	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8596385 32026737 08/31/22-23:58:24.884406	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	59638	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651985 32026737 08/31/22-23:59:03.441447	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65198	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651095 32829498 08/31/22-23:58:33.338202	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65109	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8524575 32829498 09/01/22-00:00:11.310934	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52457	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8605875 32026737 08/31/22-23:58:15.064663	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60587	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534705 32026737 08/31/22-23:58:56.772805	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53470	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8566205 32026737 09/01/22-00:00:02.142088	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56620	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8586935 32026737 08/31/22-23:58:36.550637	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58693	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8586965 32026737 08/31/22-23:58:36.619047	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58696	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8569545 32026737 08/31/22-23:58:46.594398	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56954	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8492055 32026737 08/31/22-23:59:56.360951	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49205	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8566195 32026737 09/01/22-00:00:02.120945	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56619	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8519955 32829498 08/31/22-23:59:24.227191	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51995	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8614215 32829498 08/31/22-23:59:01.511754	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61421	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8529605 32829498 08/31/22-23:58:07.384051	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52960	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8653905 32829498 08/31/22-23:59:40.910653	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65390	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8530535 32829498 08/31/22-23:59:12.348894	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53053	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8541585 32026737 08/31/22-23:59:42.322126	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54158	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8607535 32829498 08/31/22-23:58:43.024087	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60753	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8573915 32829498 09/01/22-00:00:05.158775	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57391	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8583035 32829498 08/31/22-23:59:32.323930	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58303	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8605845 32026737 08/31/22-23:58:15.004694	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60584	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8581235 32026737 08/31/22-23:59:27.268863	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58123	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8600915 32026737 08/31/22-23:59:14.371988	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60091	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8652005 32026737 08/31/22-23:59:03.482704	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65200	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534335 32829498 08/31/22-23:59:18.325585	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53433	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8507875 32829498 08/31/22-23:59:48.189200	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50787	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8607515 32829498 08/31/22-23:58:42.984219	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60751	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8507865 32829498 08/31/22-23:59:48.168544	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50786	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534685 32026737 08/31/22-23:58:56.731128	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53468	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8492065 32026737 08/31/22-23:59:56.381031	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	49206	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8604755 32829498 08/31/22-23:59:59.877731	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60475	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8634485 32026737 08/31/22-23:59:36.563649	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63448	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8519975 32829498 08/31/22-23:59:24.265731	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51997	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8566185 32026737 09/01/22-00:00:02.100951	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56618	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534715 32026737 08/31/22-23:58:56.793274	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53471	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8530545 32829498 08/31/22-23:59:12.369224	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53054	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8524585 32829498 09/01/22-00:00:11.330853	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52458	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8655135 32026737 08/31/22-23:59:20.720500	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65513	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8608285 32829498 08/31/22-23:59:53.952246	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60828	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8641245 32026737 08/31/22-23:59:50.605079	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64124	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8620525 32829498 08/31/22-23:58:21.699516	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62052	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8573905 32829498 09/01/22-00:00:05.138814	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57390	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8502335 32026737 09/01/22-00:00:07.502496	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50233	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8600905 32026737 08/31/22-23:59:14.353291	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60090	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8524595 32829498 09/01/22-00:00:11.350932	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52459	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8608275 32829498 08/31/22-23:59:53.930680	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60827	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534695 32026737 08/31/22-23:58:56.749513	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	53469	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8502325 32026737 09/01/22-00:00:07.481526	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	50232	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8653875 32829498 08/31/22-23:59:40.854236	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65387	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8634515 32026737 08/31/22-23:59:36.620733	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63451	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8641255 32026737 08/31/22-23:59:50.625202	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64125	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8604765 32829498 08/31/22-23:59:59.898864	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60476	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8541575 32026737 08/31/22-23:59:42.301537	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	54157	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8573925 32829498 09/01/22-00:00:05.176878	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57392	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8524605 32829498 09/01/22-00:00:11.371195	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	52460	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8573895 32829498 09/01/22-00:00:05.118977	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	57389	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8560435 32829498 08/31/22-23:58:21.768917	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	56043	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8530525 32829498 08/31/22-23:59:12.328339	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53052	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8614195 32829498 08/31/22-23:59:01.474961	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	61419	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8519965 32829498 08/31/22-23:59:24.245596	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	51996	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8534325 32829498 08/31/22-23:59:18.305428	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	53432	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8605855 32026737 08/31/22-23:58:15.025136	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60585	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8634505 32026737 08/31/22-23:59:36.602428	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63450	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8604775 32829498 08/31/22-23:59:59.919053	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60477	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8569515 32026737 08/31/22-23:58:46.526858	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56951	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651125 32829498 08/31/22-23:58:33.402809	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65112	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8650205 32829498 08/31/22-23:58:54.651252	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	65020	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8634495 32026737 08/31/22-23:59:36.584182	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	63449	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8652015 32026737 08/31/22-23:59:03.503720	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65201	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8608305 32829498 08/31/22-23:59:53.997132	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60830	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8596405 32026737 08/31/22-23:58:24.925442	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	59640	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8641235 32026737 08/31/22-23:59:50.576561	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	64123	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8507885 32829498 08/31/22-23:59:48.220006	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	50788	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8600925 32026737 08/31/22-23:59:14.392903	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	60092	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8581245 32026737 08/31/22-23:59:27.287358	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	58124	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8651995 32026737 08/31/22-23:59:03.462712	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65199	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8596395 32026737 08/31/22-23:58:24.905091	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	59639	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8569535 32026737 08/31/22-23:58:46.573613	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56953	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8583045 32829498 08/31/22-23:59:32.344904	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	58304	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8607525 32829498 08/31/22-23:58:43.003278	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60752	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8655145 32026737 08/31/22-23:59:20.740564	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	65514	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8608295 32829498 08/31/22-23:59:53.975918	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	60829	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8620535 32829498 08/31/22-23:58:21.721380	UDP	2829498	ETPRO TROJAN GandCrab DNS Lookup 1	62053	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8566215 32026737 09/01/22-00:00:02.160962	UDP	2026737	ET TROJAN Observed GandCrab Domain (gandcrab .bit)	56621	53	192.168.2.3	8.8.8.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:58:02.760505915 CEST	49302	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:02.778575897 CEST	53	49302	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.036793947 CEST	53975	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.649065018 CEST	53	53975	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.671662092 CEST	53976	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.690844059 CEST	53	53976	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.692158937 CEST	53977	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.712151051 CEST	53	53977	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.718662977 CEST	53978	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.738368988 CEST	53	53978	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.739443064 CEST	53979	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.757306099 CEST	53	53979	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:04.757896900 CEST	53980	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:04.775638103 CEST	53	53980	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.165702105 CEST	52955	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:07.250682116 CEST	53	52955	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.294450998 CEST	52956	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:58:07.311570883 CEST	53	52956	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.312591076 CEST	52957	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:07.330202103 CEST	53	52957	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.331283092 CEST	52958	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:07.351011992 CEST	53	52958	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.365561008 CEST	52959	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:07.383272886 CEST	53	52959	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:07.384051085 CEST	52960	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:07.404005051 CEST	53	52960	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:13.881591082 CEST	60582	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:14.902959108 CEST	60582	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:14.937246084 CEST	53	60582	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:14.982489109 CEST	60583	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:15.000052929 CEST	53	60583	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:15.004693985 CEST	60584	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:15.024588108 CEST	53	60584	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:15.025135994 CEST	60585	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:15.043148041 CEST	53	60585	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:15.043750048 CEST	60586	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:15.064032078 CEST	53	60586	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:15.064662933 CEST	60587	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:15.082518101 CEST	53	60587	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:17.123805046 CEST	57134	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.161257982 CEST	57134	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.234639883 CEST	53	57134	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.235239029 CEST	53	57134	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.284126997 CEST	57135	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.303237915 CEST	53	57135	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.304316998 CEST	57136	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.324134111 CEST	53	57136	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.324816942 CEST	57137	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.344474077 CEST	53	57137	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.345424891 