IoT Network Monitoring
for Security and Privacy

Dr. Markus Donko-Huber
NysosTech e.U.

`whois` Markus Donko-Huber

- 10 years privacy & security research
- Information Security Engineer
- Privacy Enhancing Technologies at TU Vienna
- Open Source ♥

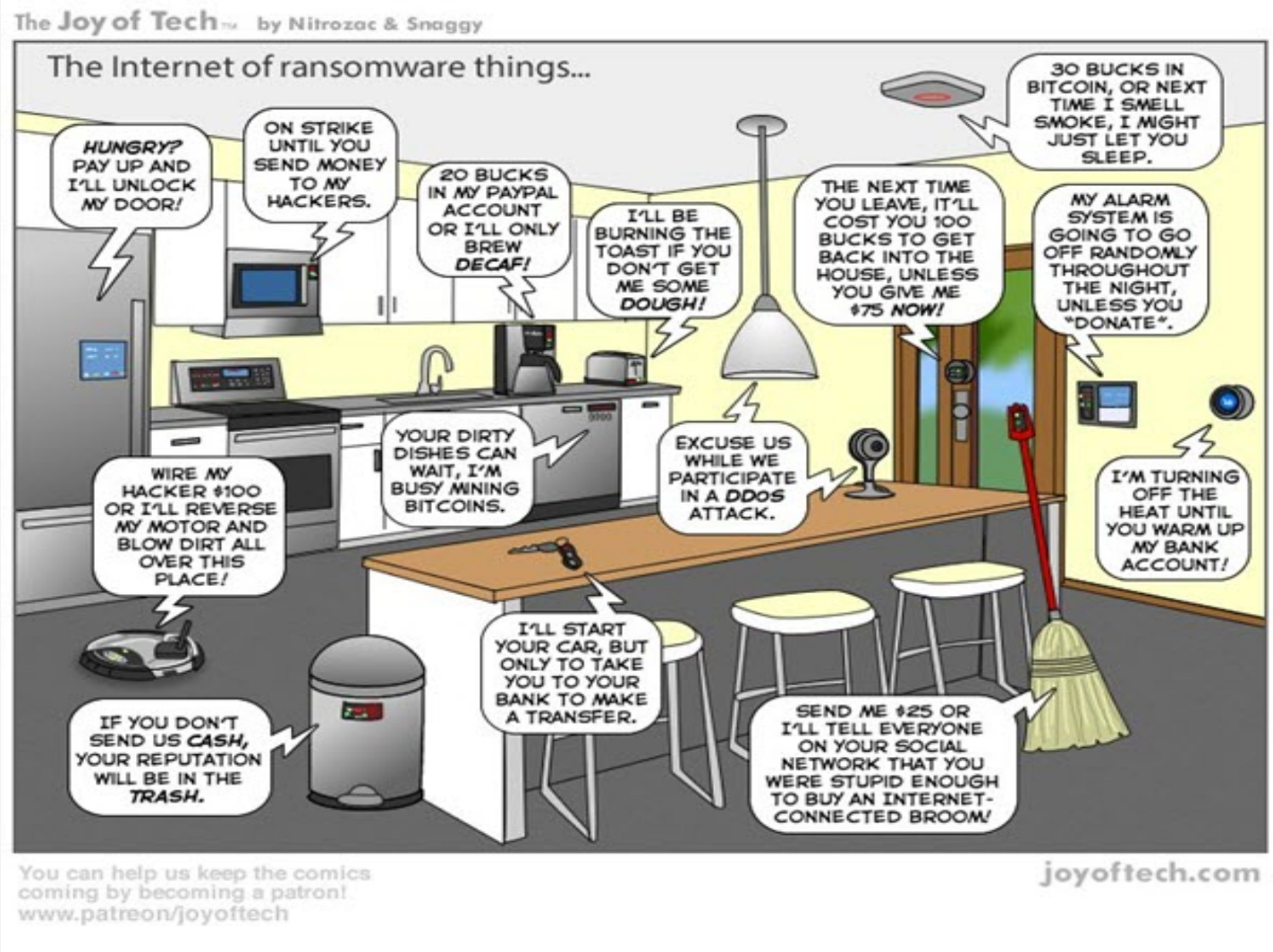
IoT Security & Privacy

IoT Vision



https://upribox.org

IoT – closer to reality



https://upribox.org

