CHOO CHOO, NETWORK TRAIN

THE ONE TO RULE YOUR PERIMETER

MARTIN HRON

black hat EUROPE 2022

TRAIN OPERATOR

NAME

MARTIN HRON

ALIAS

THINKCZ

OCCUPATION

SECURITY RESEARCH

AFFILIATES

INDEPENDENT
AVAST
2K GAMES
SODATSW

SCAN ME

DIAGNOSES

COFFEE ADDICT

THINGS BREAKER

OCD

SKILLS

LOW-LEVEL

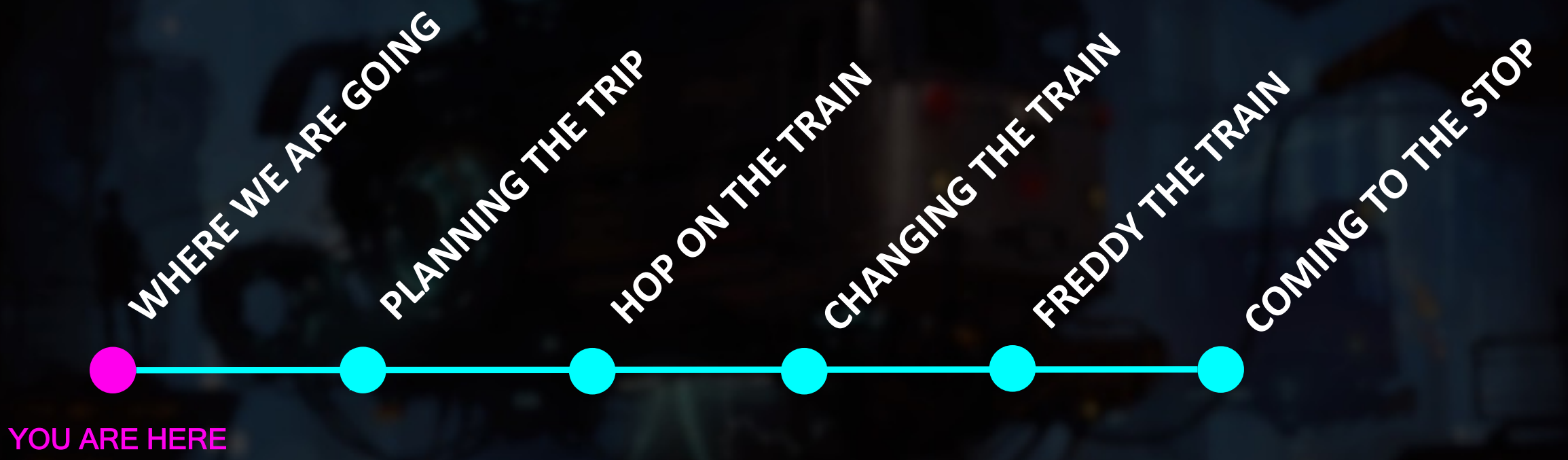
HARDWARE

REVERSING

COFFEE MACHINES

DIAL-UP AND BBS

WHERE WE ARE GOING

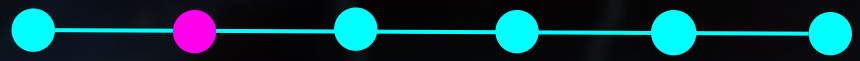


WHERE WE ARE GOING

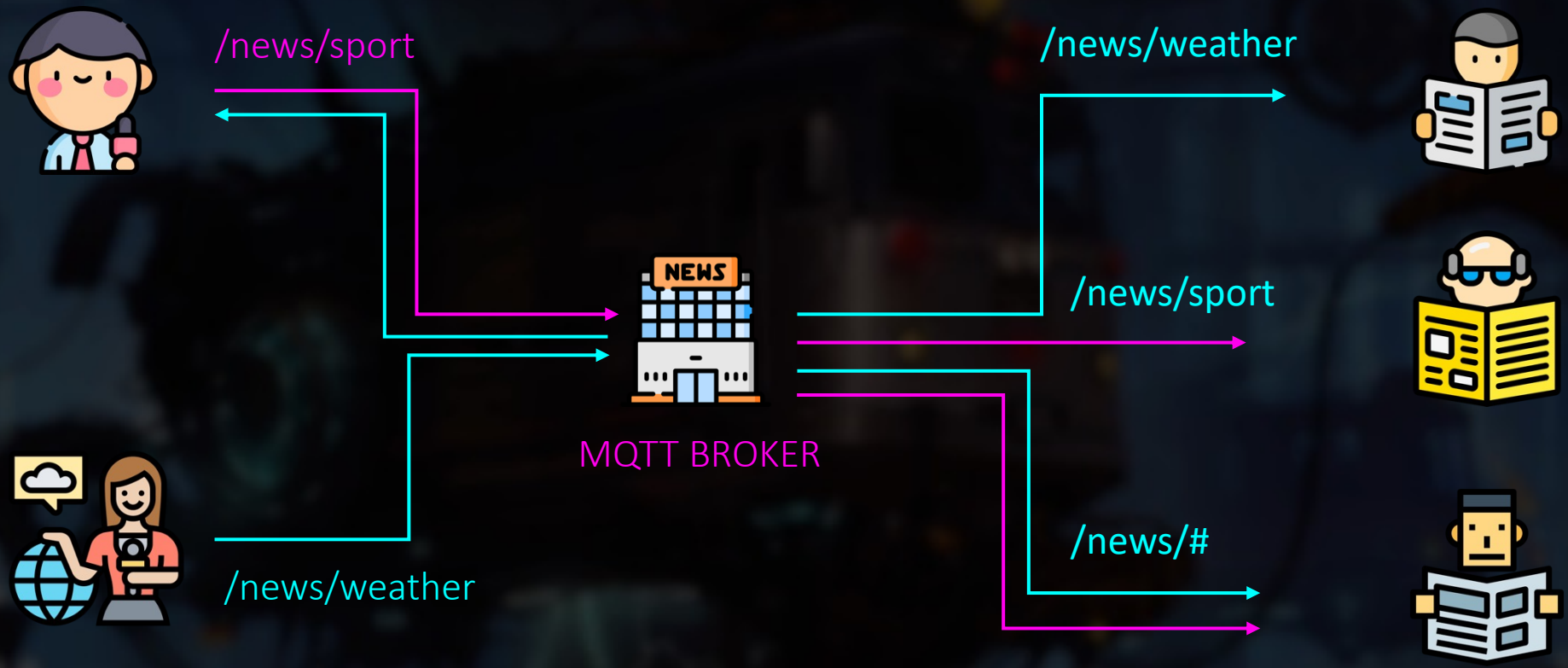
A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila.”

Mitch Ratliff

PLANNING THE TRIP

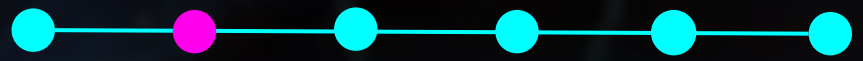


MQTT NAIVE MODEL



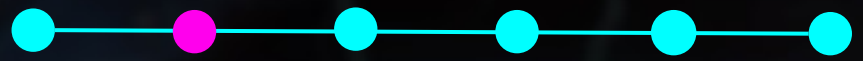
MQTT BASICS

- publisher - subscriber model
- payload agnostic
- topics can be organized in a tree like structure
- when subscribing, wildcards # and + can be used
- usually operates through TCP on port 1883 and 8883 for TLS
- supports the last will and retained topics



MQTT BROKERS

- the most famous and used is mosquitto (over 80%)
- supports ACL lists
- plaintext TCP, TLS or WS
- username, password, certificate, client identification
- multiple listeners with separate configs



WHEN OCD KICKS IN

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | AUG 20, 2018 8:41 AM PDT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

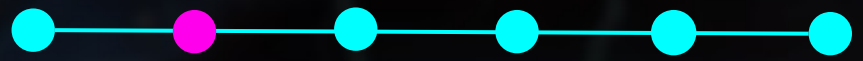
NEWS

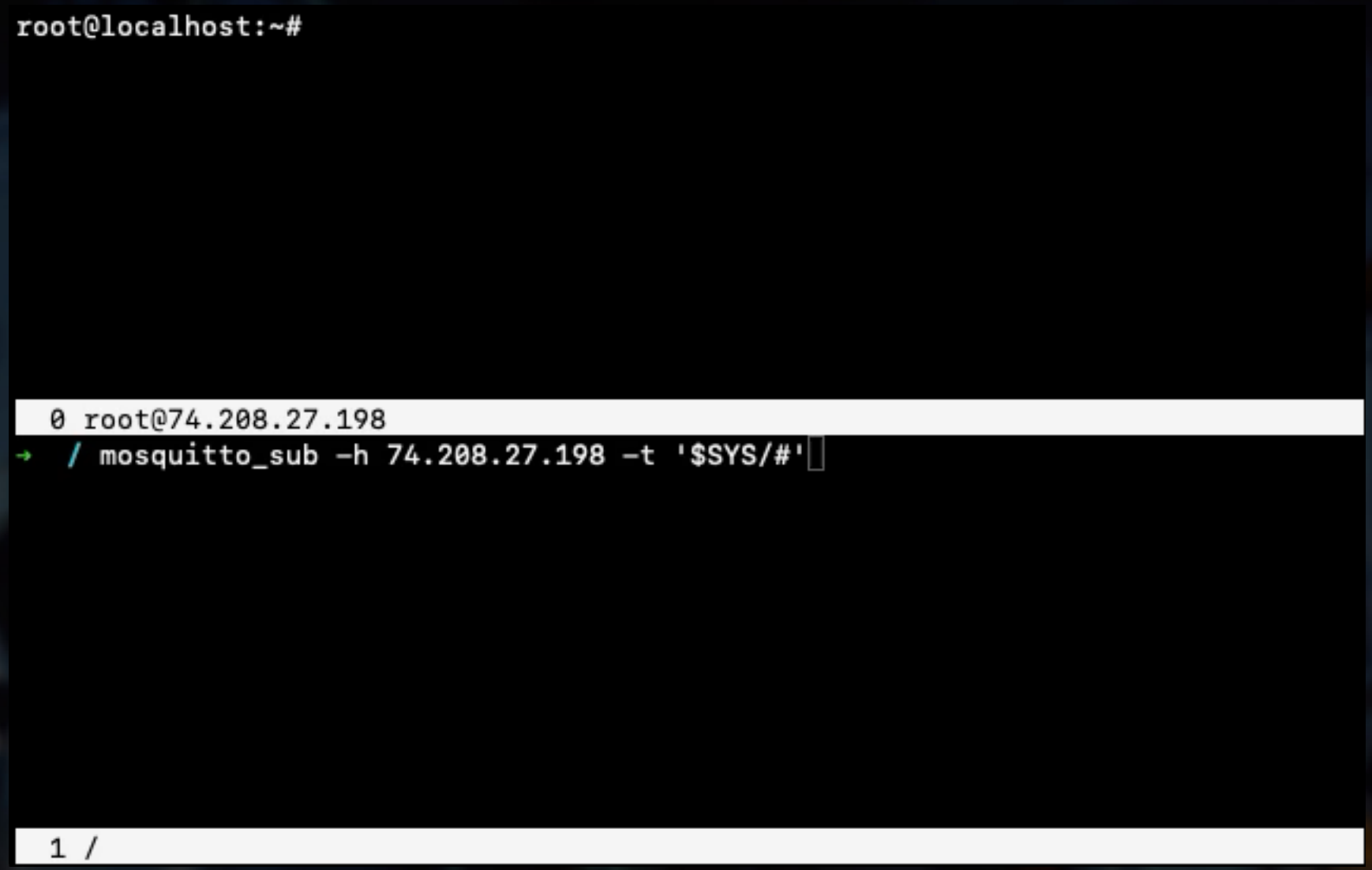
32,000 smart homes can be easily hacked due to misconfigured MQTT servers

Thanks to MQTT servers which are either misconfigured or not protected with a password, it is easy peasy to hack a smart home.

