GovCERT.ch

Organization and Tasks

- GovCERT is the technical analysis team of MELANI (Reporting and Analysis Centre for Information Assurance) and belongs to the Department of Finance.
- Supporting national critical infrastructures (CIP)
- We assist them during Security Incidents (e.g. Foreign Ministry, Ruag).

Organization and Tasks

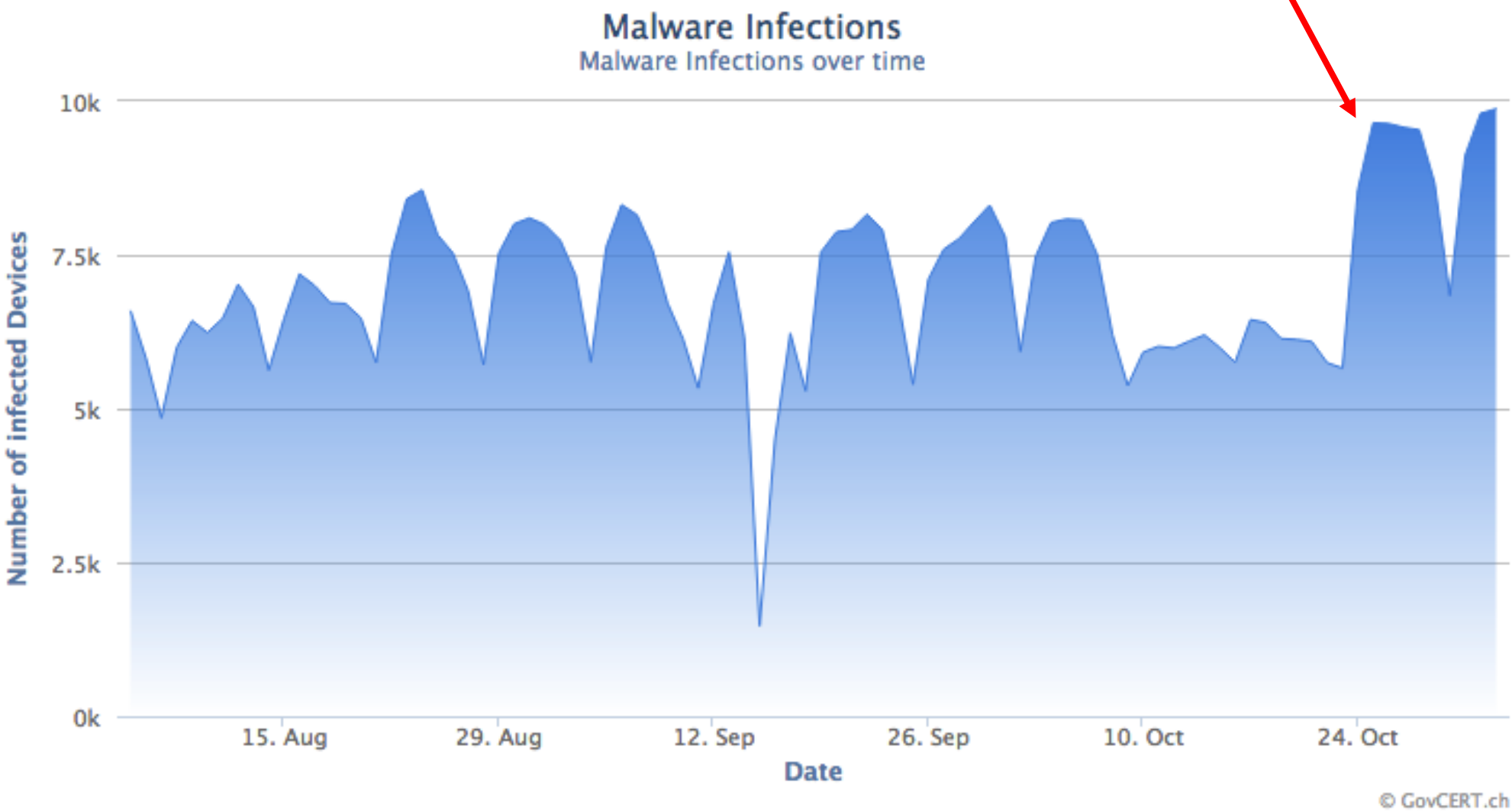
- We help protecting Swiss organizations and citizens with information about current threats (e.g. antiphishing.ch).
- Reverse engineering of Malware and writing detection rules
- We provide various threat feeds that can be processed automatically.

