Past na pokročilé botnety

CZ.NIC / CSIRT.CZ

Martin Kunc • 04.05.2023

Kdo jsme

- CSIRT.CZ
  - Národní CSIRT České Republiky
- CZ.NIC
  - Provoz domény.CZ
  - Mnoho projektů (Bird, Knot, Fred, Turris)

Řídící servery botnetu

- C&C, C2, Command and Control server
- Slouží k řízení/orchestraci botnetu
- Neutralizace typicky neutralizuje celý botnet

Evoluce řídících serverů (z CSIRT perspektivy)

- IP
  - Jednoduchá blokace
- Doména
  - složitější
- DGA Domény
  - Těžko predikovatelné
  - blokace jedné má téměř nulový efekt
- a jiné IRC, Tor, peer-to-peer

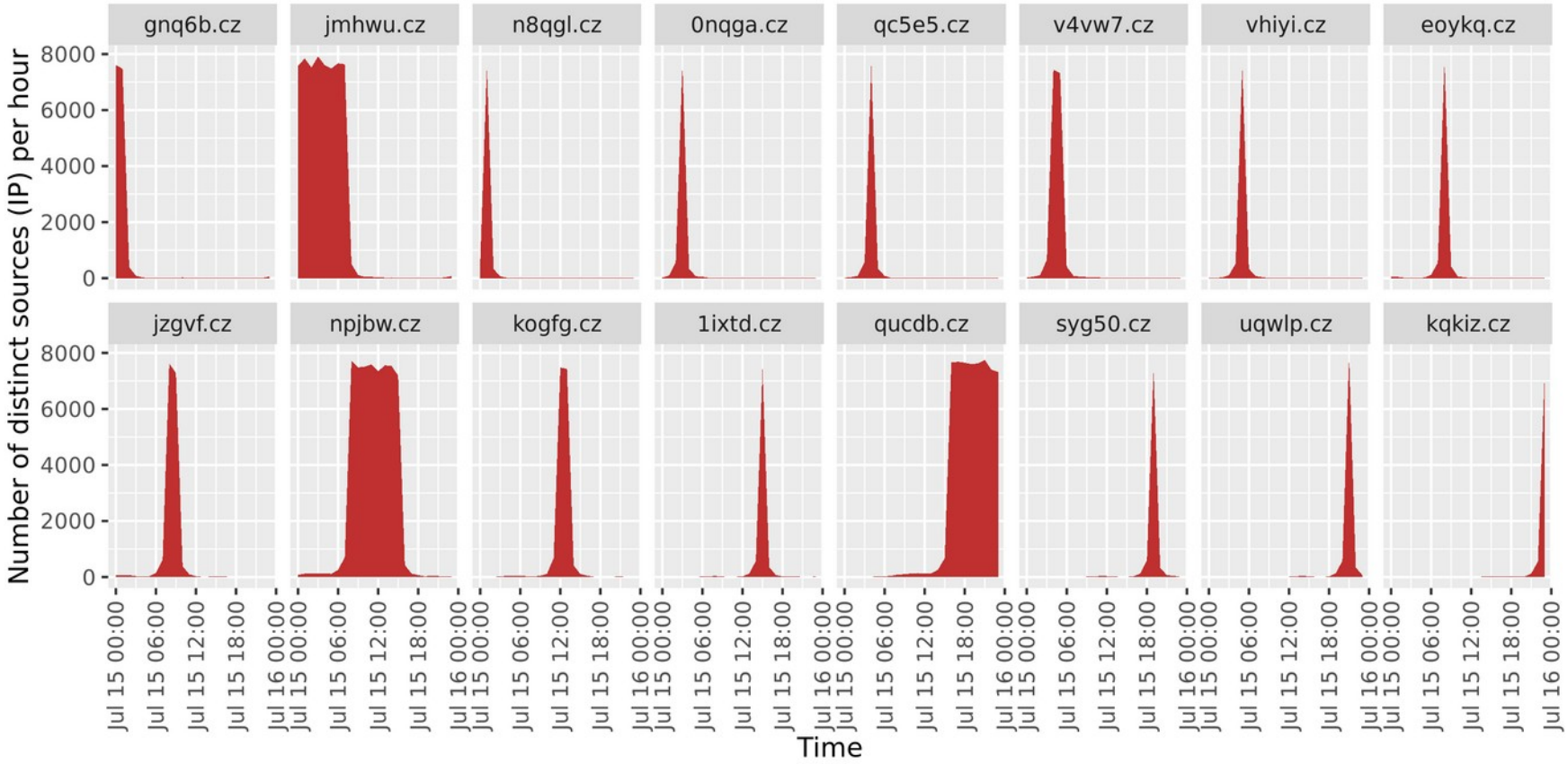
Domain Generation Algorithm - DGA

- Pseudonáhodně generované názvy domén v závislosti na času
- Unikátní per botnet
- Reverse engineering algoritmu
  - Nebo posunutí systémového času do budoucnosti