OUT-OF-THE-BOX PROBLEM

Devices and SW designed with convenience in mind more than security, leads to the situation where more then 60% installations of MQTT servers have never been set-up and left with default credentials





PLANNING THE TRIP

THE PROBLEM

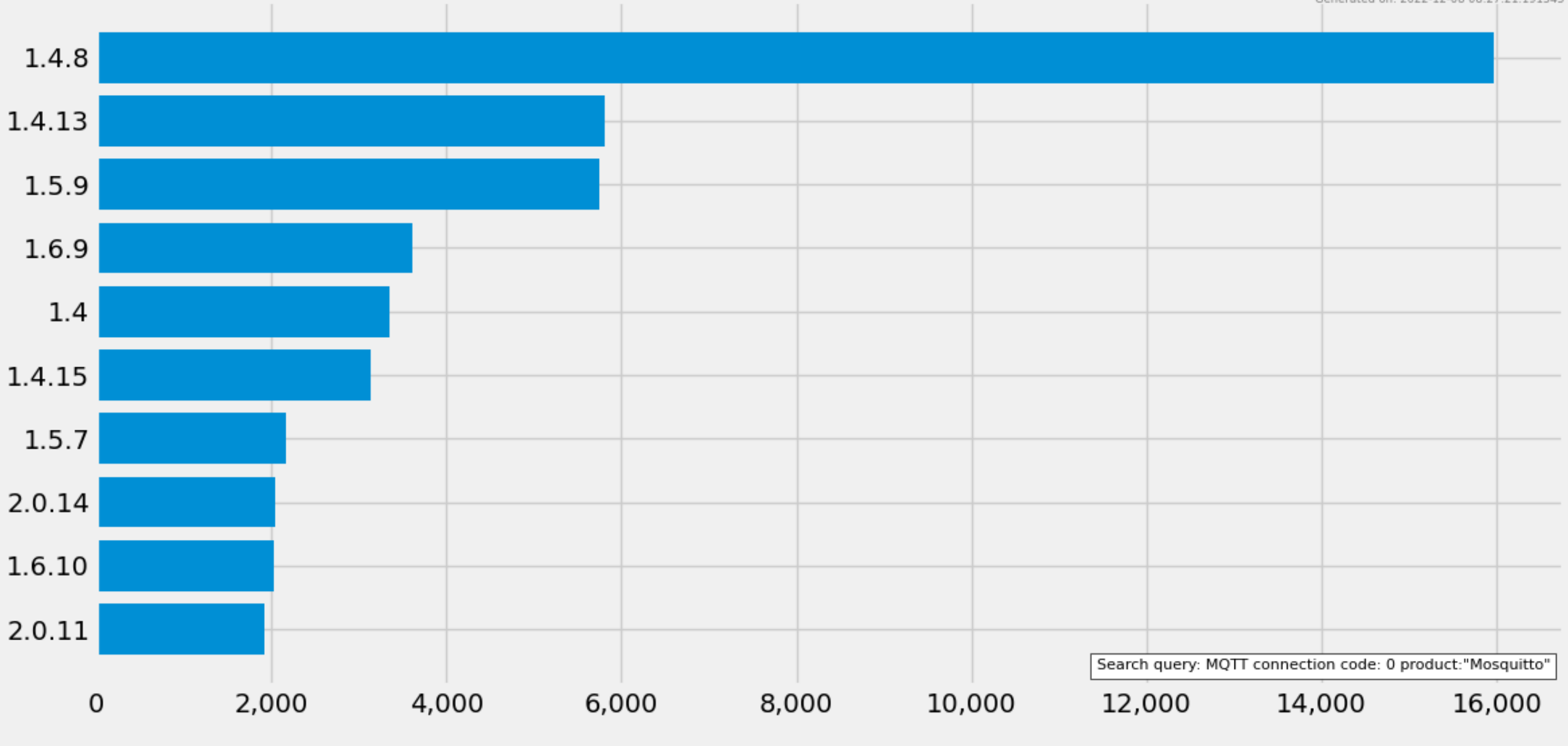
```
# defaults to true
# for version  < 2.0
# allow_anonymous false
```

```
# defaults to false
# for version  >= 2.0
# allow_anonymous false
```

