CSIRT.CZ: Stress testing services

CSIRT.CZ

Martin Kunc

• 27.09.2023

Who we are

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

Our projects

ADAM

BIRD

CSIRT.CZ

Datovka

FRED

KNOT DNS

mojeiD

Safer Internet Centrum | Česká republika

TURRIS

Outline

- Motivation
- Hardware
- Software
- Results
- Caveats
- Stories

Motivation – Why?

- Share idea
- Get opinions
- Open a discussion

Motivation – Why? cont.

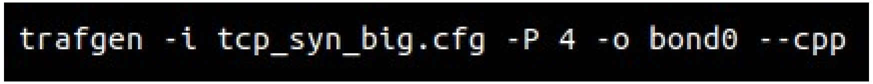
- To provide (hopefully) valuable service to our constituents
  - Test their solution
  - Test their solution provider
- Possibly learn something on the way

Current HW

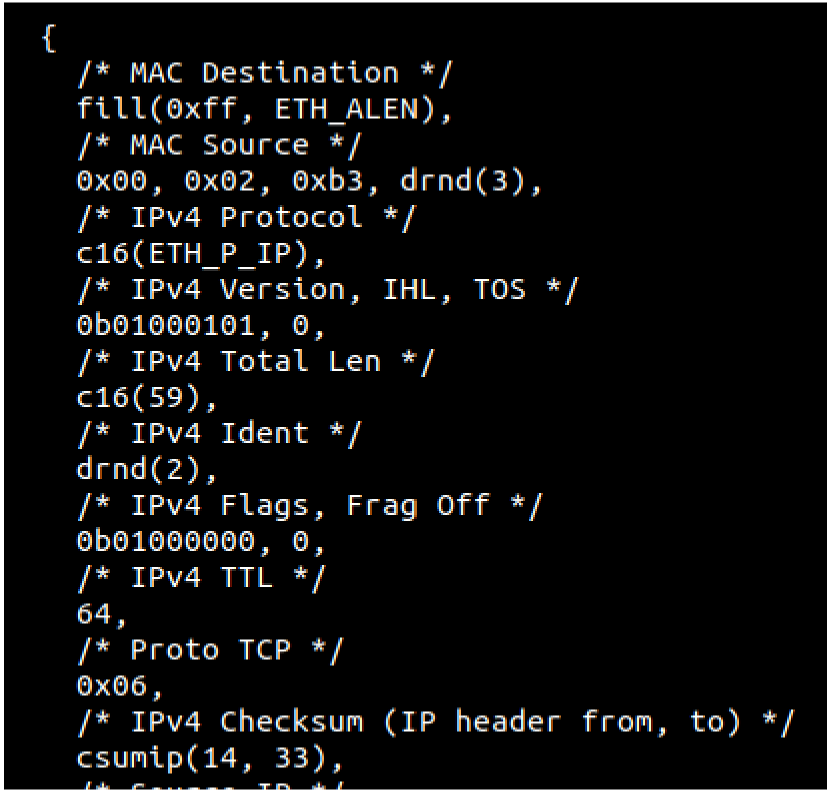
- 4 servers – 2019
- Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz
- 2 x 1 Gb NIC in bond
  - Intel X710 (10 GbE)
  - Speed reduced via slower SFP module

Software/Tooling

- Ubuntu 22.04
- Trafgen
  - configuration files
- Slowloris



```
trafgen -i tcp_syn_big.cfg -P 4 -o bond0 --cpp
```



```
{
   /* MAC Destination */
   fill(0xff, ETH_ALEN),
   /* MAC Source */
   0x00, 0x02, 0xb3, drnd(3),
   /* IPv4 Protocol */
   c16(ETH_P_IP),
   /* IPv4 Version, IHL, TOS */
   0b01000101, 0,
   /* IPv4 Total Len */
   c16(59),
   /* IPv4 Ident */
   drnd(2),
   /* IPv4 Flags, Frag Off */
   0b01000000, 0,
   /* IPv4 TTL */
   64,
   /* Proto TCP */
   0x06,
   /* IPv4 Checksum (IP header from, to) */
   csumip(14, 33),
   /* Source IP */
```

Current results

- 1 server 4 threads SYN flood
    - 1,3 Mpps – 702 Mbit/s
    - 1,8 Mpps in a special case
- Large packets
    - saturates link without problems

Caveats

- Network
  - Who will possibly suffer?
- Legal
  - Can we do/test this?
  - Contract and confirmation from all related networks
- Often done outside office hours
  - Midnight

Caveats cont.

- Committed to follow BCP-38 / RFC 2827
  - No spoofing of source addresses :(
  - Enforced by FENIX project
    - by Czech IXP – NIX.CZ
- Shared infrastructure
  - Carefull with DNS PTR records (“ddos-01”)

Story time

- Encrypted traffic
- gotcha!
- Big company fail

Thank You

Martin Kunc

CZ.NIC | CZ DOMAIN REGISTRY