Botnet trap: Hunting DGA botnets

CSIRT.CZ

Martin Kunc • 06.10.2022

cz.nic | CZ DOMAIN REGISTRY

Who we are

- CSIRT.CZ
  - National CSIRT of the Czech Republic
- CZ.NIC
  - .CZ domain registry
  - Many projects (Bird, Knot, Fred, Turris)

Command & Control server evolution (CSIRT perspective)

- IP
  - easy to block
- Domain
  - less so
- DGA domains
  - can be difficult to predict
  - blocking one has almost no effect
- others IRC, Tor, peer-to-peer

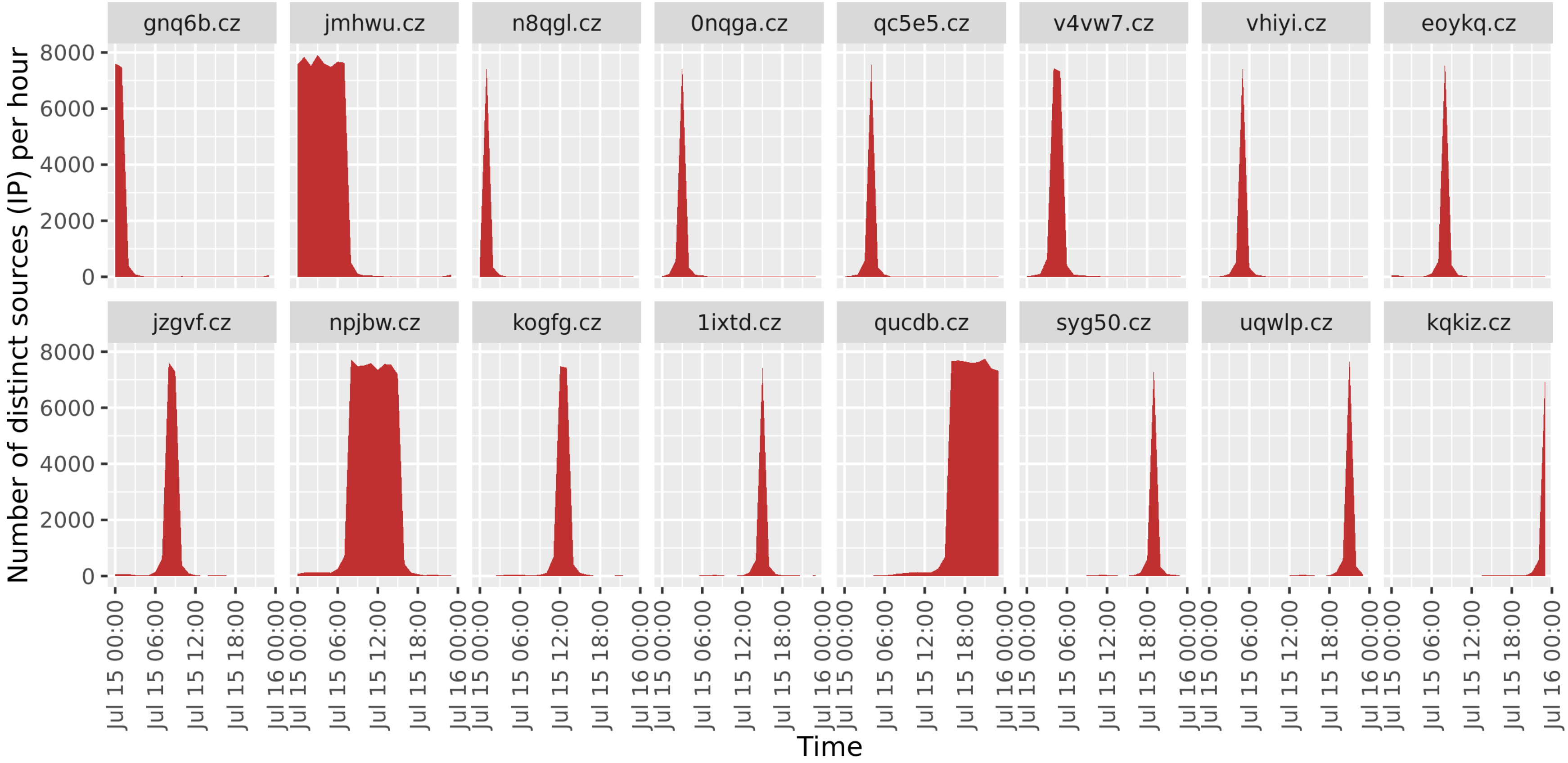
Domain Generation Algorithm - DGA

- Time based generation
- Often unique per botnet
- Need to reverse it
  - OR set clock into future
- DGA domains used by bots to communicate with C&C servers.