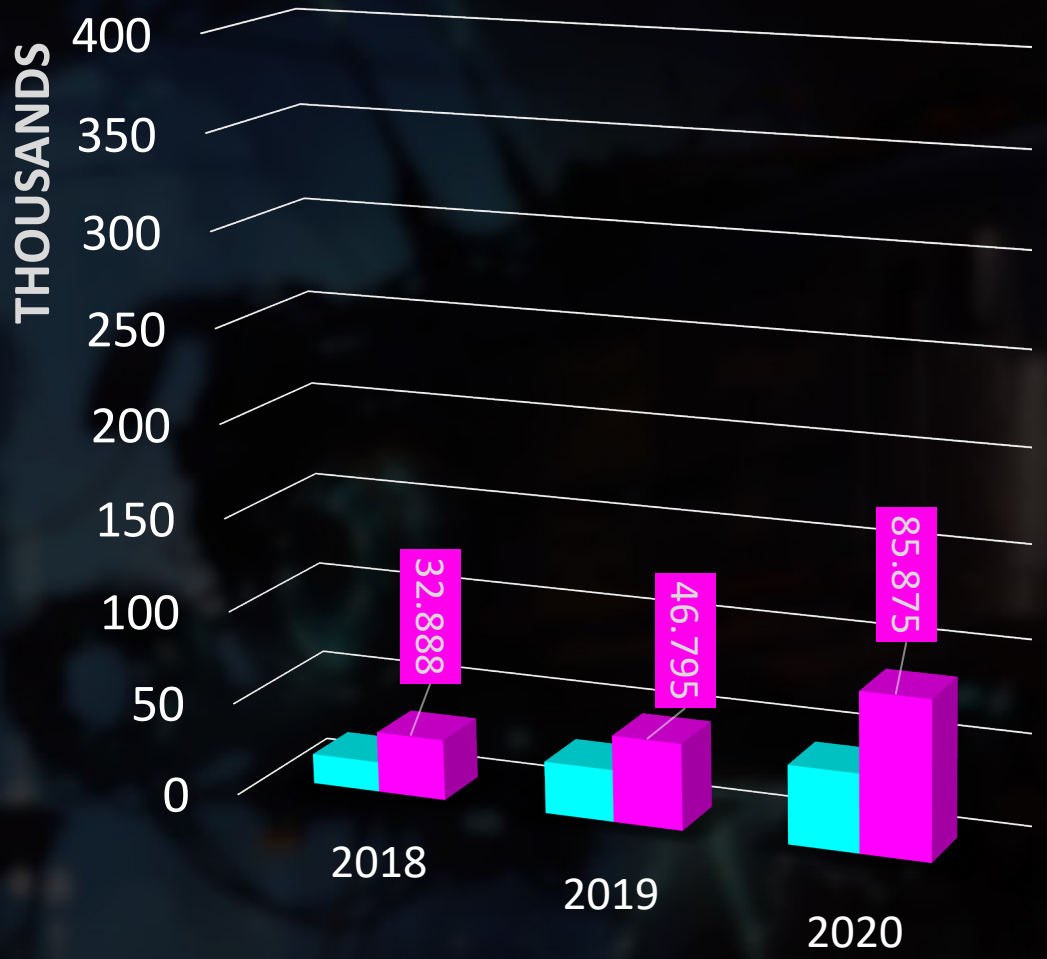
SHODAN

Top 10 Values for: version

Generated on: 2022-12-08 08:27:21.191545



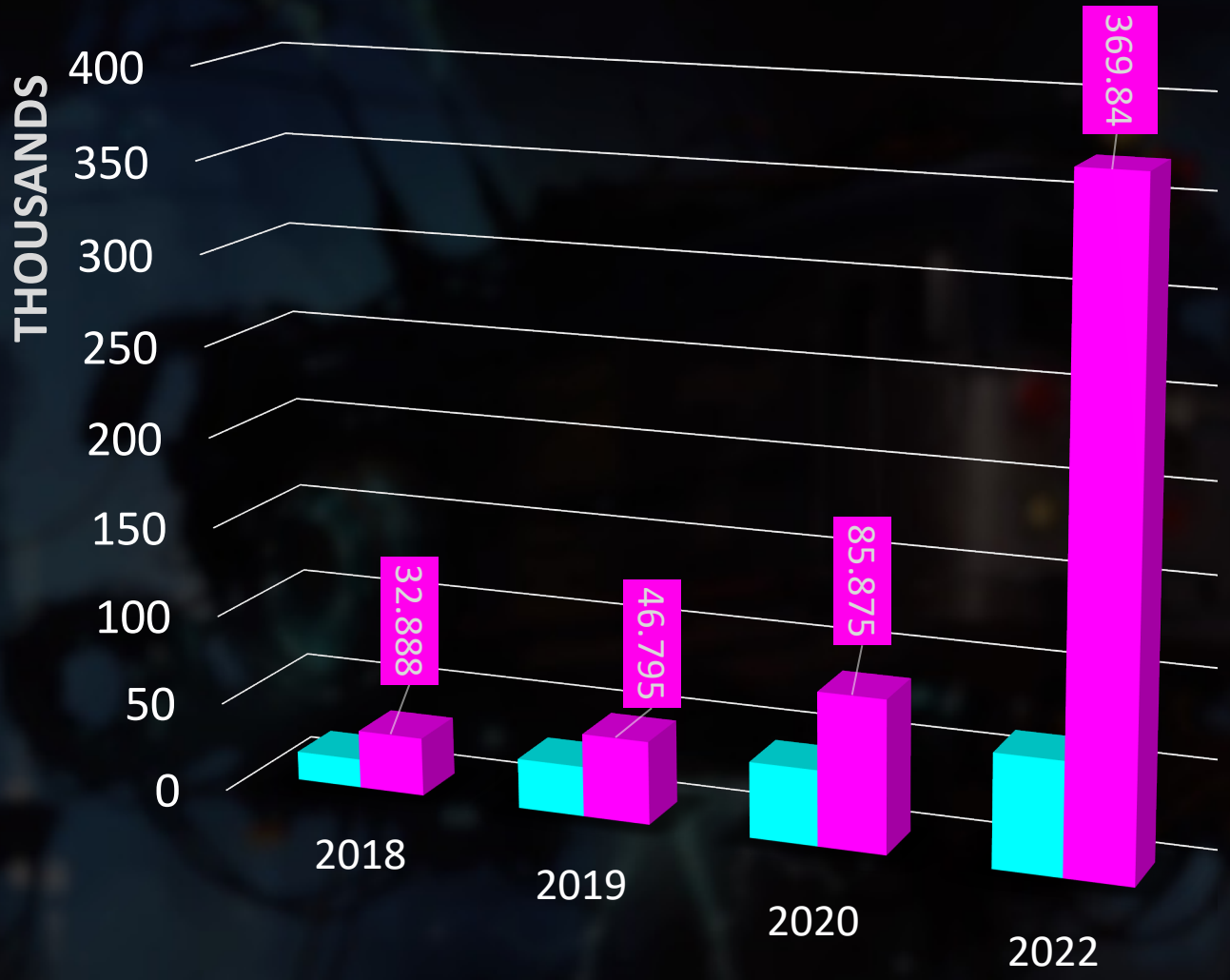
MQTT SERVERS OUT THERE



no password

protected

MQTT SERVERS OUT THERE

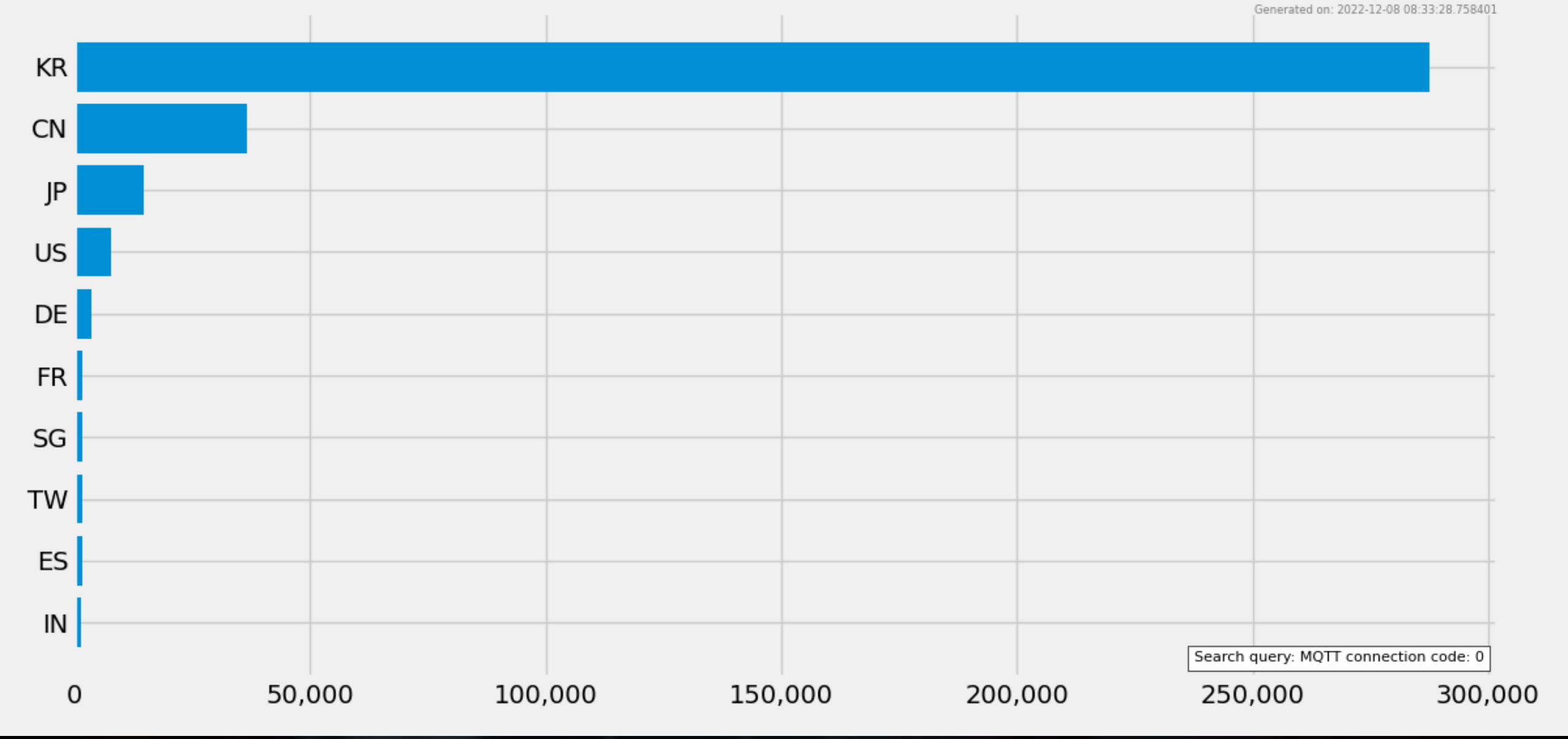


no password

password

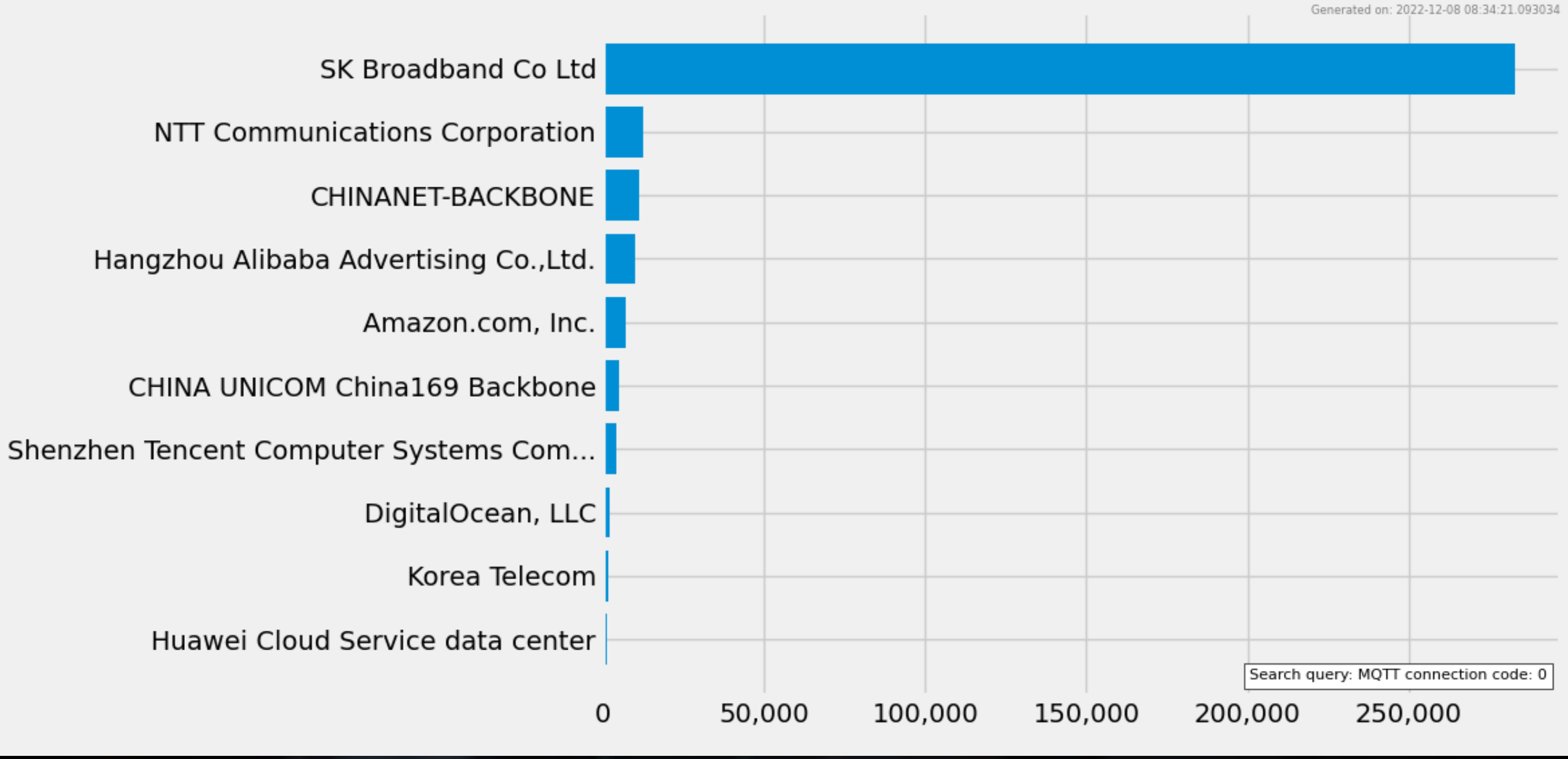