IoT 2014


black hat
USA 2014
Smart Nest Thermostat
A Smart Spy in Your Home
Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin
Security in Silicon Laboratory, University of Central Florida

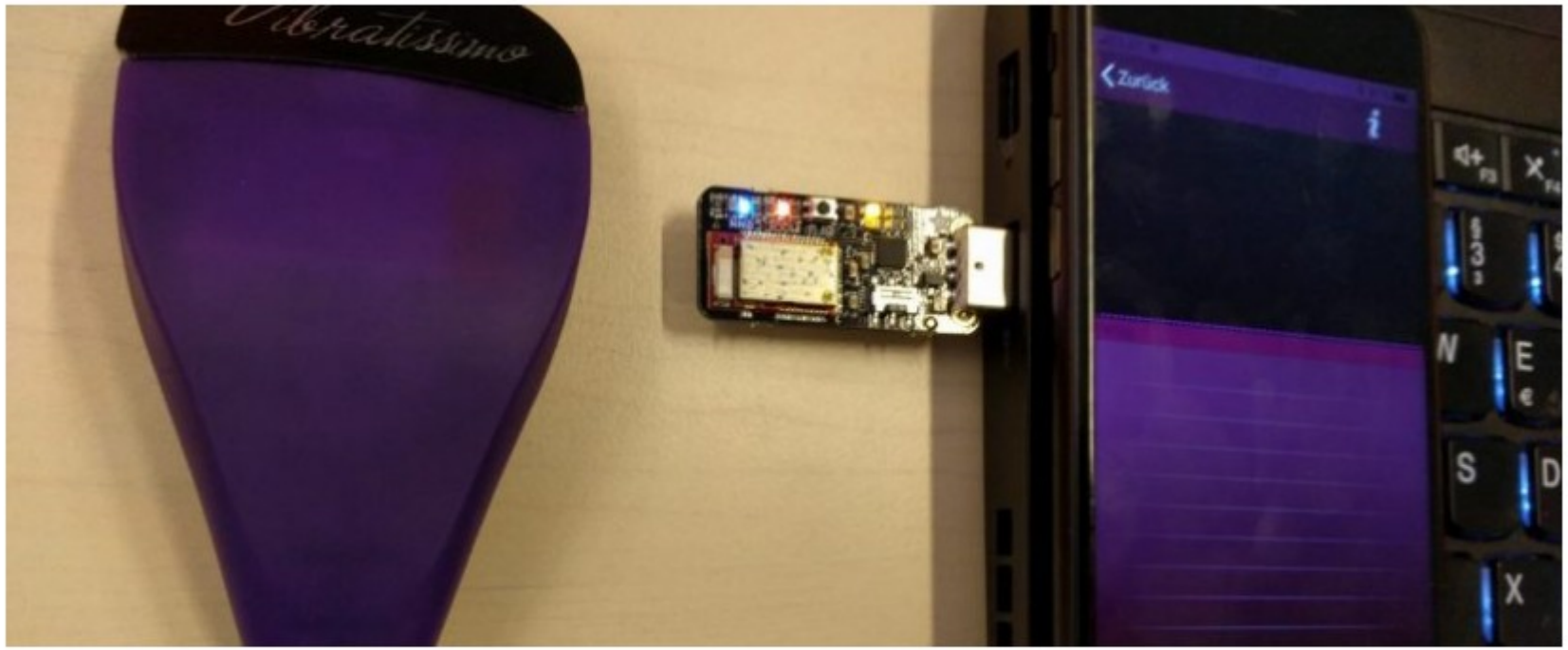
IoT 2016

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321

- Mirai Malware
  - Botnet of IoT devices
  - 60 common factory default usernames and passwords