DroneDB

- We collect and normalize information from various DNS Sinkhole Operators (from Spamhaus, ShadowServer, abuse.ch, Microsoft and BFK) about infected devices in Switzerland.
- We provide this information free of charge in the form of a feed for Swiss ISPs and critical infrastructures.
- The feed is based on the AS number.
- An additional feed we are going to launch within the next days contains data about infected IoT devices.

DroneDB

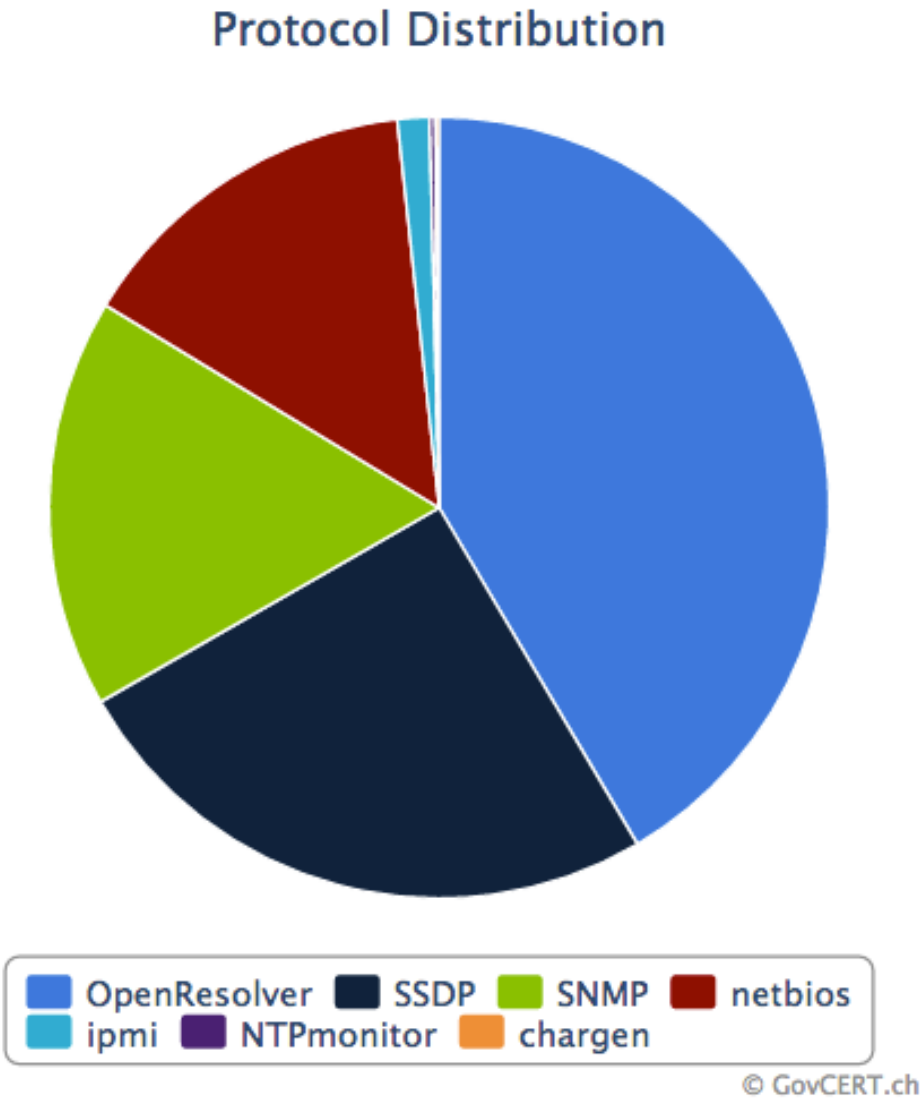
Mirai infected devices



Vulnerable Ports Feed

- We started collecting and normalizing information about devices that may be abused for DDoS attacks.
- We process information from ShadowServer, however the system is open and additional feeds can be implemented easily.
- Currently there are **80‘000** unique IPs per week that can be potentially abused for DDoS reflection attacks.

Vulnerable Ports Feed



Vulnerable Ports Feed

- Based on the hostnames, we saw this week:
  - 637 Mail Servers
  - 248 NAS Devices
  - 2 Core Routers
  - 2 Domain Controllers

Vulnerable Ports Feed

- Would you be interested in such a feed?
- Would you inform your customers about such issues?
- Please contact us at outreach@govcert.ch
- PGP Keys are here: https://www.govcert.admin.ch/downloads/govcert.pgp
- Follow us on Twitter: https://twitter.com/GovCERT_CH