SHODAN

Top 10 Values for: country



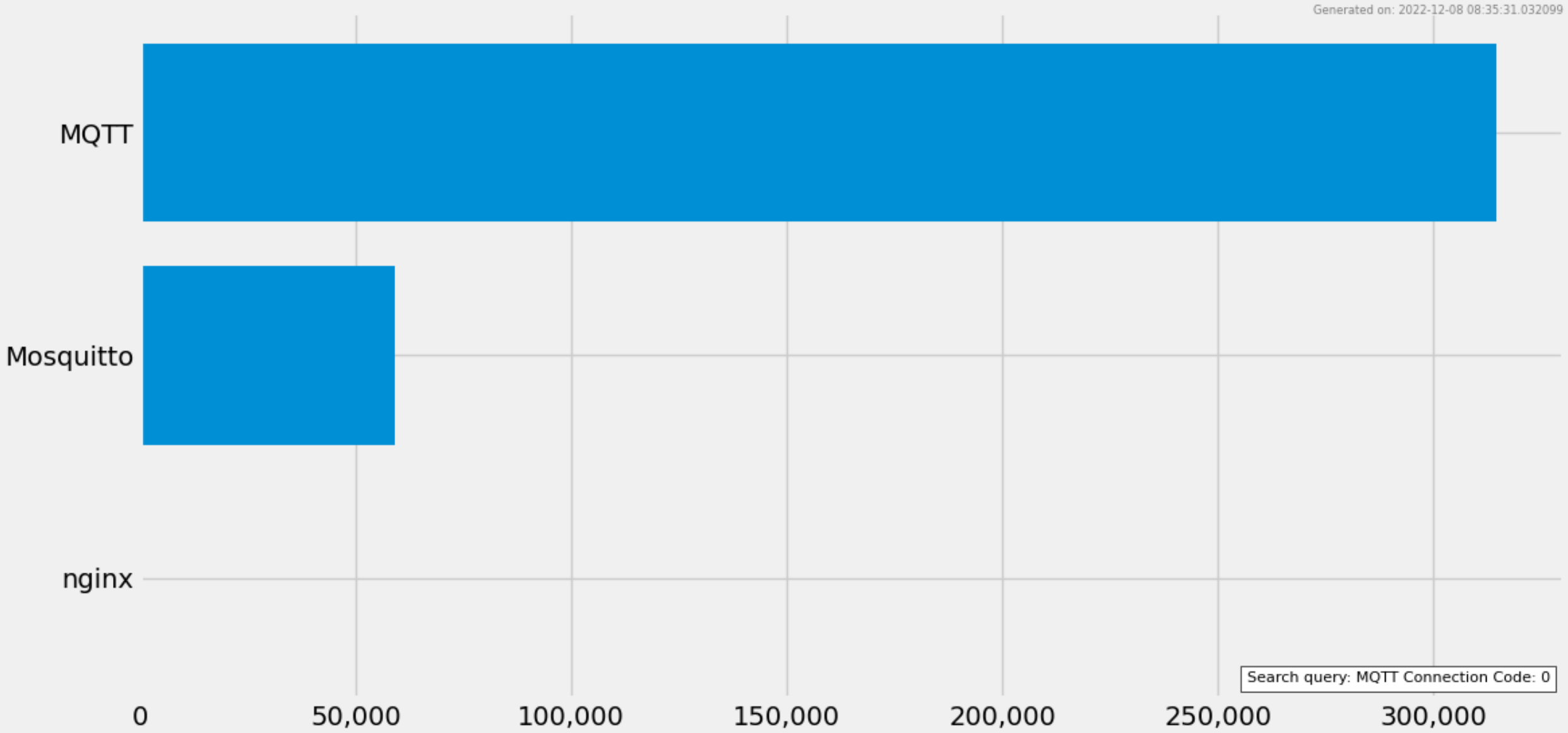
SHODAN

Top 10 Values for: isp

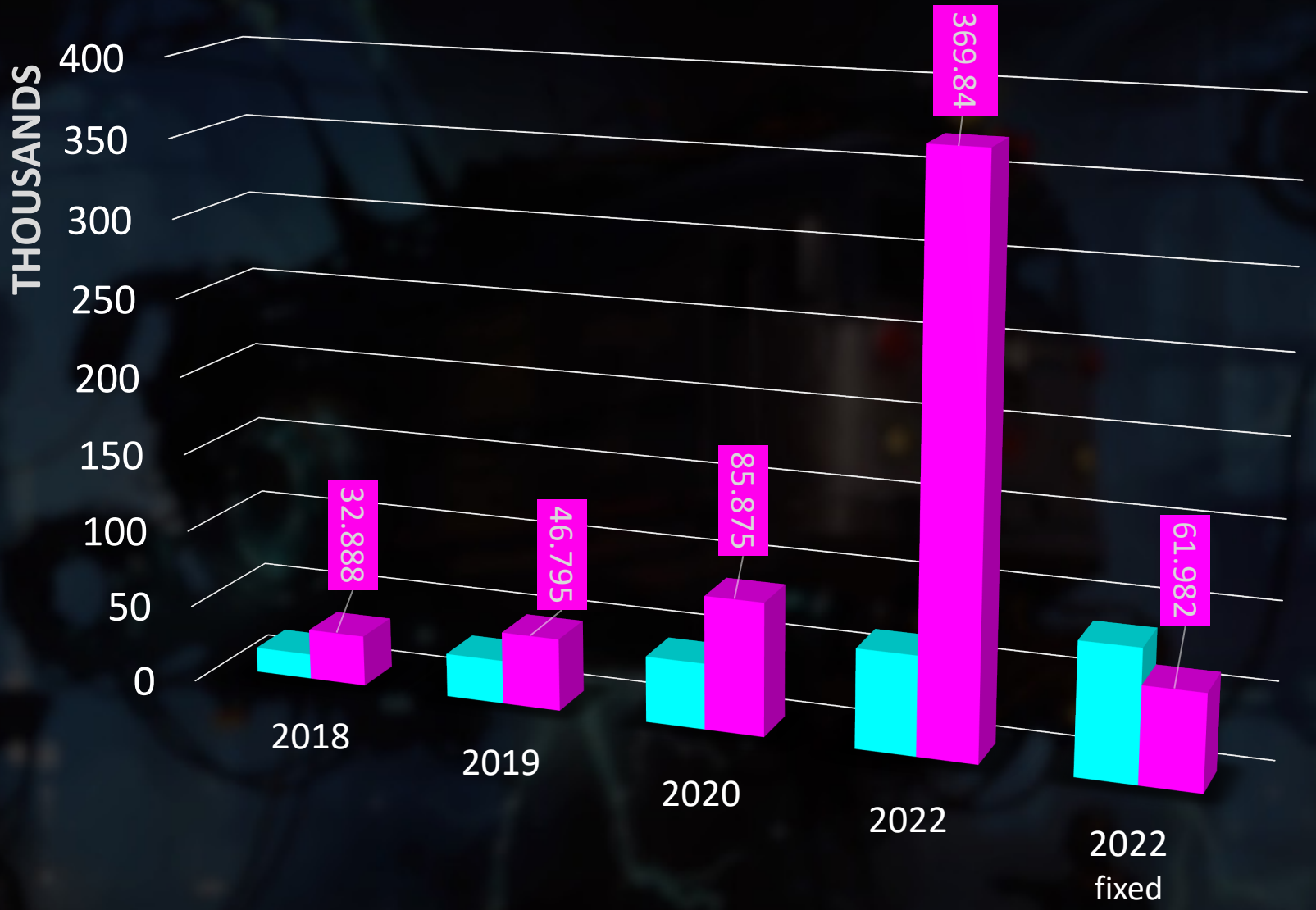


SHODAN

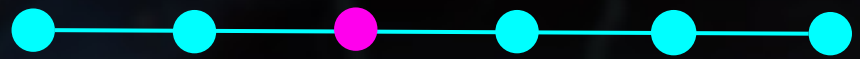
Top 10 Values for: product

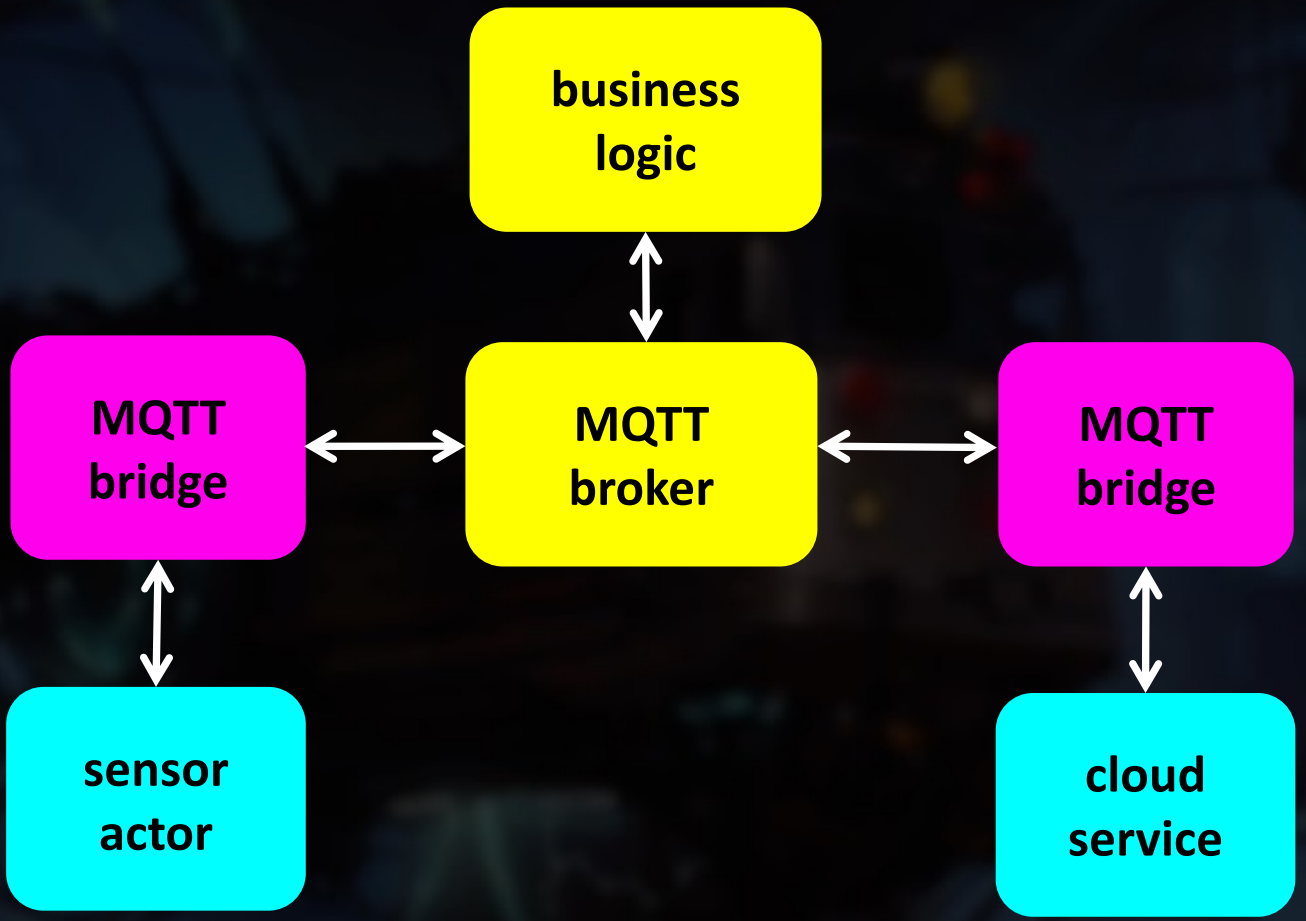


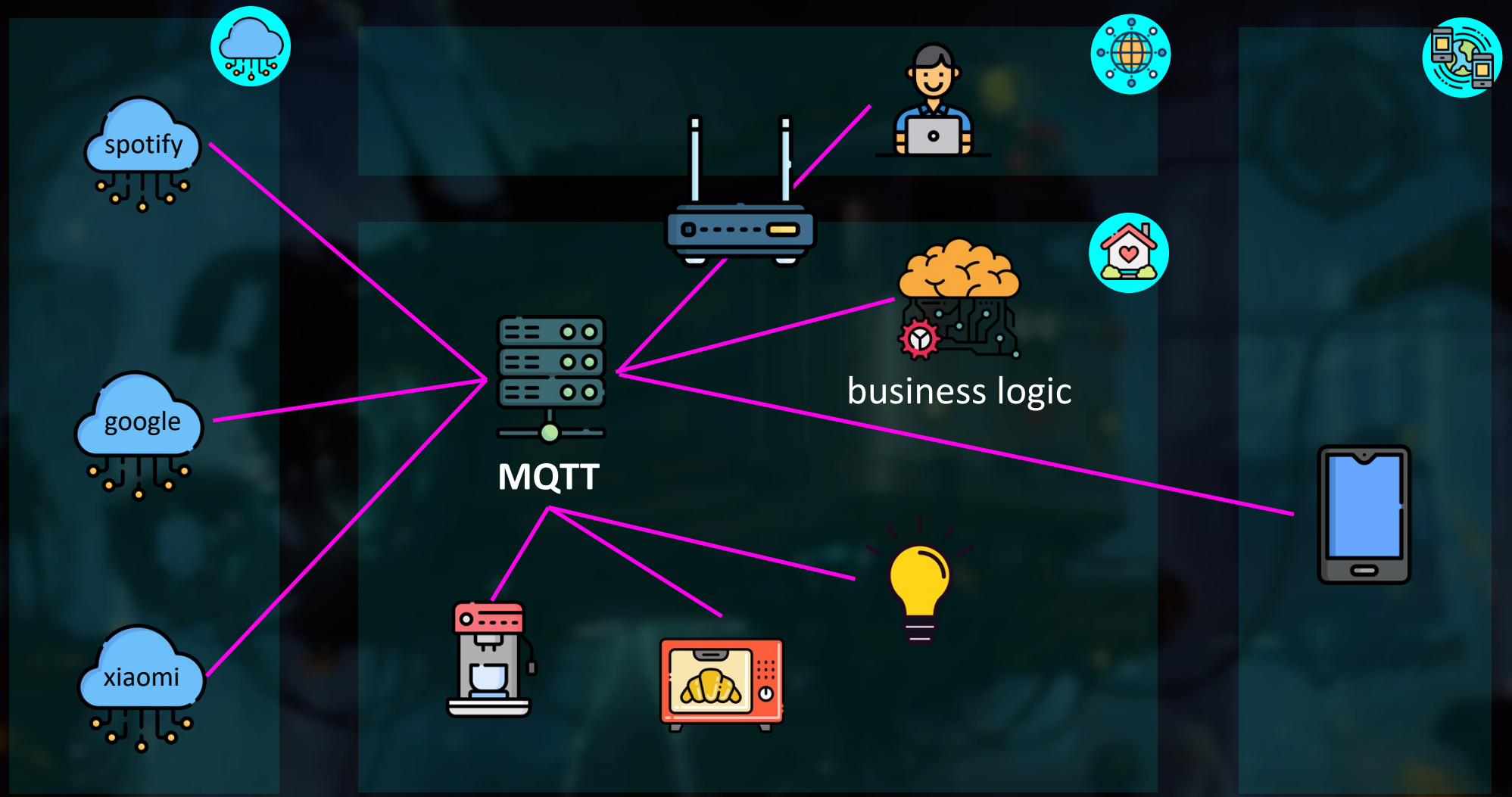
MQTT SERVERS OUT THERE