- First high-profile IoT powered attack
  - Attacks on Brian Krebs (680 Gbps), OVH (1 Tbps), Dyn

IoT 2018



INTERNET OF DILDOS: A LONG WAY TO A VIBRANT FUTURE – FROM IOT TO IOD

On 1. Feb

In the course of our Internet of Things (IoT) research SEC Consult is going to review the security of multiple smart sex toys. The current roadmap includes the following test devices:

https://upribox.org

(1) IoT devices are low hanging fruits
time to market / weak defaults

(2) IoT devices are invasive
vendors collect lots of data

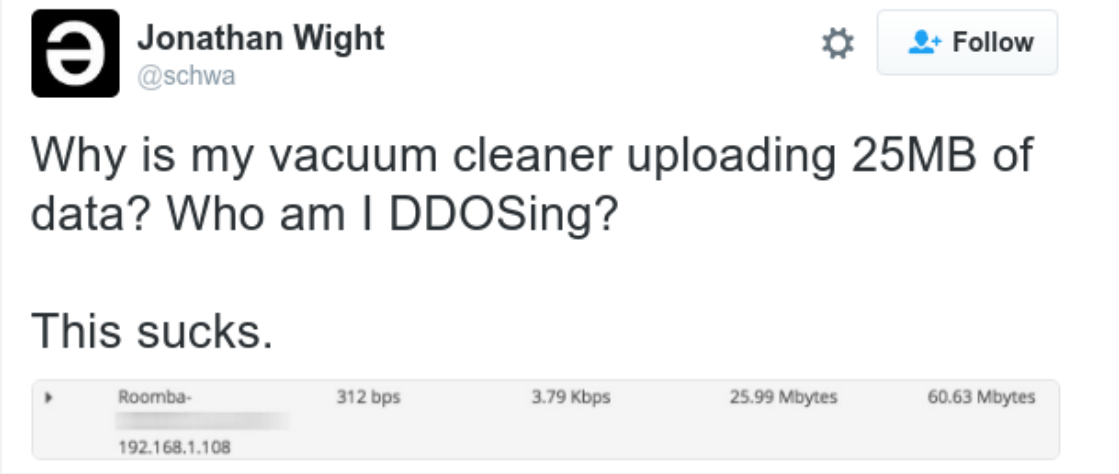
(3) So what?
all devices eventually become “smart”

IoT Network Forensics

https://upribox.org

How to find out whats going on with your devices?

(1) Setup test WiFi / router
(2) Analyze traffic with `tcpdump`



Devices

What is connected?

Behavior

Whom are the talking to?

IoT Network Forensics
Device Discovery

https://upribox.org

IoT Network Monitoring
Traffic Analysis

https://upribox.org

Traffic Characteristics

Deep packet inspection

Communication endpoints

DNS queries

ntopng

- Open Source traffic analysis tool
- Linux, *BSD, MacOS
- Realtime + historical traffic analysis
- Application protocol detection with `nDPI`

nDPI

- Supports over 100 Applications
  (Dropbox, Skype, Facebook, etc.)
- Classification independent of used ports
- Encrypted traffic is classified based on certificates in TLS handshake [TLS 1.3]

Analysis of DNS queries

- Simple to analyze DNS queries (`tcpdump`, `scapy`, `dnsmasq`, etc.)
- Good indicator for exchanged data
  - updates.samsung.com, api.weather.org ...