CEST	57138	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.363096952 CEST	53	57138	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.371185064 CEST	57139	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:18.391031981 CEST	53	57139	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:18.899728060 CEST	53	60582	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:20.518393040 CEST	62050	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.514583111 CEST	62050	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.646465063 CEST	53	62050	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.674954891 CEST	62051	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.675831079 CEST	53	62050	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.698769093 CEST	53	62051	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.699516058 CEST	62052	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.720890999 CEST	53	62052	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.721379995 CEST	62053	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.744118929 CEST	53	62053	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.744663000 CEST	62054	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.768213034 CEST	53	62054	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:21.768917084 CEST	56043	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:21.789768934 CEST	53	56043	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:23.738740921 CEST	59636	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.732259989 CEST	59636	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.804043055 CEST	53	59636	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:24.850137949 CEST	59637	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.869385004 CEST	53	59637	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:24.884406090 CEST	59638	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.904200077 CEST	53	59638	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:24.905091047 CEST	59639	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:58:24.924804926 CEST	53	59639	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:24.925441980 CEST	59640	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.943135023 CEST	53	59640	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:24.944174051 CEST	59641	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:24.964257956 CEST	53	59641	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.219465017 CEST	55638	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.255918026 CEST	53	55638	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.292717934 CEST	55639	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.311678886 CEST	53	55639	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.316054106 CEST	55640	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.336108923 CEST	53	55640	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.336745024 CEST	55641	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.355282068 CEST	53	55641	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.361900091 CEST	55642	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.381726027 CEST	53	55642	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:27.382469893 CEST	55643	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:27.402415991 CEST	53	55643	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:28.756191015 CEST	53	59636	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:32.660929918 CEST	60767	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.272780895 CEST	53	60767	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:33.320008993 CEST	65108	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.337179899 CEST	53	65108	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:33.338202000 CEST	65109	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.357716084 CEST	53	65109	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:33.358758926 CEST	65110	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.378457069 CEST	53	65110	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:33.379307032 CEST	65111	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.398911953 CEST	53	65111	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:33.402808905 CEST	65112	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:33.424699068 CEST	53	65112	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:35.661753893 CEST	58691	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.474462986 CEST	53	58691	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:36.532491922 CEST	58692	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.549562931 CEST	53	58692	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:36.550637007 CEST	58693	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.570236921 CEST	53	58693	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:36.580327988 CEST	58694	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.600003004 CEST	53	58694	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:36.600605965 CEST	58695	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.618398905 CEST	53	58695	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:36.619046926 CEST	58696	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:36.638629913 CEST	53	58696	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:38.594002962 CEST	53305	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.608630896 CEST	53305	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.644859076 CEST	53	53305	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:39.711462975 CEST	59434	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.735524893 CEST	53	59434	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:39.736547947 CEST	59435	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.759757996 CEST	53	59435	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:39.762542009 CEST	59436	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.798645973 CEST	53	59436	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:39.799617052 CEST	59437	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.823673964 CEST	53	59437	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:39.827074051 CEST	59438	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:39.854238987 CEST	53	59438	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:40.380073071 CEST	53	53305	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:41.899421930 CEST	60749	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:42.906723976 CEST	60749	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:42.943233967 CEST	53	60749	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:58:42.963799000 CEST	60750	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:42.983344078 CEST	53	60750	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:42.984219074 CEST	60751	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:43.002011061 CEST	53	60751	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:43.003278017 CEST	60752	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:43.023278952 CEST	53	60752	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:43.024086952 CEST	60753	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:43.043633938 CEST	53	60753	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:43.044194937 CEST	60754	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:43.062766075 CEST	53	60754	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:43.196578026 CEST	53	60749	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:45.860322952 CEST	56949	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.470341921 CEST	53	56949	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:46.506845951 CEST	56950	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.525938988 CEST	53	56950	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:46.526858091 CEST	56951	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.544490099 CEST	53	56951	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:46.555077076 CEST	56952	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.573009968 CEST	53	56952	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:46.573612928 CEST	56953	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.593744993 CEST	53	56953	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:46.594398022 CEST	56954	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:46.614161015 CEST	53	56954	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.439661980 CEST	53844	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.489172935 CEST	53	53844	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.509126902 CEST	53845	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.528167963 CEST	53	53845	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.529035091 CEST	53846	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.548969030 CEST	53	53846	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.552397013 CEST	53847	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.570151091 CEST	53	53847	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.570688963 CEST	53848	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.590229988 CEST	53	53848	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:52.590786934 CEST	53849	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:52.608671904 CEST	53	53849	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.559582949 CEST	65017	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.588342905 CEST	53	65017	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.611123085 CEST	65018	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.628262997 CEST	53	65018	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.630989075 CEST	65019	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.650563002 CEST	53	65019	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.651252031 CEST	65020	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.668998957 CEST	53	65020	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.669703007 CEST	65021	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.689425945 CEST	53	65021	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:54.690068007 CEST	65022	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:54.709500074 CEST	53	65022	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.637871027 CEST	53466	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.674391985 CEST	53	53466	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.711035013 CEST	53467	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.730349064 CEST	53	53467	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.731127977 CEST	53468	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.748970032 CEST	53	53468	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.749512911 CEST	53469	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.769344091 CEST	53	53469	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.772804976 CEST	53470	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.792510033 CEST	53	53470	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:56.793273926 CEST	53471	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:56.812910080 CEST	53	53471	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:58:59.232460976 CEST	53623	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.266350985 CEST	53	53623	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:59.292783976 CEST	53624	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.311882973 CEST	53	53624	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:59.312763929 CEST	53625	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.332475901 CEST	53	53625	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:59.338818073 CEST	53626	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.356389046 CEST	53	53626	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:59.357353926 CEST	53627	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.374880075 CEST	53	53627	8.8.8.8	192.168.2.3
Aug 31, 2022 23:58:59.376303911 CEST	53628	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:58:59.394289017 CEST	53	53628	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.363595963 CEST	61416	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.399610996 CEST	53	61416	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.436424971 CEST	61417	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.453686953 CEST	53	61417	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.454658031 CEST	61418	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.474419117 CEST	53	61418	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.474961042 CEST	61419	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.492651939 CEST	53	61419	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.493232965 CEST	61420	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.511037111 CEST	53	61420	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:01.511754036 CEST	61421	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:01.529551029 CEST	53	61421	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.366775036 CEST	65196	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.405114889 CEST	53	65196	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.423759937 CEST	65197	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.440768003 CEST	53	65197	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.441447020 CEST	65198	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.461023092 CEST	53	65198	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.462712049 CEST	65199	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.482172012 CEST	53	65199	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.482703924 CEST	65200	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.502460003 CEST	53	65200	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:03.503720045 CEST	65201	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:03.521188974 CEST	53	65201	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:05.917948008 CEST	58708	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.501457930 CEST	53	58708	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:06.518330097 CEST	58709	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.537347078 CEST	53	58709	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:06.541033030 CEST	58710	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.560595989 CEST	53	58710	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:06.561108112 CEST	58711	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.581572056 CEST	53	58711	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:06.582118988 CEST	58712	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.599746943 CEST	53	58712	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:06.600199938 CEST	58713	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:06.617580891 CEST	53	58713	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:11.520944118 CEST	53049	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:12.252245903 CEST	53	53049	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:12.277647972 CEST	53050	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:12.296758890 CEST	53	53050	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:12.297575951 CEST	53051	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:12.317811966 CEST	53	53051	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:12.328339100 CEST	53052	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:12.348246098 CEST	53	53052	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:12.348893881 CEST	53053	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:12.368700981 CEST	53	53053	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:12.369224072 CEST	53054	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:59:12.389571905 CEST	53	53054	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.234563112 CEST	60088	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.311661005 CEST	53	60088	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.331684113 CEST	60089	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.352329969 CEST	53	60089	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.353291035 CEST	60090	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.371464014 CEST	53	60090	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.371988058 CEST	60091	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.392226934 CEST	53	60091	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.392903090 CEST	60092	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.412553072 CEST	53	60092	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:14.413882971 CEST	60093	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:14.435400963 CEST	53	60093	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.707844973 CEST	63562	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.756638050 CEST	53	63562	