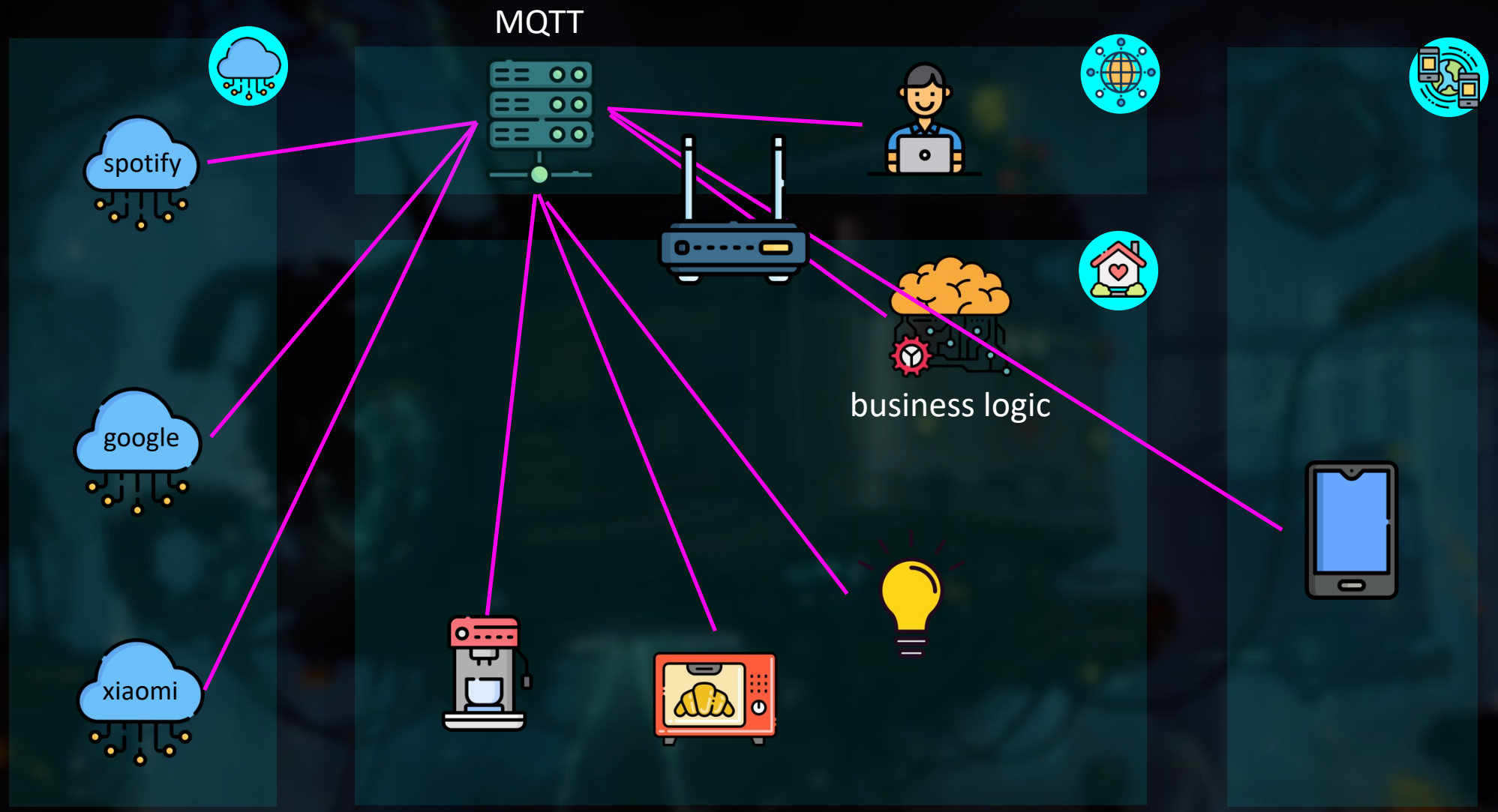


HOP ON THE TRAIN









SET CREDENTIALS

USE ACL

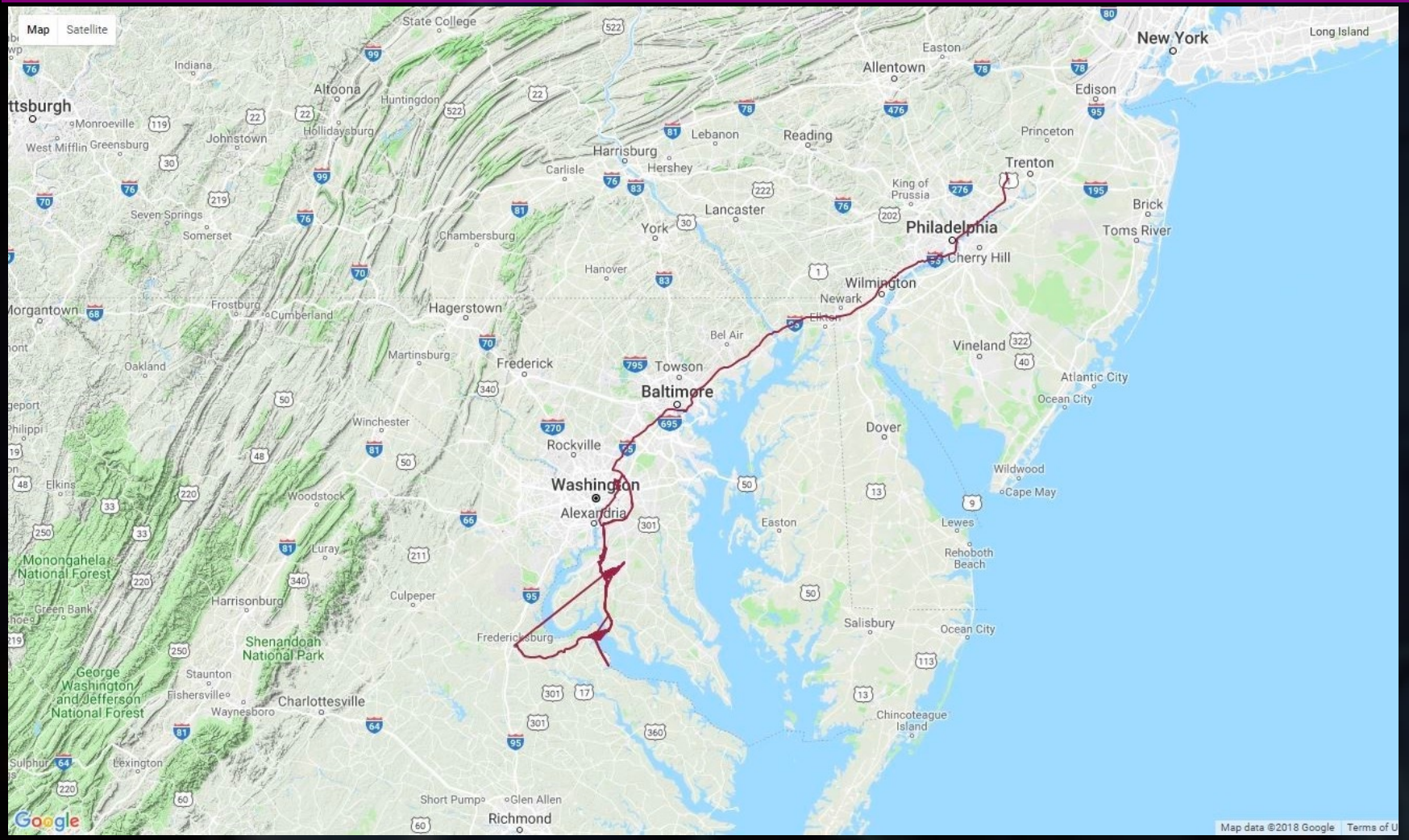
USE TLS

HOP ON THE TRAIN

imgdata/RBS_Kosanica/Camera_Indoor_axis_cam_device/application/x-tar

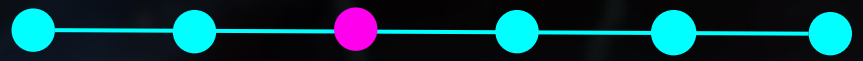
imgdata/RBS_Kosanica/Camera_Indoor_axis_cam_device/application/x-tar