(1) Device Discovery
User Agent String + SSDP

(2) Traffic Analysis
ntopng + DNS queries

(3) Making this easy to use
usable privacy box

Usable Privacy Box

upribox v2

https://upribox.org

Usable Privacy Box (upribox)

- Funded by IPA netidee.at

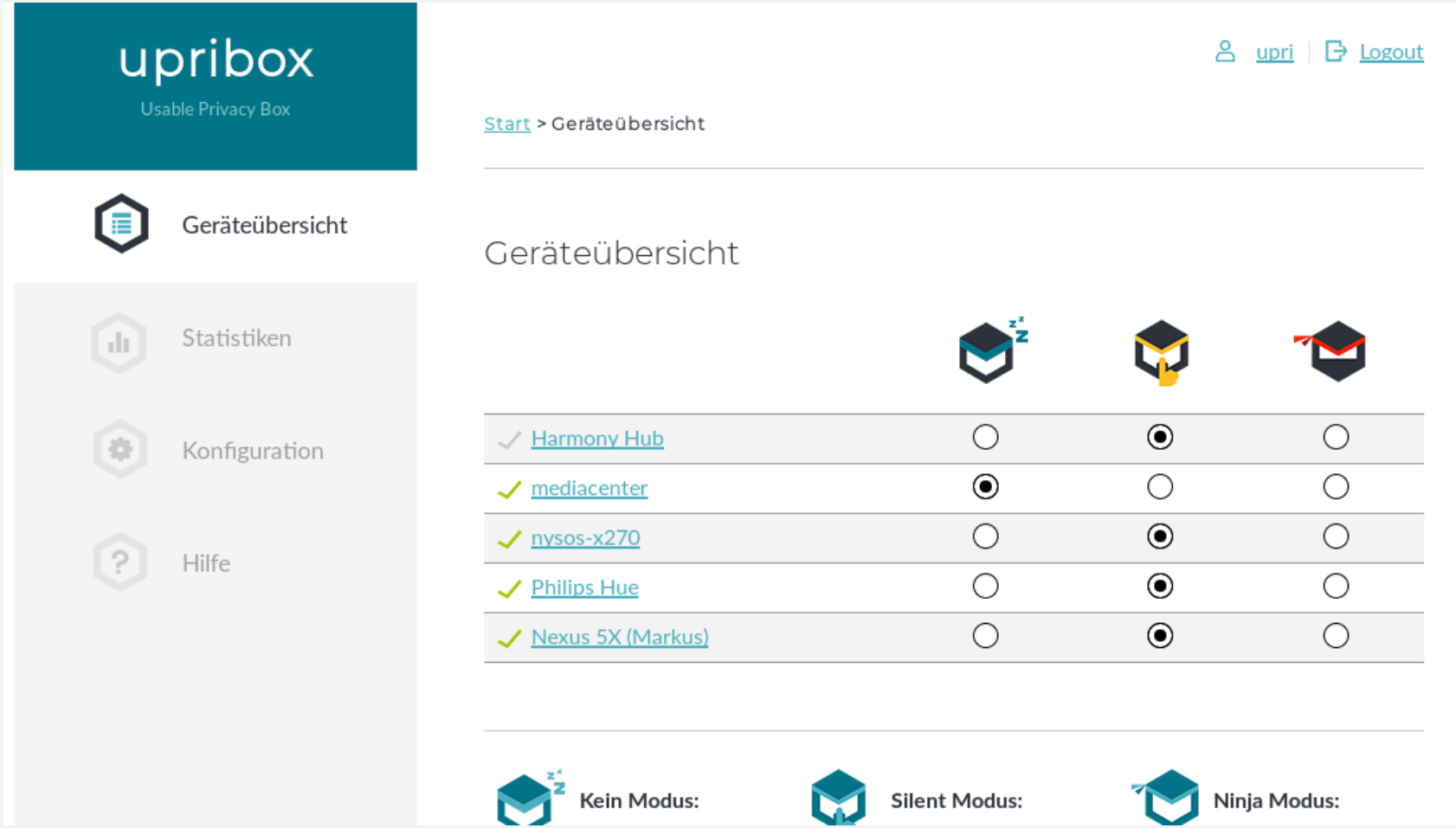
netidee
OPEN INNOVATIONS

- Open Source Software for RaspberryPi 3
- Focus on Usability
  - Standalone WiFi / Router
  - Adblocking, Tor
  - Device Monitoring