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.767276049 CEST	63563	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.786377907 CEST	53	63563	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.789041996 CEST	63564	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.808978081 CEST	53	63564	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.809427023 CEST	63565	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.827245951 CEST	53	63565	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.838541031 CEST	63566	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.856257915 CEST	53	63566	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:15.856786013 CEST	63567	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:15.874497890 CEST	53	63567	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:17.091232061 CEST	53428	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.080478907 CEST	53428	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.240111113 CEST	53	53428	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.249520063 CEST	53429	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.268676043 CEST	53	53429	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.269253969 CEST	53430	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.286752939 CEST	53	53430	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.287184954 CEST	53431	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.304971933 CEST	53	53431	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.305428028 CEST	53432	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.325037003 CEST	53	53432	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.325584888 CEST	53433	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:18.345073938 CEST	53	53433	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:18.697067022 CEST	53	53428	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:19.656590939 CEST	65511	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.653614998 CEST	65511	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.690124035 CEST	53	65511	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.699863911 CEST	65512	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.719475031 CEST	53	65512	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.720499992 CEST	65513	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.740108013 CEST	53	65513	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.740564108 CEST	65514	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.757486105 CEST	53	65511	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.760489941 CEST	53	65514	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.761806011 CEST	65515	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.779664040 CEST	53	65515	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:20.780160904 CEST	65516	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:20.799532890 CEST	53	65516	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:22.015532970 CEST	59820	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.145498037 CEST	53	59820	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:22.154289007 CEST	59821	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.173274994 CEST	53	59821	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:22.173866034 CEST	59822	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.191287994 CEST	53	59822	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:59:22.195880890 CEST	59823	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.215575933 CEST	53	59823	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:22.215950966 CEST	59824	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.235313892 CEST	53	59824	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:22.235685110 CEST	59825	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:22.255491972 CEST	53	59825	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:23.593552113 CEST	64823	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.179404020 CEST	53	64823	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:24.188785076 CEST	51993	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.206090927 CEST	53	51993	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:24.206868887 CEST	51994	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.226692915 CEST	53	51994	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:24.227190971 CEST	51995	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.245124102 CEST	53	51995	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:24.245595932 CEST	51996	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.265338898 CEST	53	51996	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:24.265731096 CEST	51997	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:24.285284042 CEST	53	51997	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:25.542416096 CEST	58119	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:26.630718946 CEST	58119	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.165951967 CEST	53	58119	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.172085047 CEST	58120	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.189124107 CEST	53	58120	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.189977884 CEST	58121	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.209870100 CEST	53	58121	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.247838974 CEST	58122	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.267399073 CEST	53	58122	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.268862963 CEST	58123	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.286777020 CEST	53	58123	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.287358046 CEST	58124	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:27.307277918 CEST	53	58124	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:27.705112934 CEST	53	58119	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:28.925348043 CEST	49166	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.260584116 CEST	49166	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.836324930 CEST	53	49166	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:30.844980955 CEST	49167	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.862699986 CEST	53	49167	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:30.866137028 CEST	49168	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.884212971 CEST	53	49168	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:30.884764910 CEST	49169	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.904670000 CEST	53	49169	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:30.905071974 CEST	49170	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.922668934 CEST	53	49170	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:30.923072100 CEST	49171	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:30.942532063 CEST	53	49171	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.146146059 CEST	53	49166	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.225573063 CEST	58301	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.299428940 CEST	53	58301	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.305984020 CEST	58302	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.323093891 CEST	53	58302	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.323930025 CEST	58303	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.343451023 CEST	53	58303	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.344903946 CEST	58304	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.364872932 CEST	53	58304	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.365597963 CEST	58305	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.385454893 CEST	53	58305	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:32.396919012 CEST	58306	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:32.415087938 CEST	53	58306	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:33.635987043 CEST	63446	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:59:34.632500887 CEST	63446	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:35.644903898 CEST	63446	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.530746937 CEST	53	63446	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.543714046 CEST	63447	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.563038111 CEST	53	63447	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.563648939 CEST	63448	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.583677053 CEST	53	63448	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.584182024 CEST	63449	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.602057934 CEST	53	63449	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.602427959 CEST	63450	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.620131016 CEST	53	63450	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.620733023 CEST	63451	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:36.640644073 CEST	53	63451	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:36.792453051 CEST	53	63446	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:37.851984024 CEST	49874	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:38.863599062 CEST	49874	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.088445902 CEST	53	63446	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.439719915 CEST	53	49874	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.448174953 CEST	49875	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.465456009 CEST	53	49875	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.465929985 CEST	49876	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.483722925 CEST	53	49876	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.484544992 CEST	49877	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.503002882 CEST	53	49877	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.503390074 CEST	49878	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.521054029 CEST	53	49878	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.521467924 CEST	49879	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:39.540900946 CEST	53	49879	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:39.567404985 CEST	53	49874	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.790900946 CEST	65385	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.827275038 CEST	53	65385	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.836529016 CEST	65386	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.853662968 CEST	53	65386	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.854235888 CEST	65387	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.873889923 CEST	53	65387	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.874320984 CEST	65388	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.891818047 CEST	53	65388	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.892307043 CEST	65389	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.909749031 CEST	53	65389	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:40.910653114 CEST	65390	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:40.930310965 CEST	53	65390	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.179858923 CEST	54153	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.224383116 CEST	53	54153	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.235496044 CEST	54154	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.254621983 CEST	53	54154	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.262891054 CEST	54155	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.280628920 CEST	53	54155	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.281209946 CEST	54156	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.301055908 CEST	53	54156	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.301537037 CEST	54157	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.321456909 CEST	53	54157	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:42.322125912 CEST	54158	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:42.341794014 CEST	53	54158	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:43.590250015 CEST	64602	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:44.583146095 CEST	64602	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.599035978 CEST	64602	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.634243011 CEST	53	64602	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:45.651026011 CEST	64603	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.670564890 CEST	53	64603	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:59:45.671057940 CEST	64604	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.691019058 CEST	53	64604	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:45.691448927 CEST	64605	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.711270094 CEST	53	64605	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:45.711695910 CEST	64606	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.729429960 CEST	53	64606	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:45.737027884 CEST	64607	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:45.756819010 CEST	53	64607	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:45.793020010 CEST	53	64602	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:46.698057890 CEST	53	64602	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:47.058562040 CEST	50784	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.075234890 CEST	50784	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.139800072 CEST	53	50784	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.150029898 CEST	50785	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.167660952 CEST	53	50785	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.168544054 CEST	50786	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.188586950 CEST	53	50786	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.189199924 CEST	50787	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.209095001 CEST	53	50787	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.220005989 CEST	50788	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.238341093 CEST	53	50788	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.239259958 CEST	50789	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:48.259392023 CEST	53	50789	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:48.697335958 CEST	53	50784	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:49.506455898 CEST	64121	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.521322966 CEST	64121	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.544496059 CEST	53	64121	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.556144953 CEST	64122	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.575448990 CEST	53	64122	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.576560974 CEST	64123	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.592947006 CEST	53	64121	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.596391916 CEST	53	64123	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.605078936 CEST	64124	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.624696016 CEST	53	64124	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.625201941 CEST	64125	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.648333073 CEST	53	64125	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:50.649034023 CEST	64126	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:50.668668032 CEST	53	64126	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:51.926340103 CEST	64967	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:51.954930067 CEST	53	64967	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:51.969147921 CEST	64968	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:51.988468885 CEST	53	64968	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:51.989362001 CEST	64969	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:52.008342981 CEST	53	64969	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:52.023263931 CEST	64970	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:52.042766094 CEST	53	64970	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:52.043279886 CEST	64971	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:52.062791109 CEST	53	64971	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:52.063211918 CEST	64972	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:52.083273888 CEST	53	64972	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.315284014 CEST	60825	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:53.888886929 CEST	53	60825	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.910933018 CEST	60826	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:53.930005074 CEST	53	60826	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.930680037 CEST	60827	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:53.951704979 CEST	53	60827	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.952245951 CEST	60828	