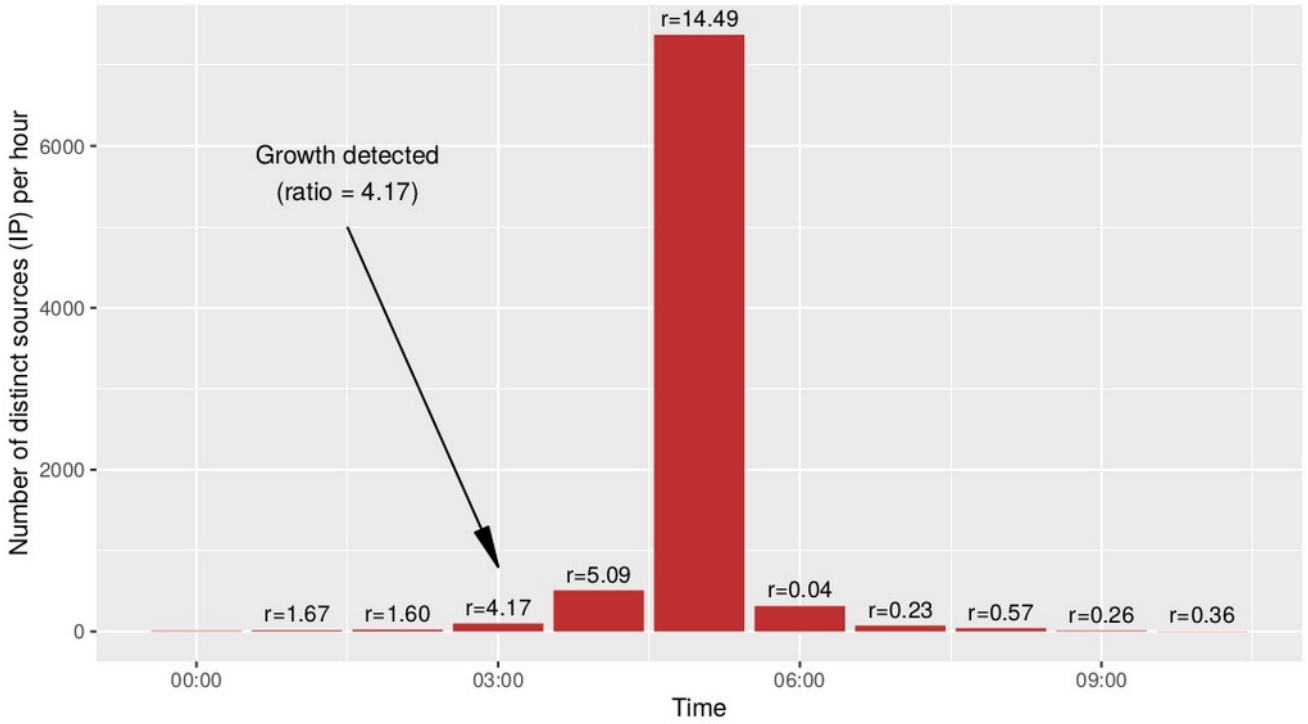
Existují DGA domény na .CZ?

- Maciej Andziński
- Žádné v běžně používaných DGA seznamech
- ~54M dotazů na unikátní domény denně (15.7.2020)
  - ~40x více než počet registrovaných .CZ domén (1.3M)
- n-gram based DGA doménový klasifikátor

Detekce DGA domén v DNS provozu



Detekce DGA domén v DNS provozu



Počet unikátních zdrojových IP adres pro DNS dotazy na doménu qnc1p.cz 16.7.2020

Plán

- Registrovat DGA doménu (tč. volnou)
- Nasměrovat na náš server (IP)
- profit?

InetSim a.k.a. naše “past na botnety“

- ...software suite for simulating common internet services in a lab environment, e.g. for analysing the network behaviour of unknown malware samples.
- neznamý botnet → neznámá síťová služba
- InetSim – snadná implementace mnoha služeb naráz
- tcpdump jako záloha

Registrace DGA domény

- Dne 16.11.2021 jsme detekovali a registrovali DGA doménu: **naqsz.cz**
- InetSim připraven..
- tcpdump běží..
- čekáme…

- HTTPS provoz začal přicházet!

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)

Výsledky

- **4028** unikátních IP adres
  - **726** sítí (AS)
  - **90** zemí

CSIRT e-mailová kampaň

- Kontaktování operátorů koncových sítí pomocí abuse kontaktů ve WHOIS
- Rozeslání e-mails s informacemi o infikovaném QNAP zařízení
  - **56** national/governmental CSIRTs (**3585** Ips)
  - **597** abroad e-mail addresses

Budoucí plány

- Automatizace
  - klasifikace DGA domén ✓
  - registrace domén (netestováno)
  - InetSim funkční pro libovolnou doménu ✓
- Analýza dalších výsledků
- Automatické rozesílání mailů

Děkuji za pozornost

Martin Kunc

CZ DOMAIN REGISTRY