owntracks/#

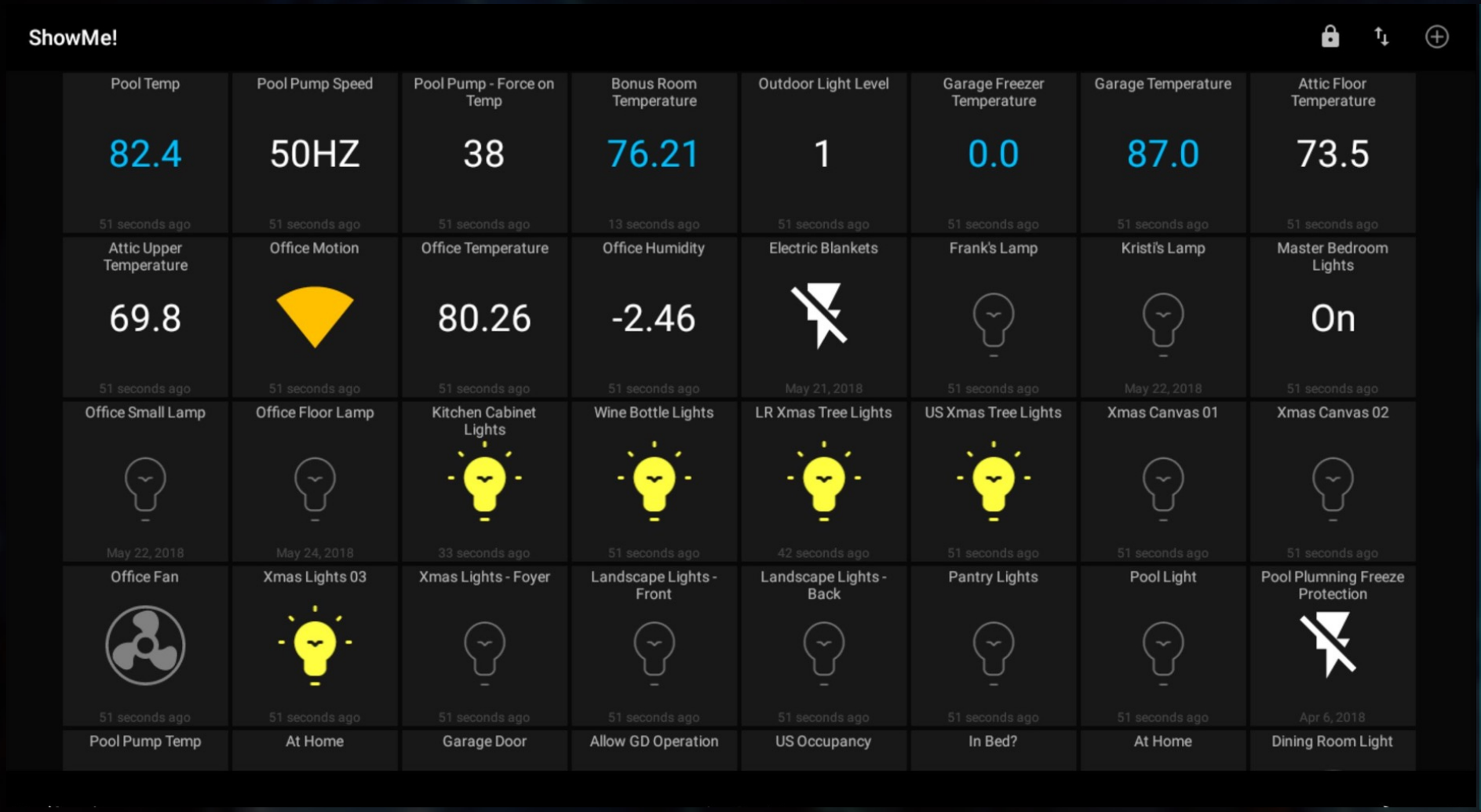


OWNTRACKS

HOP ON THE TRAIN

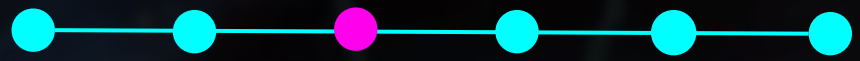


metrics/exchange



MQTT DASH

HOP ON THE TRAIN

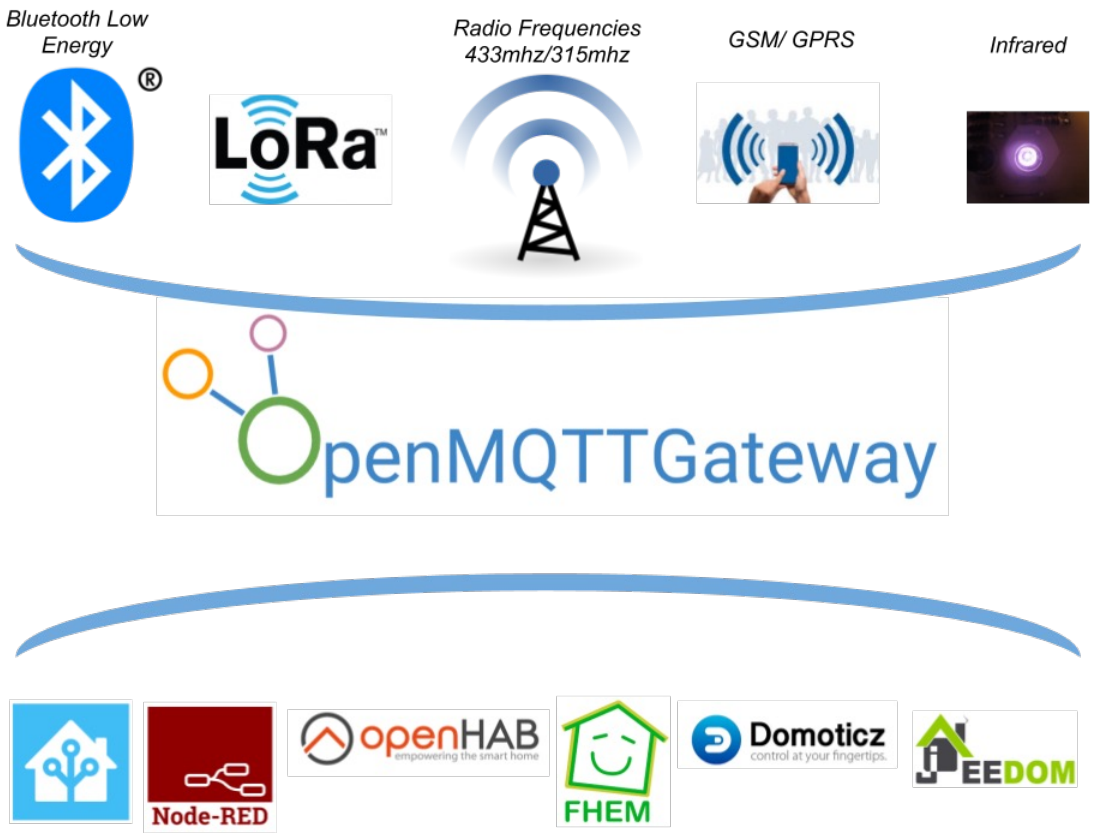


SET CREDENTIALS

USE ACL

USE TLS

HOP ON THE TRAIN


Bluetooth Low Energy
LoRa
Radio Frequencies 433mhz/315mhz
GSM/ GPRS
Infrared
OpenMQTTGateway
Node-RED
openHAB
empowering the smart home
FHEM
Domoticz
control at your fingertips.
EEDOM

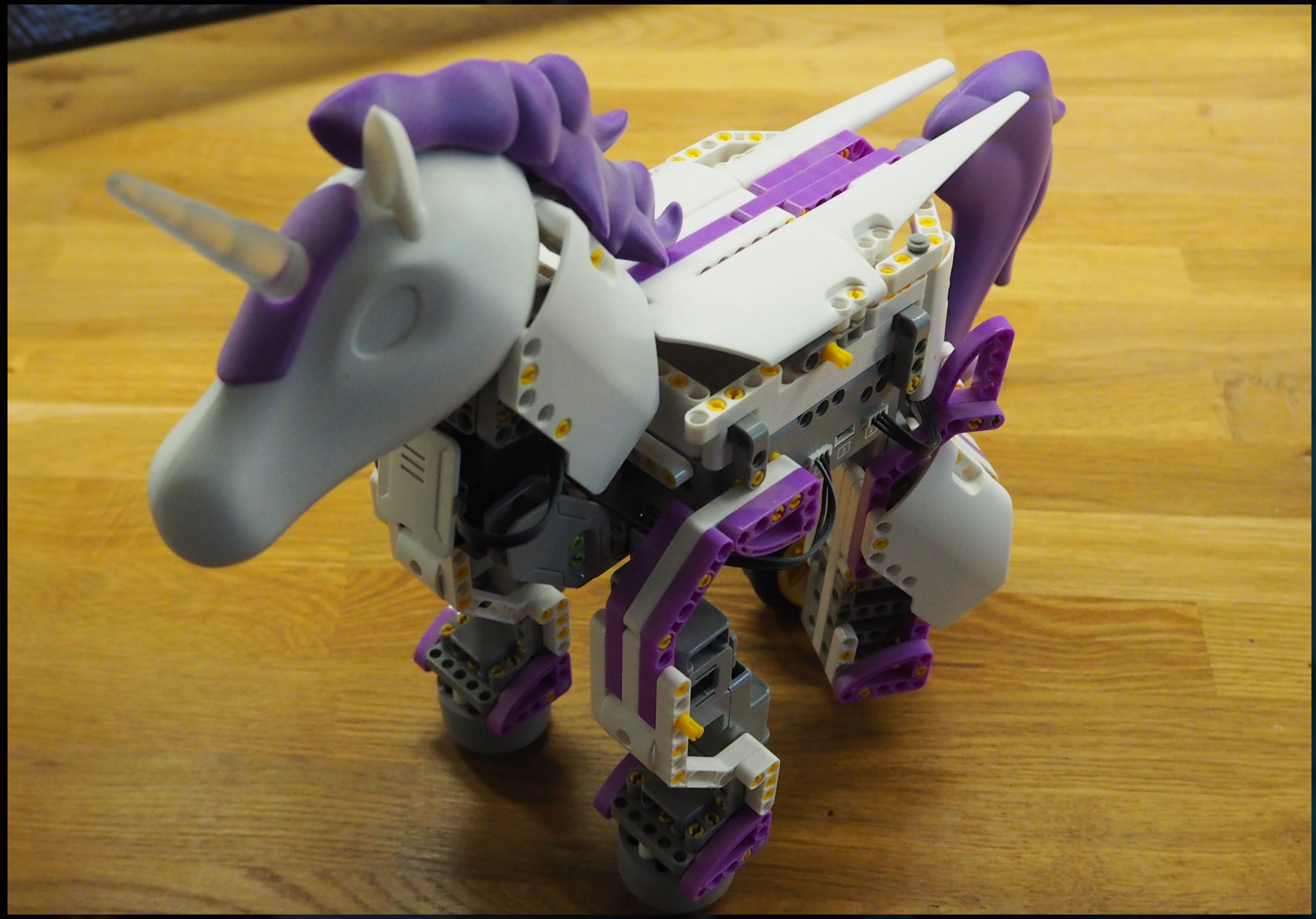
Read/write BLE characteristics over MQTT (ESP32 only)