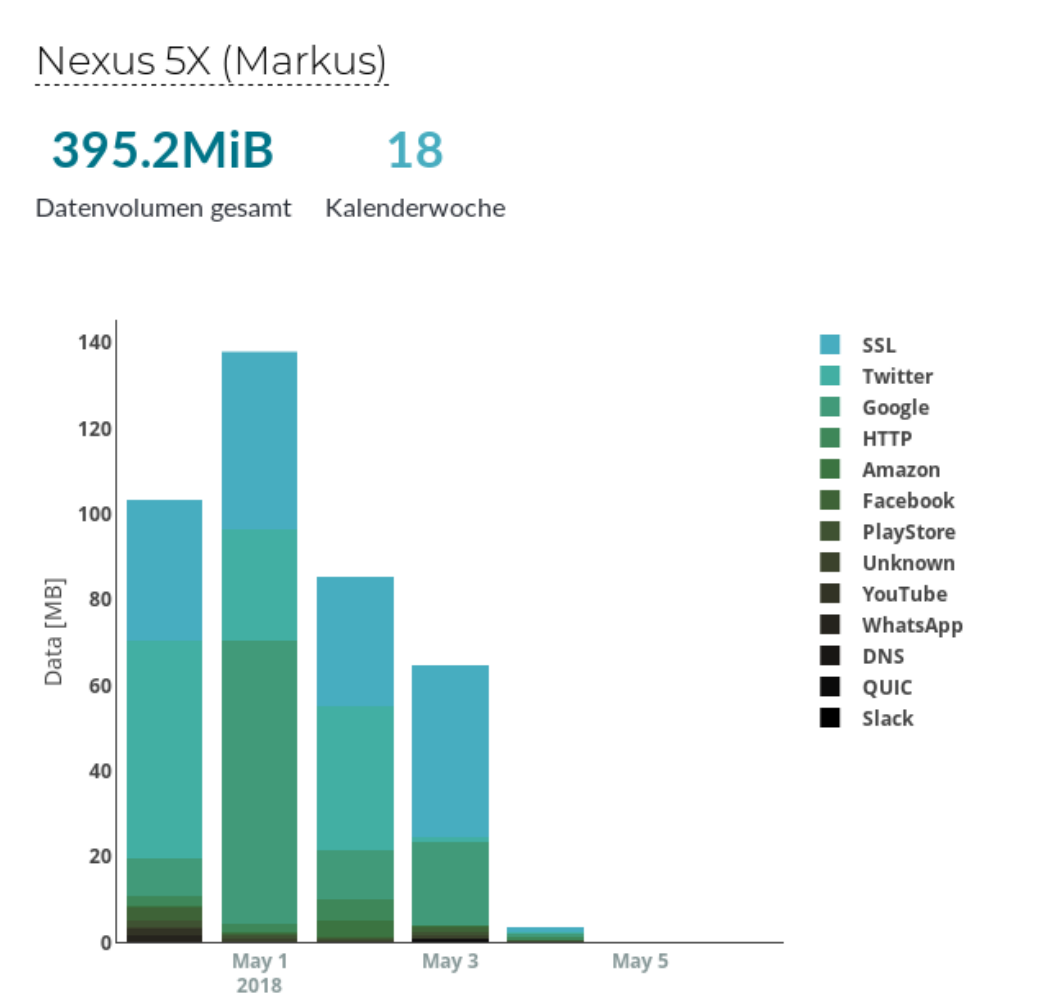


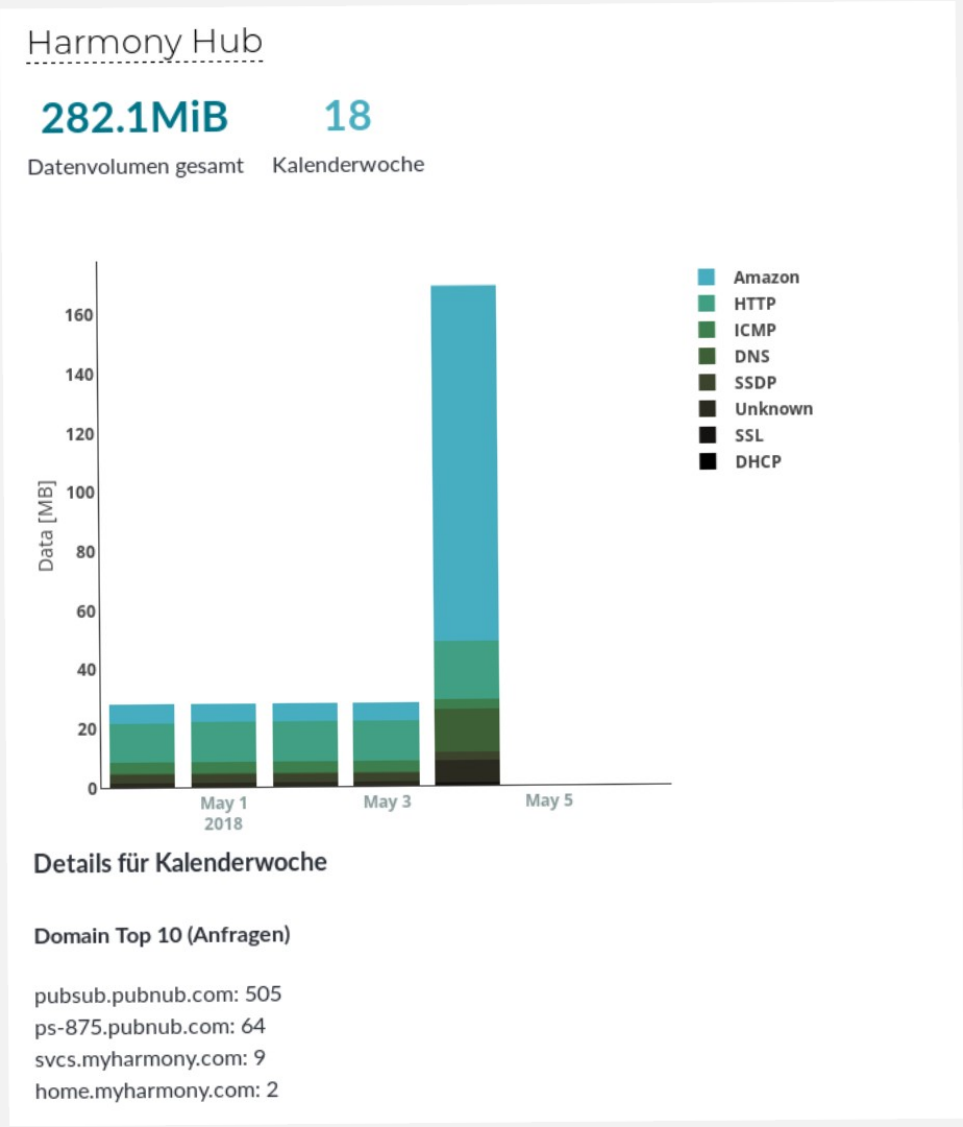
https://upribox.org

upribox v2 – Device Overview



upribox v2 – Traffic Overview





https://upribox.org

Usable Privacy Box

- Download the latest image on Github
- Document (and fix) bugs on Github
- Funding via Onlineshop

  https://upribox.org/shop

IoT Network Forensics

Passive Detection Methods

play with fingerbank, SSDP

Analyze Network Behavior

play with ntopng, DNS

Setup Usable Privacy Box

v2 image will be released soon

Dr. Markus Donko-Huber
markus@upribox.org