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:53.972112894 CEST	53	60828	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.975918055 CEST	60829	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:59:53.996426105 CEST	53	60829	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:53.997132063 CEST	60830	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:54.017124891 CEST	53	60830	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:55.249011993 CEST	49201	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.259572983 CEST	49201	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.294773102 CEST	53	49201	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.303123951 CEST	49202	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.322354078 CEST	53	49202	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.322889090 CEST	49203	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.342601061 CEST	53	49203	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.342972994 CEST	49204	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.360450983 CEST	53	49204	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.360950947 CEST	49205	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.380527020 CEST	53	49205	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.381031036 CEST	49206	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:56.400538921 CEST	53	49206	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:56.951119900 CEST	53	49201	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.561789036 CEST	64936	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.635045052 CEST	53	64936	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.647419930 CEST	64937	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.666646004 CEST	53	64937	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.667177916 CEST	64938	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.687072039 CEST	53	64938	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.687539101 CEST	64939	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.705380917 CEST	53	64939	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.705862045 CEST	64940	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.725605011 CEST	53	64940	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:57.726016045 CEST	64941	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:57.745647907 CEST	53	64941	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:58.812098026 CEST	60473	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.818274021 CEST	60473	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.852207899 CEST	53	60473	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:59.859764099 CEST	60474	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.877156019 CEST	53	60474	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:59.877731085 CEST	60475	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.898338079 CEST	53	60475	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:59.898864031 CEST	60476	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.918551922 CEST	53	60476	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:59.919053078 CEST	60477	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.938997030 CEST	53	60477	8.8.8.8	192.168.2.3
Aug 31, 2022 23:59:59.939438105 CEST	60478	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:59:59.959988117 CEST	53	60478	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:01.037652969 CEST	59374	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.037312031 CEST	59374	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.071805954 CEST	53	59374	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.080656052 CEST	56617	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.100327969 CEST	53	56617	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.100950956 CEST	56618	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.120507956 CEST	53	56618	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.120944977 CEST	56619	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.141537905 CEST	53	56619	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.142087936 CEST	56620	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.160455942 CEST	53	56620	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.160962105 CEST	56621	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:02.179536104 CEST	53	56621	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:02.700483084 CEST	53	59374	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.267693043 CEST	61184	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:03.343596935 CEST	53	61184	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.353477001 CEST	61185	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:00:03.370637894 CEST	53	61185	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.371157885 CEST	61186	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:03.390731096 CEST	53	61186	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.391253948 CEST	61187	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:03.410953045 CEST	53	61187	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.411292076 CEST	61188	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:03.430705070 CEST	53	61188	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.431119919 CEST	61189	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:03.450587988 CEST	53	61189	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:03.829907894 CEST	53	60473	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:04.517784119 CEST	57387	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.091319084 CEST	53	57387	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:05.099412918 CEST	57388	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.118396044 CEST	53	57388	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:05.118977070 CEST	57389	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.138398886 CEST	53	57389	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:05.138813972 CEST	57390	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.158288956 CEST	53	57390	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:05.158775091 CEST	57391	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.176443100 CEST	53	57391	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:05.176877975 CEST	57392	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:05.194662094 CEST	53	57392	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:06.266103029 CEST	50228	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.256401062 CEST	50228	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.399528980 CEST	53	50228	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.412708044 CEST	50229	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.432984114 CEST	53	50229	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.433896065 CEST	50230	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.454828024 CEST	53	50230	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.455720901 CEST	50231	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.479063988 CEST	53	50231	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.481525898 CEST	50232	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.501718998 CEST	53	50232	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.502496004 CEST	50233	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:07.524806976 CEST	53	50233	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:07.918035030 CEST	53	50228	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:08.675157070 CEST	53269	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.687948942 CEST	53269	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.840522051 CEST	53	53269	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:09.849908113 CEST	53270	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.867008924 CEST	53	53270	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:09.867791891 CEST	53271	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.887459040 CEST	53	53271	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:09.889720917 CEST	59828	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.910227060 CEST	53	59828	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:09.911396027 CEST	59829	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.933176994 CEST	53	59829	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:09.936009884 CEST	59830	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:09.956068039 CEST	53	59830	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.257081985 CEST	51105	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:11.285418034 CEST	53	51105	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.291388988 CEST	52456	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:11.304387093 CEST	53	53269	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.310426950 CEST	53	52456	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.310934067 CEST	52457	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:11.330421925 CEST	53	52457	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.330852985 CEST	52458	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:11.350558043 CEST	53	52458	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.350931883 CEST	52459	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:00:11.370852947 CEST	53	52459	8.8.8.8	192.168.2.3
Sep 1, 2022 00:00:11.371195078 CEST	52460	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:00:11.388839006 CEST	53	52460	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 31, 2022 23:58:18.899866104 CEST	192.168.2.3	8.8.8.8	cff3	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:58:21.675904036 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:58:28.756336927 CEST	192.168.2.3	8.8.8.8	cff3	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:58:40.380204916 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:58:43.196728945 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:18.697181940 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:20.757663965 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:27.705205917 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:32.146743059 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:36.792562962 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:39.088548899 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:45.793106079 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:46.698131084 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:48.699120045 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:50.593031883 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Aug 31, 2022 23:59:56.952230930 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:00:02.702019930 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:00:03.830478907 CEST	192.168.2.3	8.8.8.8	cff3	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:00:07.922203064 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable
Sep 1, 2022 00:00:11.304521084 CEST	192.168.2.3	8.8.8.8	d030	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:58:02.760505915 CEST	192.168.2.3	8.8.8.8	0xfb1f	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.036793947 CEST	192.168.2.3	8.8.8.8	0x837d	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.671662092 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:04.692158937 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.718662977 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:58:04.739443064 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.757896900 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:58:07.165702105 CEST	192.168.2.3	8.8.8.8	0xc956	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.294450998 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:58:07.312591076 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.331283092 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:07.365561008 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.384051085 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:13.881591082 CEST	192.168.2.3	8.8.8.8	0x17	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:14.902959108 CEST	192.168.2.3	8.8.8.8	0x17	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:14.982489109 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:15.004693985 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:15.025135994 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:15.043750048 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:15.064662933 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:17.123805046 CEST	192.168.2.3	8.8.8.8	0xbb4f	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.161257982 CEST	192.168.2.3	8.8.8.8	0xbb4f	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.284126997 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:18.304316998 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.324816942 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:18.345424891 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.371185064 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:20.518393040 CEST	192.168.2.3	8.8.8.8	0xccdb	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.514583111 CEST	192.168.2.3	8.8.8.8	0xccdb	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.674954891 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:21.699516058 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.721379995 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:21.744663000 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.768917084 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:23.738740921 CEST	192.168.2.3	8.8.8.8	0xea6e	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.732259989 CEST	192.168.2.3	8.8.8.8	0xea6e	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.850137949 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:24.884406090 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.905091047 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:24.925441980 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.944174051 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:27.219465017 CEST	192.168.2.3	8.8.8.8	0xa774	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:27.292717934 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:27.316054106 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:58:27.336745024 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:27.361900091 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:27.382469893 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:32.660929918 CEST	192.168.2.3	8.8.8.8	0xaf62	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.320008993 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:33.338202000 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.358758926 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:33.379307032 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.402808905 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:35.661753893 CEST	192.168.2.3	8.8.8.8	0xd7cb	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.532491922 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:36.550637007 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.580327988 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:36.600605965 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.619046926 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:38.594002962 CEST	192.168.2.3	8.8.8.8	0x3115	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.608630896 CEST	192.168.2.3	8.8.8.8	0x3115	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.711462975 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:39.736547947 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.762542009 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:39.799617052 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.827074051 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:41.899421930 CEST	192.168.2.3	8.8.8.8	0x4b60	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:42.906723976 CEST	192.168.2.3	8.8.8.8	0x4b60	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:42.963799000 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:42.984219074 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:43.003278017 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:43.024086952 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:43.044194937 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:45.860322952 CEST	192.168.2.3	8.8.8.8	0xc71c	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.506845951 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:46.526858091 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.555077076 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:46.573612928 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.594398022 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:58:52.439661980 CEST	192.168.2.3	8.8.8.8	0x4a62	