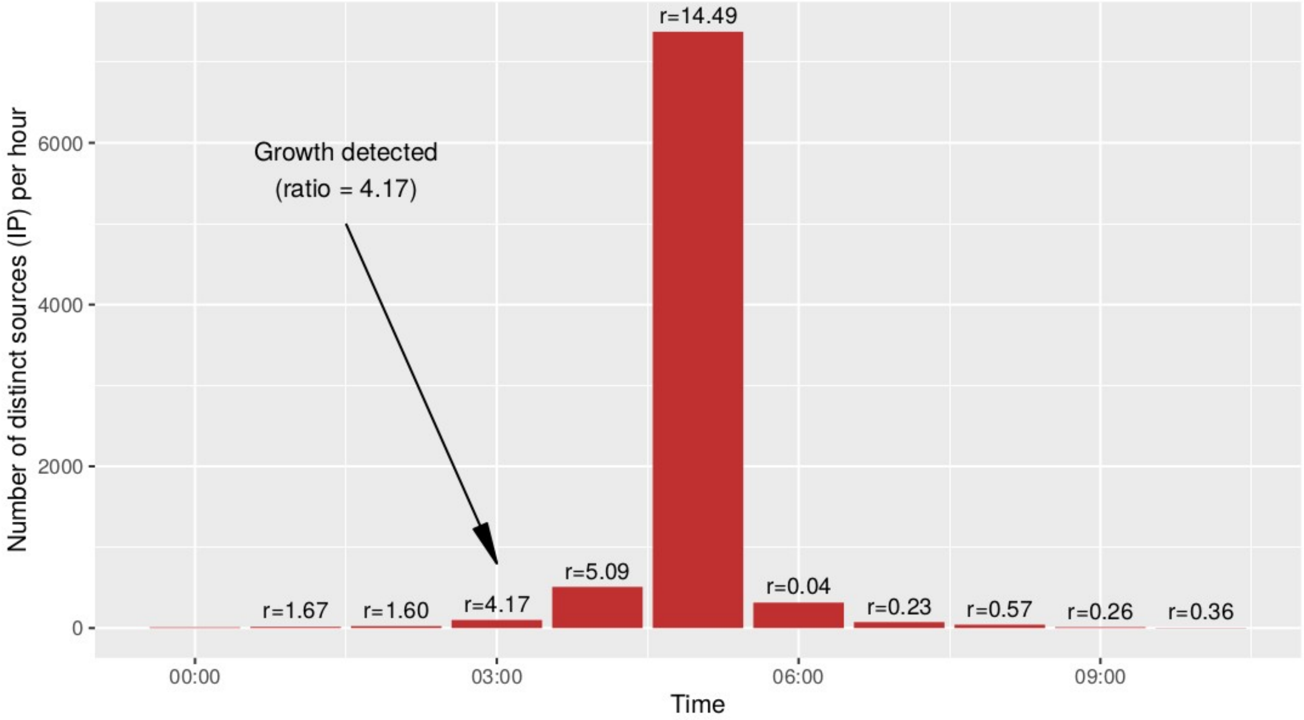
Are there any DGA domains in .CZ?

- Maciej Andziński
- None in popular DGA feeds
- ~54M distinct domains* daily (15 July 2020)
  - ~40x more than registered .CZ domains (1.3M)
- n-gram based DGA domain classifier

Detecting DGA domains in DNS traffic



Detecting DGA domains in DNS traffic



Number of unique sources for DNS queries for domain qnc1p.cz on 16 July 2020

Our plan

- register a DGA domain
- point towards our server
- profit?

InetSim a.k.a. our “Botnet trap“

- ...software suite for simulating common internet services in a lab environment, e.g. for analysing the network behaviour of unknown malware samples.
- unknown botnet → unknown network service
- easily enable many services
- packet capture as backup

Registering a DGA domain

- On 16.11.2021 we detected and registered a DGA domain: **naqsz.cz**
- InetSim ready..
- Packet capture running..
- Team waiting and expecting…

- HTTPS traffic starts coming!