The gateway can read and write BLE characteristics from devices and provide the results in an MQTT message.

> **TIP**
>
> These actions will be taken on the next BLE connection, which occurs after scanning and after the scan count is reached, see above to set this. This can be overridden by providing an (optional) parameter `"immediate": true` within the command. This will cause the BLE scan to stop if currently in progress, allowing the command to be immediately processed. All other connection commands in queue will also be processed for the same device, commands for other devices will be deferred until the next normally scheduled connection.
>
> **Note** Some devices need to have the MAC address type specified. You can find this type by checking the log/MQTT data and looking for "mac_type". By default the type is 0 but some devices use different type values. You must specify the correct type to connect successfully. To specify the MAC address type add the parameter `"mac_type"` to the command. For example `"mac_type": 1` to connect with a device with the MAC address type of 1.

Example write command

```
mosquitto_pub -t home/OpenMQTTGateway/commands/MQTTtoBT/config -m '{
  "ble_write_address":"AA:BB:CC:DD:EE:FF",
  "ble_write_service":"cba20d00-224d-11e6-9fb8-0002a5d5c51b",
  "ble_write_char":"cba20002-224d-11e6-9fb8-0002a5d5c51b",
  "ble_write_value":"TEST",
  "value_type":"STRING",
  "ttl":4,
  "immediate":true }'
```



BREED

UNICORNBOT

SPECIAL SKILLS

RGB HORN

SERVOS

SPEAKS BLE

```
[>] home/OpenMQTTGateway_BH/LWT
    online
[>] home/OpenMQTTGateway_BH/version
    version_tag
[>] home/OpenMQTTGateway_BH/SYStoMQTT
    {"uptime":371,"version":"version_tag","freemem":144624,"mqttport"
:"1883","mqttsecure":false,"freestack":4660,"rssi":-14,"SSID":"demo-w
ifi","BSSID":"D6:CA:6D:D0:89:1D","ip":"192.168.88.252","mac":"24:6F:2
8:25:13:34","lowpowermode":0,"btqblck":0,"btqsum":61,"btqsnd":61,"btq
avg":1,"interval":55555,"scanbcnct":10,"scnct":0,"modules":["BT"]}
```

0 ~ 1 python3

```
martin at bumblebee in ~ 22-12-05 - 14:51:15
[py3]-o
```

2 ~

Open source firmware for ESP8266 devices

Total local control with quick setup and updates.
Control using MQTT, Web UI, HTTP or serial.
Automate using timers, rules or scripts.
Integration with home automation solutions.
Incredibly expandable and flexible.

For OTA updates please use the new server http://ota.tasmota.com/tasmota and http://ota.tasmota.com/tasmota32

Download Tasmotizer v1.1c to use the new OTA server during flashing.

Tasmota Supported Devices Repository

2528 supported devices submitted by you!

Recently added:

AZzardo 10W RGBCCT Bulb AZ3213

AZzardo Led Vintage CCT Bulb AZ3210

Petoneer Smart Dot Cat Toy TY011 - DIY Replacement

Swisstone SH 310 CCT Bulb SH 310

Devices by electrical standard:

ALL DEVICES

AU | BR | CH | CN | EU

FR | GLOBAL | IL | IN | IS

IT | JP | UK | US | ZA

Light Bulbs by base:

B22 | B22 | E12 | E14 | E26

E26 | E27 | G4 | GU10

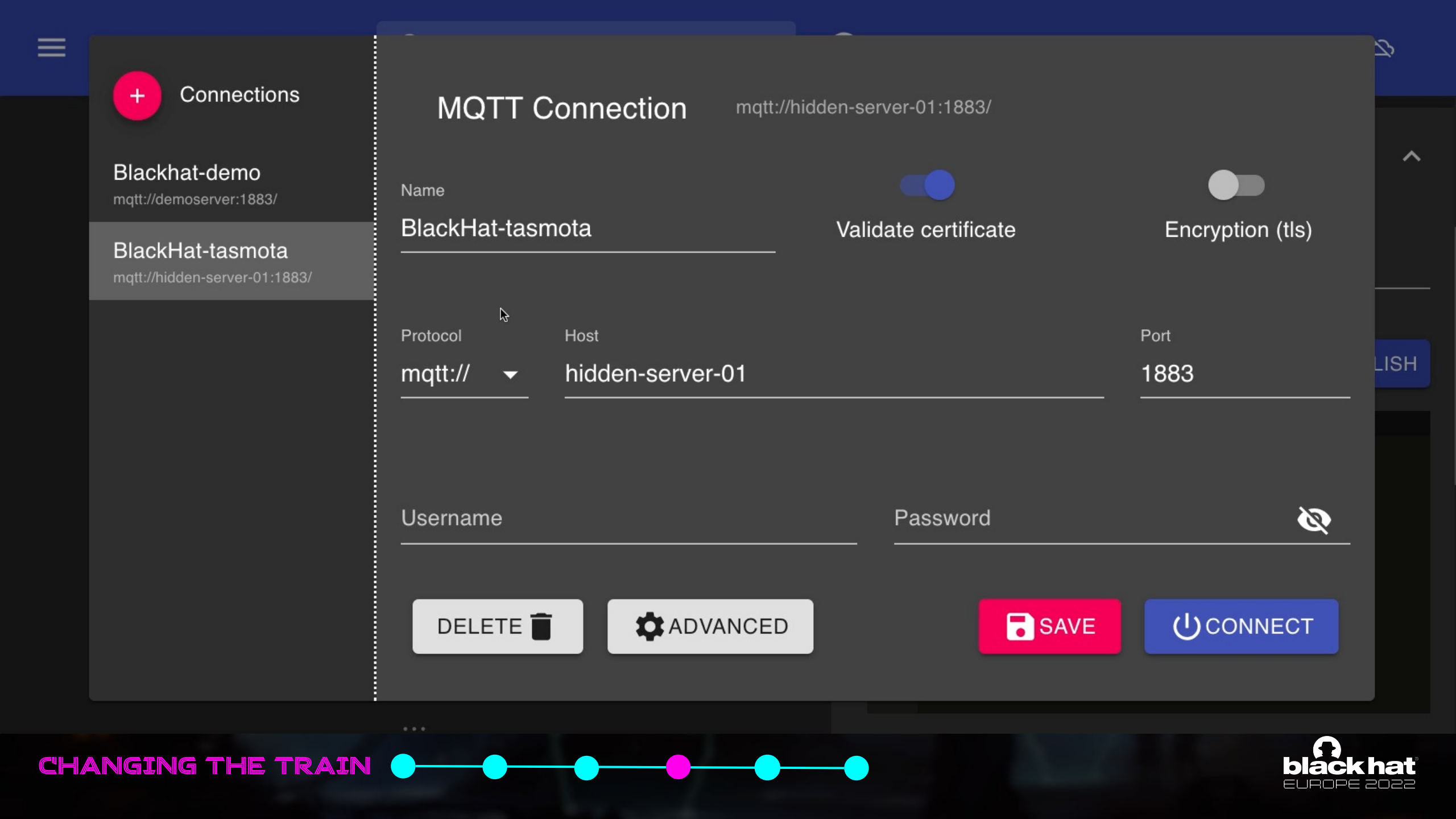
GU5.3 | GX53 | MR16

See world map of plugs and light bulb base list for more information.

GroupTopic

Having two devices with the same topic allowed for MQTT commands to be sent once to make the devices act in conjunction. That inspired a third topic called GroupTopic. Devices with the same GroupTopic will all listen to that GroupTopic and react to the same MQTT command sent to it. You can use this to take global actions like updating firmware on all devices or split up devices into different groups using a unique GroupTopic for each group.