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.509126902 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:52.529035091 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.552397013 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:52.570688963 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.590786934 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:54.559582949 CEST	192.168.2.3	8.8.8.8	0xcea6	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:54.611123085 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:54.630989075 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:54.651252031 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:54.669703007 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:54.690068007 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:58:56.637871027 CEST	192.168.2.3	8.8.8.8	0x98da	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.711035013 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:56.731127977 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.749512911 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:56.772804976 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.793273926 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:58:59.232460976 CEST	192.168.2.3	8.8.8.8	0xbf18	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.292783976 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:59.312763929 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.338818073 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:58:59.357353926 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.376303911 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:01.363595963 CEST	192.168.2.3	8.8.8.8	0x33a6	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.436424971 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:01.454658031 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.474961042 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:01.493232965 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.511754036 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:03.366775036 CEST	192.168.2.3	8.8.8.8	0x4894	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:03.423759937 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:03.441447020 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:03.462712049 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:03.482703924 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:59:03.503720045 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:05.917948008 CEST	192.168.2.3	8.8.8.8	0x428c	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.518330097 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:06.541033030 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.561108112 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:06.582118988 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.600199938 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:11.520944118 CEST	192.168.2.3	8.8.8.8	0xf42e	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.277647972 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:12.297575951 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.328339100 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:12.348893881 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.369224072 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:14.234563112 CEST	192.168.2.3	8.8.8.8	0x4340	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.331684113 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:14.353291035 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.371988058 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:14.392903090 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.413882971 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:15.707844973 CEST	192.168.2.3	8.8.8.8	0xca4b	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.767276049 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:15.789041996 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.809427023 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:15.838541031 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.856786013 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:17.091232061 CEST	192.168.2.3	8.8.8.8	0x160b	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.080478907 CEST	192.168.2.3	8.8.8.8	0x160b	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.249520063 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:18.269253969 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.287184954 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:18.305428028 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.325584888 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:19.656590939 CEST	192.168.2.3	8.8.8.8	0x9891	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.653614998 CEST	192.168.2.3	8.8.8.8	0x9891	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.699863911 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:59:20.720499992 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.740564108 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:20.761806011 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.780160904 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:22.015532970 CEST	192.168.2.3	8.8.8.8	0xc448	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:22.154289007 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:22.173866034 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:22.195880890 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:22.215950966 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:22.235685110 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:23.593552113 CEST	192.168.2.3	8.8.8.8	0x9641	Standard query (0)	dns1.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.188785076 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:24.206868887 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.227190971 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:24.245595932 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.265731096 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:25.542416096 CEST	192.168.2.3	8.8.8.8	0x72c8	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:26.630718946 CEST	192.168.2.3	8.8.8.8	0x72c8	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.172085047 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:27.189977884 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.247838974 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:27.268862963 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.287358046 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:28.925348043 CEST	192.168.2.3	8.8.8.8	0xbe66	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.260584116 CEST	192.168.2.3	8.8.8.8	0xbe66	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.844980955 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:30.866137028 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.884764910 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:30.905071974 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.923072100 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomoreransom.coin	28	IN (0x0001)
Aug 31, 2022 23:59:32.225573063 CEST	192.168.2.3	8.8.8.8	0xc8b1	Standard query (0)	dns2.soprodns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.305984020 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:32.323930025 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.344903946 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomoreransom.bit	28	IN (0x0001)
Aug 31, 2022 23:59:32.365597963 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomoreransom.bit	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:59:32.396919012 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:33.635987043 CEST	192.168.2.3	8.8.8.8	0x6b6b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:34.632500887 CEST	192.168.2.3	8.8.8.8	0x6b6b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:35.644903898 CEST	192.168.2.3	8.8.8.8	0x6b6b	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.543714046 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:36.563648939 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.584182024 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:36.602427959 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.620733023 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:37.851984024 CEST	192.168.2.3	8.8.8.8	0xbe0f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:38.863599062 CEST	192.168.2.3	8.8.8.8	0xbe0f	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.448174953 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:39.465929985 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.484544992 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:39.503390074 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.521467924 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:40.790900946 CEST	192.168.2.3	8.8.8.8	0x3976	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.836529016 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:40.854235888 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.874320984 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:40.892307043 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.910653114 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:42.179858923 CEST	192.168.2.3	8.8.8.8	0x94a7	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.235496044 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:42.262891054 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.281209946 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:42.301537037 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.322125912 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:43.590250015 CEST	192.168.2.3	8.8.8.8	0x70ae	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:44.583146095 CEST	192.168.2.3	8.8.8.8	0x70ae	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.599035978 CEST	192.168.2.3	8.8.8.8	0x70ae	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.651026011 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:45.671057940 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.691448927 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:45.711695910 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:59:45.737027884 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:47.058562040 CEST	192.168.2.3	8.8.8.8	0xed4	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.075234890 CEST	192.168.2.3	8.8.8.8	0xed4	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.150029898 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:48.168544054 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.189199924 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:48.220005989 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.239259958 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:49.506455898 CEST	192.168.2.3	8.8.8.8	0xae84	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.521322966 CEST	192.168.2.3	8.8.8.8	0xae84	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.556144953 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:50.576560974 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.605078936 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:50.625201941 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.649034023 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:51.926340103 CEST	192.168.2.3	8.8.8.8	0x4be7	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:51.969147921 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:51.989362001 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:52.023263931 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:52.043279886 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:52.063211918 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:53.315284014 CEST	192.168.2.3	8.8.8.8	0x8b86	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:53.910933018 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:53.930680037 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:53.952245951 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:53.975918055 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:53.997132063 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:55.249011993 CEST	192.168.2.3	8.8.8.8	0x1e6d	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.259572983 CEST	192.168.2.3	8.8.8.8	0x1e6d	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.303123951 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:56.322889090 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.342972994 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:56.360950947 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.381031036 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Aug 31, 2022 23:59:57.561789036 CEST	192.168.2.3	8.8.8.8	0x2252	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:59:57.647419930 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:57.667177916 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.687539101 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:57.705862045 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.726016045 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Aug 31, 2022 23:59:58.812098026 CEST	192.168.2.3	8.8.8.8	0x82c8	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.818274021 CEST	192.168.2.3	8.8.8.8	0x82c8	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.859764099 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:59.877731085 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.898864031 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Aug 31, 2022 23:59:59.919053078 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.939438105 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:00:01.037652969 CEST	192.168.2.3	8.8.8.8	0xb09	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.037312031 CEST	192.168.2.3	8.8.8.8	0xb09	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.080656052 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:02.100950956 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.120944977 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:00:02.142087936 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.160962105 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:00:03.267693043 CEST	192.168.2.3	8.8.8.8	0xa990	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.353477001 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:03.371157885 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.391253948 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Sep 1, 2022 00:00:03.411292076 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.431119919 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Sep 1, 2022 00:00:04.517784119 CEST	192.168.2.3	8.8.8.8	0x31a	Standard query (0)	dns1.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.099412918 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:05.118977070 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.138813972 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:00:05.158775091 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.176877975 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:00:06.266103029 CEST	192.168.2.3	8.8.8.8	0xd96a	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.256401062 CEST	192.168.2.3	8.8.8.8	0xd96a	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.412708044 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:07.433896065 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:00:07.455720901 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:00:07.481525898 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	gandcrab.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.502496004 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	gandcrab.bit	28	IN (0x0001)
Sep 1, 2022 00:00:08.675157070 CEST	192.168.2.3	8.8.8.8	0xa920	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.687948942 CEST	192.168.2.3	8.8.8.8	0xa920	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.849908113 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:09.867791891 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.889720917 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Sep 1, 2022 00:00:09.911396027 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.coin	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.936009884 CEST	192.168.2.3	8.8.8.8	0x5	Standard query (0)	nomorerans om.coin	28	IN (0x0001)
Sep 1, 2022 00:00:11.257081985 CEST	192.168.2.3	8.8.8.8	0xa868	Standard query (0)	dns2.sopro dns.ru	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.291388988 CEST	192.168.2.3	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:11.310934067 CEST	192.168.2.3	8.8.8.8	0x2	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.330852985 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	nomorerans om.bit	28	IN (0x0001)