HTTPS on TCP/443

```
87.154.x.x - - [16/Nov/2021:13:11:25 +0100] "GET /qnap_firmware.xml?t=1637064685 HTTP/1.1" 502 182 "-" "curl/7.43.0"
23.241.x.x - - [16/Nov/2021:13:11:26 +0100] "GET /qnap_firmware.xml?t=1637064420 HTTP/1.1" 502 182 "-" "curl/7.43.0"
153.186.x.x - - [16/Nov/2021:13:11:27 +0100] "GET /qnap_firmware.xml?t=1637064688 HTTP/1.1" 502 182 "-" "curl/7.43.0"
83.68.x.x - - [16/Nov/2021:13:11:30 +0100] "GET /qnap_firmware.xml?t=1637064690 HTTP/1.1" 502 182 "-" "curl/7.43.0"
124.120.x.x - - [16/Nov/2021:13:11:30 +0100] "GET /qnap_firmware.xml?t=1637067173 HTTP/1.1" 502 182 "-" "curl/7.43.0"
222.64.x.x - - [16/Nov/2021:13:11:30 +0100] "GET /qnap_firmware.xml?t=1637064699 HTTP/1.1" 502 182 "-" "curl/7.43.0"
84.106.x.x - - [16/Nov/2021:13:11:31 +0100] "GET /qnap_firmware.xml?t=1637064682 HTTP/1.1" 502 182 "-" "curl/7.43.0"
223.19.x.x - - [16/Nov/2021:13:11:33 +0100] "GET /qnap_firmware.xml?t=1637064692 HTTP/1.1" 502 182 "-" "curl/7.43.0"
73.233.x.x - - [16/Nov/2021:13:11:33 +0100] "GET /qnap_firmware.xml?t=1637064690 HTTP/1.1" 502 182 "-" "curl/7.43.0"
151.54.x.x - - [16/Nov/2021:13:11:33 +0100] "GET /qnap_firmware.xml?t=1637064692 HTTP/1.1" 502 182 "-" "curl/7.43.0"
79.184.x.x - - [16/Nov/2021:13:11:33 +0100] "GET /qnap_firmware.xml?t=1637065440 HTTP/1.1" 502 182 "-" "curl/7.43.0"
126.85.x.x - - [16/Nov/2021:13:11:36 +0100] "GET /qnap_firmware.xml?t=1637067096 HTTP/1.1" 502 182 "-" "curl/7.43.0"
89.143.x.x - - [16/Nov/2021:13:11:36 +0100] "GET /qnap_firmware.xml?t=1637064695 HTTP/1.1" 502 182 "-" "curl/7.43.0"
92.154.x.x - - [16/Nov/2021:13:11:36 +0100] "GET /qnap_firmware.xml?t=1637064695 HTTP/1.1" 502 182 "-" "curl/7.43.0"
212.106.x.x - - [16/Nov/2021:13:11:37 +0100] "GET /qnap_firmware.xml?t=1637064695 HTTP/1.1" 502 182 "-" "curl/7.43.0"
84.30.x.x - - [16/Nov/2021:13:11:38 +0100] "GET /qnap_firmware.xml?t=1637064033 HTTP/1.1" 502 182 "-" "curl/7.43.0"
95.154.x.x - - [16/Nov/2021:13:11:38 +0100] "GET /qnap_firmware.xml?t=1637064696 HTTP/1.1" 502 182 "-" "curl/7.43.0"
185.125.x.x - - [16/Nov/2021:13:11:39 +0100] "GET /qnap_firmware.xml?t=1637064698 HTTP/1.1" 502 182 "-" "curl/7.43.0"
112.193.x.x - - [16/Nov/2021:13:11:41 +0100] "GET /qnap_firmware.xml?t=1637064699 HTTP/1.1" 502 182 "-" "curl/7.43.0"
```

QSnatch malware

- **Potential Legacy Risk from Malware Targeting QNAP NAS Devices**

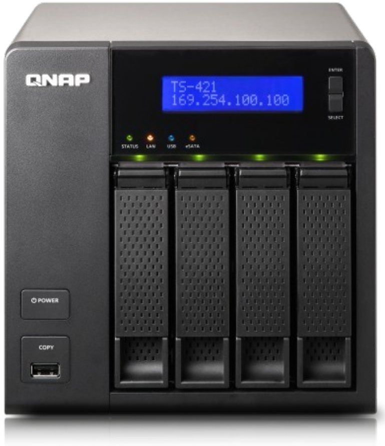
  ...The attacker then uses a domain generation algorithm (DGA) to establish a command and control (C2) channel that periodically generates multiple domain names for use in C2 communications - using the following HTTP GET request [1]:

  HTTP GET https://[generated-address]/qnap_firmware.xml?=t[timestamp]

[1] https://www.cisa.gov/uscert/ncas/alerts/aa20-209a

QNAP

- Network-attached storage (NAS) appliances



Results

- **4028** unique IP addresses
  - **726** networks (AS)
  - **90** countries

CSIRT mailing campaign

- We used abuse contact to reach IP address operator
- We sent e-mails with notification about infected QNAP device
  - **56** national/governmental CSIRTs (**3585** Ips)
  - **597** abroad e-mail addresses

Future steps

- Automatization
  - DGA domain candidates ✓
  - Domain registration (not tested)
  - InetSim can accept any domain ✓
- Analyse results
- Automate mailing results

Thank You

Martin Kunc

CZ DOMAIN
REGISTRY