Default GroupTopic is `tasmotas`


Connections
Blackhat-demo
mqtt://demoserver:1883/
BlackHat-tasmota
mqtt://hidden-server-01:1883/
MQTT Connection
mqtt://hidden-server-01:1883/
Name
BlackHat-tasmota
Validate certificate
Encryption (tls)
Protocol
mqtt://
Host
hidden-server-01
Port
1883
Username
Password
DELETE
ADVANCED
SAVE
CONNECT

WebSend	Send a command to Tasmota host over http. If a command starts with a `/` it will be used as a link.
	`[<host>:<port>,<user>:<password>] <command>`
	`<host>` = hostname or IP address.
	`<port>` = port for the device if not the default `80`
	`<user>` = enter username of the device you're sending the command to
	`<password>` = enter password of the device you're sending the command to
	`<command>` = command and payload
	example 1: `[<ip>] POWER1 ON` *sends* `http://<ip>/cm?cmnd=POWER1 ON`
	example 2: `WebSend [myserver.com] /fancy/data.php?log=1234` *sends* `http://myserver.com/fancy/data.php?log=1234`

```
root@acme:~#
```

```
  0 root@92.38.163.119
```

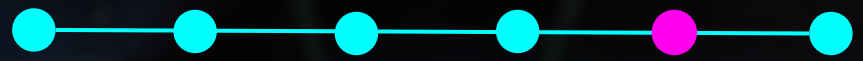
```
martin at bumblebee in ~ 22-12-05 - 10:43:43
```

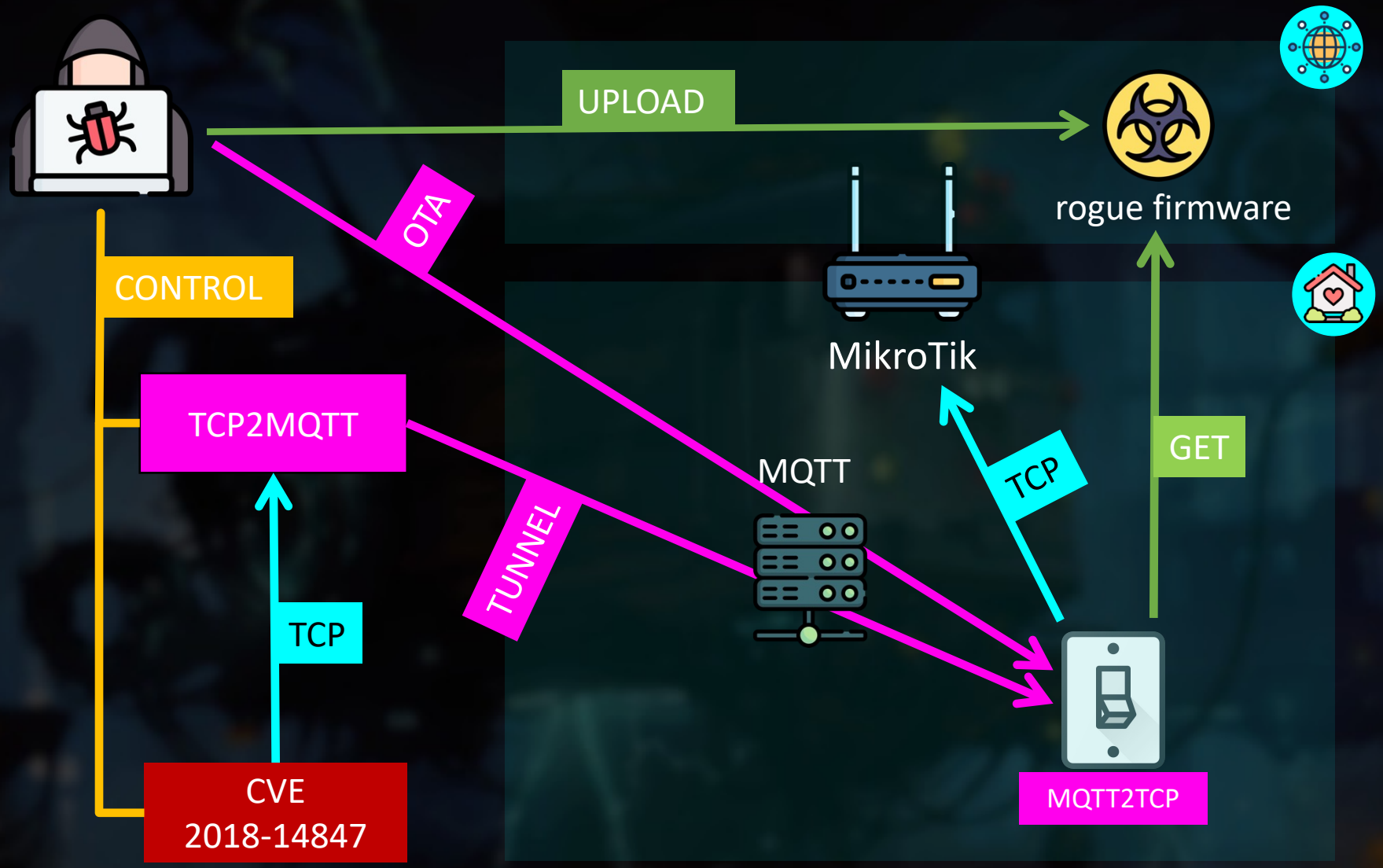
```
  1 ~
```

FREDDY THE TRAIN

OtaUrl	Display current OTA URL `1` = Reset OtaUrl to firmware default `url` = set address for OTA (100 char limit)

Upgrade	`1` = download firmware from `OtaUrl` and restart `<value>` = download firmware from `OtaUrl` if <value> is higher than device version






SONOFF


Power
hAP
LAN
PoE out

xdrv_01_webserver.ino — tasmota-rogue-fw

xdrv_01_webserver.ino 4, M

tasmota > xdrv_01_webserver.ino

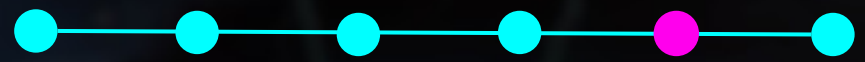
```
3409    &CmndEmulation,
3410  #endif
3411  #ifdef USE_SENDMAIL
3412    &CmndSendmail,
3413  #endif
3414    &CmndWebServer, &CmndWebPassword, &CmndWeblog, &CmndWebRefresh, &CmndWebSend, &CmndWebColor,
3415    &CmndWebSensor, &CmndWebButton, &CmndCors, &CmndTCPConnect, &CmndTCPSend, &CmndTCPClose };
3416
3417  /*********************************************************************************************\
3418   * Commands
3419  \*********************************************************************************************/
```

```
root@rogue:~#
```

```
[>] tele/demo-switch/LWT
    Online
```

```
  0 root@92.38.163.119                                  2 python
martin at bumblebee in ~ 22-12-05 - 11:24:01
```

```
  1 ~
```

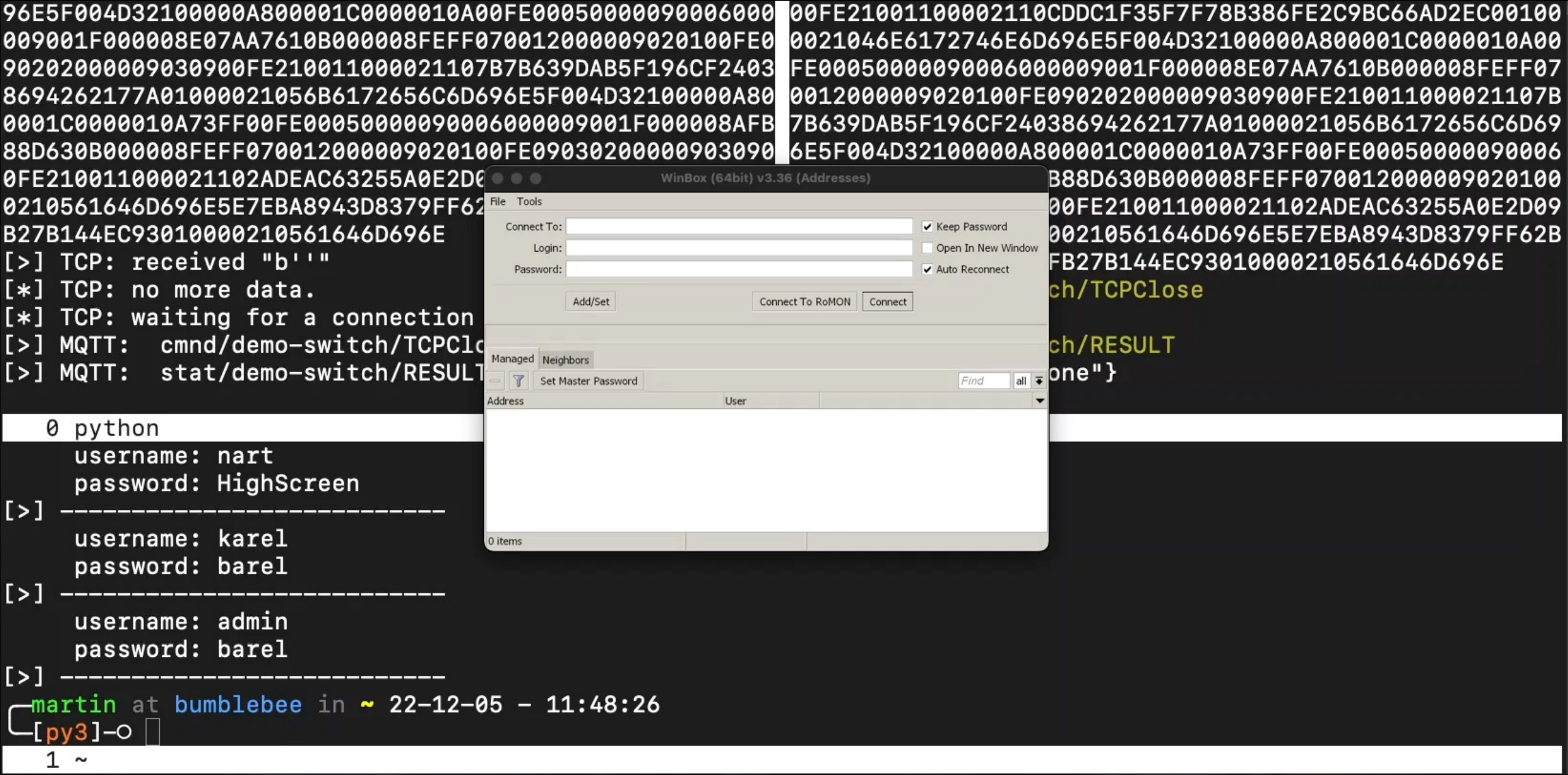
```
martin at bumblebee in ~ 22-12-05 - 11:43:30
[py3]-o
```

```
[>] tele/demo-switch/LWT
    Online
```

```
 0 ~                                                    2 python
```

```
martin at bumblebee in ~ 22-12-05 - 11:46:21
[py3]-o
```

```
 1 ~
```



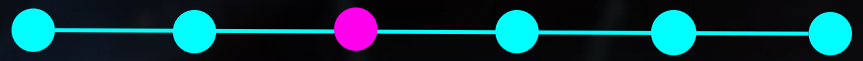
SET CREDENTIALS

USE ACL

USE TLS

HOP ON THE TRAIN

ALWAYS SECURE YOUR MQTT



HOP ON THE TRAIN

AS THE RISKS COULD BE "HIGH"

lab/webcams/feed01/snapshot_1m

THANK YOU & QA

References:

Tools and PoC	https://github.com/thinkcz/tasmota_tcp2mqtt
Shodan.io	http://shodan.io
Tasmota repo	https://tasmota.github.io/docs
Welcome home! @Bsides Manchester	https://www.youtube.com/watch?v=QX09BFAZqic
MQTT Explorer	https://mqtt-explorer.com/
Unsplash images	https://unsplash.com
Alejandro Burdisio	https://www.artstation.com/burda

Martin Hron (@thinkcz)
martin@hron.eu

BLACK HAT SOUND BYTES

DON'T DO DEFAULT...EVER

ALWAYS SECURE OTA CHANNEL

ALWAYS SETUP CREDENTIALS

CONTROL ACCESS AT THE HIGHEST POSSIBLE GRANULARITY