Sep 1, 2022 00:00:11.350931883 CEST	192.168.2.3	8.8.8.8	0x4	Standard query (0)	nomorerans om.bit	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.371195078 CEST	192.168.2.3	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
Aug 31, 2022 23:58:04.649065018 CEST	8.8.8.8	192.168.2.3	0x837d	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.690844059 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:04.712151051 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.738368988 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:04.757306099 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:04.775638103 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:07.250682116 CEST	8.8.8.8	192.168.2.3	0xc956	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.311570883 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:07.330202103 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.351011992 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:07.383272886 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:07.404005051 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:14.937246084 CEST	8.8.8.8	192.168.2.3	0x17	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:15.000052929 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:15.024588108 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:15.043148041 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:15.064032078 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:58:15.082518101 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:18.234639883 CEST	8.8.8.8	192.168.2.3	0xbb4f	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.235239029 CEST	8.8.8.8	192.168.2.3	0xbb4f	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.303237915 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:18.324134111 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.344474077 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:18.363096952 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:18.391031981 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:18.899728060 CEST	8.8.8.8	192.168.2.3	0x17	Server failure (2)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.646465063 CEST	8.8.8.8	192.168.2.3	0xccdb	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.675831079 CEST	8.8.8.8	192.168.2.3	0xccdb	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.698769093 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:21.720890999 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.744118929 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:21.768213034 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:21.789768934 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:24.804043055 CEST	8.8.8.8	192.168.2.3	0xea6e	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.869385004 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:24.904200077 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.924804926 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:24.943135023 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:24.964257956 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:27.255918026 CEST	8.8.8.8	192.168.2.3	0xa774	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:27.311678886 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:27.336108923 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:27.355282068 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:27.381726027 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:27.402415991 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:28.756191015 CEST	8.8.8.8	192.168.2.3	0xea6e	Server failure (2)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.272780895 CEST	8.8.8.8	192.168.2.3	0xaf62	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.337179899 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:33.357716084 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.378457069 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:33.398911953 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:33.424699068 CEST	8.8.8.8	192.168.2.3	0x5	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
Aug 31, 2022 23:58:36.474462986 CEST	8.8.8.8	192.168.2.3	0xd7cb	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.549562931 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:36.570236921 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.600003004 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:36.618398905 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:36.638629913 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:39.644859076 CEST	8.8.8.8	192.168.2.3	0x3115	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.735524893 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:39.759757996 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.798645973 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:39.823673964 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:39.854238987 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:40.380073071 CEST	8.8.8.8	192.168.2.3	0x3115	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:42.943233967 CEST	8.8.8.8	192.168.2.3	0x4b60	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:42.983344078 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:43.002011061 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:43.023278952 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:43.043633938 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:43.062766075 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:43.196578026 CEST	8.8.8.8	192.168.2.3	0x4b60	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.470341921 CEST	8.8.8.8	192.168.2.3	0xc71c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.525938988 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:46.544490099 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.573009968 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:46.593744993 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.614161015 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:52.489172935 CEST	8.8.8.8	192.168.2.3	0x4a62	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.528167963 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:52.548969030 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.570151091 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:52.590229988 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:52.608671904 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:54.588342905 CEST	8.8.8.8	192.168.2.3	0xcea6	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:54.628262997 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:54.650563002 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:58:54.668998957 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:54.689425945 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:54.709500074 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:56.674391985 CEST	8.8.8.8	192.168.2.3	0x98da	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.730349064 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:56.748970032 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.769344091 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:56.792510033 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:56.812910080 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:59.266350985 CEST	8.8.8.8	192.168.2.3	0xbf18	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.311882973 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:58:59.332475901 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.356389046 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:58:59.374880075 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:59.394289017 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:01.399610996 CEST	8.8.8.8	192.168.2.3	0x33a6	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.453686953 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:01.474419117 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.492651939 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:01.511037111 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:01.529551029 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:03.405114889 CEST	8.8.8.8	192.168.2.3	0x4894	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:03.440768003 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:03.461023092 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:03.482172012 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:03.502460003 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:03.521188974 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:06.501457930 CEST	8.8.8.8	192.168.2.3	0x428c	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.537347078 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:06.560595989 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.581572056 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:06.599746943 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:06.617580891 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:12.252245903 CEST	8.8.8.8	192.168.2.3	0xf42e	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.296758890 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:59:12.317811966 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.348246098 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:12.368700981 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:12.389571905 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:14.311661005 CEST	8.8.8.8	192.168.2.3	0x4340	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.352329969 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:14.371464014 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.392226934 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:14.412553072 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:14.435400963 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:15.756638050 CEST	8.8.8.8	192.168.2.3	0xca4b	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.786377907 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:15.808978081 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.827245951 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:15.856257915 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:15.874497890 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:18.240111113 CEST	8.8.8.8	192.168.2.3	0x160b	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.268676043 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:18.286752939 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.304971933 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:18.325037003 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:18.345073938 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:18.697067022 CEST	8.8.8.8	192.168.2.3	0x160b	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.690124035 CEST	8.8.8.8	192.168.2.3	0x9891	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.719475031 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:20.740108013 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.757486105 CEST	8.8.8.8	192.168.2.3	0x9891	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.760489941 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:20.779664040 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:20.799532890 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:22.145498037 CEST	8.8.8.8	192.168.2.3	0xc448	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:22.173274994 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:22.191287994 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:22.215575933 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:22.235313892 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:59:22.255491972 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:24.179404020 CEST	8.8.8.8	192.168.2.3	0x9641	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.206090927 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:24.226692915 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.245124102 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:24.265338898 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:24.285284042 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:27.165951967 CEST	8.8.8.8	192.168.2.3	0x72c8	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.189124107 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:27.209870100 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.267399073 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:27.286777020 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:27.307277918 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:27.705112934 CEST	8.8.8.8	192.168.2.3	0x72c8	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.836324930 CEST	8.8.8.8	192.168.2.3	0xbe66	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.862699986 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:30.884212971 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.904670000 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:30.922668934 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:30.942532063 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:32.146146059 CEST	8.8.8.8	192.168.2.3	0xbe66	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.299428940 CEST	8.8.8.8	192.168.2.3	0xc8b1	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.323093891 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:32.343451023 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.364872932 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:32.385454893 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:32.415087938 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:36.530746937 CEST	8.8.8.8	192.168.2.3	0x6b6b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.563038111 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:36.583677053 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.602057934 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:36.620131016 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:36.640644073 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:36.792453051 CEST	8.8.8.8	192.168.2.3	0x6b6b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.088445902 CEST	8.8.8.8	192.168.2.3	0x6b6b	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:59:39.439719915 CEST	8.8.8.8	192.168.2.3	0xbe0f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.465456009 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:39.483722925 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.503002882 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:39.521054029 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:39.540900946 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:39.567404985 CEST	8.8.8.8	192.168.2.3	0xbe0f	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.827275038 CEST	8.8.8.8	192.168.2.3	0x3976	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.853662968 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:40.873889923 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.891818047 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:40.909749031 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:40.930310965 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:42.224383116 CEST	8.8.8.8	192.168.2.3	0x94a7	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.254621983 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:42.280628920 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.301055908 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:42.321456909 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:42.341794014 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:45.634243011 CEST	8.8.8.8	192.168.2.3	0x70ae	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.670564890 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:45.691019058 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.711270094 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:45.729429960 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:45.756819010 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:45.793020010 CEST	8.8.8.8	192.168.2.3	0x70ae	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:46.698057890 CEST	8.8.8.8	192.168.2.3	0x70ae	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.139800072 CEST	8.8.8.8	192.168.2.3	0xed4	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.167660952 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:48.188586950 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.209095001 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:48.238341093 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:48.259392023 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:48.697335958 CEST	8.8.8.8	192.168.2.3	0xed4	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.544496059 CEST	8.8.8.8	192.168.2.3	0xae84	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)

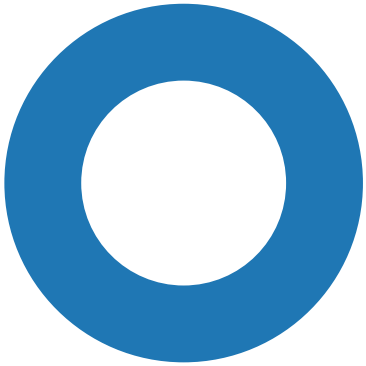
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:59:50.575448990 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:50.592947006 CEST	8.8.8.8	192.168.2.3	0xae84	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.596391916 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.624696016 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:50.648333073 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:50.668668032 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:51.954930067 CEST	8.8.8.8	192.168.2.3	0x4be7	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:51.988468885 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:52.008342981 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomoreransom.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:52.042766094 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomoreransom.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:52.062791109 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomoreransom.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:52.083273888 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomoreransom.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:53.888886929 CEST	8.8.8.8	192.168.2.3	0x8b86	Name error (3)	dns1.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:53.930005074 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:53.951704979 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:53.972112894 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:53.996426105 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:54.017124891 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:56.294773102 CEST	8.8.8.8	192.168.2.3	0x1e6d	Name error (3)	dns2.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.322354078 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:56.342601061 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.360450983 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:56.380527020 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:56.400538921 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:56.951119900 CEST	8.8.8.8	192.168.2.3	0x1e6d	Name error (3)	dns2.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.635045052 CEST	8.8.8.8	192.168.2.3	0x2252	Name error (3)	dns2.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.666646004 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:57.687072039 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomoreransom.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.705380917 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomoreransom.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:57.725605011 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomoreransom.coin	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.745647907 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomoreransom.coin	none	none	28	IN (0x0001)
Aug 31, 2022 23:59:59.852207899 CEST	8.8.8.8	192.168.2.3	0x82c8	Name error (3)	dns2.soprodns.ru	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.877156019 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Aug 31, 2022 23:59:59.898338079 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomoreransom.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.918551922 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomoreransom.bit	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:59:59.938997030 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:59.959988117 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:02.071805954 CEST	8.8.8.8	192.168.2.3	0xb09	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.100327969 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:02.120507956 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.141537905 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:02.160455942 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:02.179536104 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:02.700483084 CEST	8.8.8.8	192.168.2.3	0xb09	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.343596935 CEST	8.8.8.8	192.168.2.3	0xa990	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.370637894 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:03.390731096 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.410953045 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:03.430705070 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:03.450587988 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:03.829907894 CEST	8.8.8.8	192.168.2.3	0x82c8	Server failure (2)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.091319084 CEST	8.8.8.8	192.168.2.3	0x31a	Name error (3)	dns1.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.118396044 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:05.138398886 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.158288956 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:05.176443100 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:05.194662094 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:07.399528980 CEST	8.8.8.8	192.168.2.3	0xd96a	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.432984114 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:07.454828024 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.479063988 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:07.501718998 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	gandcrab.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:07.524806976 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	gandcrab.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:07.918035030 CEST	8.8.8.8	192.168.2.3	0xd96a	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.840522051 CEST	8.8.8.8	192.168.2.3	0xa920	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.867008924 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:09.887459040 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.910227060 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:09.933176994 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.coin	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:09.956068039 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.coin	none	none	28	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:00:11.285418034 CEST	8.8.8.8	192.168.2.3	0xa868	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.304387093 CEST	8.8.8.8	192.168.2.3	0xa920	Name error (3)	dns2.sopro dns.ru	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.310426950 CEST	8.8.8.8	192.168.2.3	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Sep 1, 2022 00:00:11.330421925 CEST	8.8.8.8	192.168.2.3	0x2	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.350558043 CEST	8.8.8.8	192.168.2.3	0x3	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)
Sep 1, 2022 00:00:11.370852947 CEST	8.8.8.8	192.168.2.3	0x4	Name error (3)	nomorerans om.bit	none	none	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.388839006 CEST	8.8.8.8	192.168.2.3	0x5	Name error (3)	nomorerans om.bit	none	none	28	IN (0x0001)

Statistics

Behavior



- gI5xZdIxUs.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- isqmkp.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- isqmkp.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost.exe
- nslookup.exe
- conhost

General	
Target ID:	1
Start time:	23:57:53
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\gI5xZdIxUs.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gI5xZdIxUs.exe"
Imagebase:	0xfc60000
File size:	101710 bytes
MD5 hash:	98A12EC721C098842FBFD7384D5A72AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000001.00000000.272296797.000000000FC6A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000001.00000002.537541962.000000000FC6A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000001.00000002.537565986.000000000FC72000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000001.00000000.272303387.000000000FC72000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	bwduumgtptl	unicode	"C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe"	success or wait	1	FC62AAA	RegSetValueExW

Analysis Process: nslookup.exe PID: 5960, Parent PID: 5280

General	
Target ID:	5
Start time:	23:58:02
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns1.soprodns.ru
Imagebase:	0x140000
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: 792, Parent PID: 5960

General

Target ID:	7
Start time:	23:58:03
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4684**, Parent PID: **5280**

General

Target ID:	11
Start time:	23:58:05
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0x140000
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: **5556**, Parent PID: **4684**

General

Target ID:	13
Start time:	23:58:06
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: isqmkp.exe PID: **5464**, Parent PID: **3452**

General

Target ID:	14
Start time:	23:58:08
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe"
Imagebase:	0xf9d0000
File size:	101710 bytes
MD5 hash:	F4758788F11A0DE8D11EB4B8C515FFBD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000002.315651936.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000E.00000000.307654244.000000000F9E2000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000000.307645700.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000E.00000002.315662109.000000000F9E2000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe, Author: kevoreilly
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: nslookup.exe PID: **4596**, Parent PID: **5280**

General

Target ID:	15
Start time:	23:58:08
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns2.soprodns.ru
Imagebase:	0x140000
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: **1920**, Parent PID: **4596**

General	
Target ID:	16
Start time:	23:58:13
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **6112**, Parent PID: **5280**

General	
Target ID:	17
Start time:	23:58:16
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns2.soprodns.ru
Imagebase:	0x140000
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: **4624**, Parent PID: **6112**

General	
Target ID:	18
Start time:	23:58:16
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: isqmkp.exe PID: **1572**, Parent PID: **3452**

General	
Target ID:	20
Start time:	23:58:17
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\isqmkp.exe"
Imagebase:	0xf9d0000
File size:	101710 bytes
MD5 hash:	F4758788F11A0DE8D11EB4B8C515FFBD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000000.322631215.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000002.325486891.000000000F9DA000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000014.00000002.325494839.000000000F9E2000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000014.00000000.322638424.000000000F9E2000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security

Analysis Process: nslookup.exe PID: **1916**, Parent PID: **5280**

General	
Target ID:	21
Start time:	23:58:19
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns2.soprodns.ru
Imagebase:	0x140000
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: **5388**, Parent PID: **1916**

General	
Target ID:	22
Start time:	23:58:19
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: 5244, Parent PID: 5280

General

Target ID:	23
Start time:	23:58:22
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0x140000
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: 4592, Parent PID: 5244

General

Target ID:	24
Start time:	23:58:23
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff68f300000
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: 6028, Parent PID: 5280

General

Target ID:	25
Start time:	23:58:25
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns1.soprodns.ru
Imagebase:	0x140000
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: 1012, Parent PID: 6028

General

Target ID:	26
Start time:	23:58:26
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: 5116, Parent PID: 5280

General

Target ID:	27
Start time:	23:58:28
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0x7ff651c80000
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: 5552, Parent PID: 5116

General

Target ID:	28
Start time:	23:58:31
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **680**, Parent PID: **5280**

General

Target ID:	30
Start time:	23:58:34
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns2.soprodns.ru
Imagebase:	0x140000
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: **496**, Parent PID: **680**

General

Target ID:	31
Start time:	23:58:34
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5124**, Parent PID: **5280**

General

Target ID:	33
Start time:	23:58:37
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true

Commandline:	nslookup nomoreransom.coin dns2.soprodns.ru
Imagebase:	0x140000
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: **5484**, Parent PID: **5124**

General

Target ID:	34
Start time:	23:58:37
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4972**, Parent PID: **5280**

General

Target ID:	36
Start time:	23:58:40
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns2.soprodns.ru
Imagebase:	0x140000
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: **6096**, Parent PID: **4972**

General	
Target ID:	37
Start time:	23:58:41
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5604**, Parent PID: **5280**

General	
Target ID:	39
Start time:	23:58:44
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0x140000
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: **1784**, Parent PID: **5604**

General	
Target ID:	40
Start time:	23:58:45
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **736**, Parent PID: **5280**

General

Target ID:	41
Start time:	23:58:48
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns1.soprodns.ru
Imagebase:	0x140000
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: **6060**, Parent PID: **736**

General

Target ID:	42
Start time:	23:58:49
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4460**, Parent PID: **5280**

General

Target ID:	43
Start time:	23:58:53
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0x140000
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: 4560, Parent PID: 4460

General

Target ID:	44
Start time:	23:58:53
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: 6052, Parent PID: 5280

General

Target ID:	45
Start time:	23:58:55
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns2.soprodns.ru
Imagebase:	0x140000
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: 5984, Parent PID: 6052

General

Target ID:	46
Start time:	23:58:56
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **5424**, Parent PID: **5280**

General

Target ID:	47
Start time:	23:58:57
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns2.soprodns.ru
Imagebase:	0x140000
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: **1000**, Parent PID: **5424**

General

Target ID:	48
Start time:	23:58:58
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4364**, Parent PID: **5280**

General

Target ID:	49
Start time:	23:59:00
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns2.soprodns.ru
Imagebase:	0x140000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

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: **1552**, Parent PID: **4364**

General

Target ID:	50
Start time:	23:59:00
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5188**, Parent PID: **5280**

General

Target ID:	51
Start time:	23:59:02
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns1.soprodns.ru
Imagebase:	0x140000
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: **1960**, Parent PID: **5188**

General

Target ID:	52
Start time:	23:59:02
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

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: **1164**, Parent PID: **5280**

General

Target ID:	53
Start time:	23:59:04
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.coin dns1.soprodns.ru
Imagebase:	0x140000
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: **5824**, Parent PID: **1164**

General

Target ID:	55
Start time:	23:59:04
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **1092**, Parent PID: **5280**

General

Target ID:	58
Start time:	23:59:07
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup nomoreransom.bit dns1.soprodns.ru
Imagebase:	0x140000
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: **5844**, Parent PID: **1092**

General

Target ID:	59
Start time:	23:59:08
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **968**, Parent PID: **5280**

General

Target ID:	60
Start time:	23:59:13
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	nslookup gandcrab.bit dns2.soprodns.ru
Imagebase:	0x140000
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: **5636**, Parent PID: **968**

General

Target ID:	61
Start time:	23:59:13

Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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