ARTEMIS

An Open-source tool for Detecting BGP prefix hijacking in Real-Time

Intro & Updates

RIPE 85
Belgrade, Serbia
24 - 28 October 2022

Lefteris Manassakis | COO, Code BGP

bgpartemis.org

Funded by RIPE NCC Community Projects

About me

Lefteris Manassakis

COO & co-founder | Code BGP

lefteris@codebgp.com

Lefteris Manassakis

Team

- Xenofontas Dimitropoulos
- Vasileios Kotronis
- Alexandros Kornilakis
- Korina Kalergi
- George Nomikos
- Pavlos Sermpezis
- Dimitris Mavrommatis
- Petros Gigis
- Alberto Dainotti
- Alistair King

ARTEMIS paper: IEEE/ACM Transactions on Networking, 2018

Organizations

Code BGP

FORTH
INSTITUTE OF COMPUTER SCIENCE

caida

ARTEMIS Design Goals

- **Real-time BGP observability**
- **Advanced BGP hijacking detection**
- **On-prem** operation to keep local information in-house
- **Custom UI** for better user experience
- **Modern software stack** for modularity & extensibility

ARTEMIS Overview

Data Sources

Public BGP feeds

RIS live

BGPstream

Your BGP routers

BGP/BMP

ARTEMIS

(on-prem)

Monitoring & detection

Exact-prefix type-0/1, path + policy violations, sub-prefix, squatting attacks

User

UI

Notifications
(slack/email/syslog)

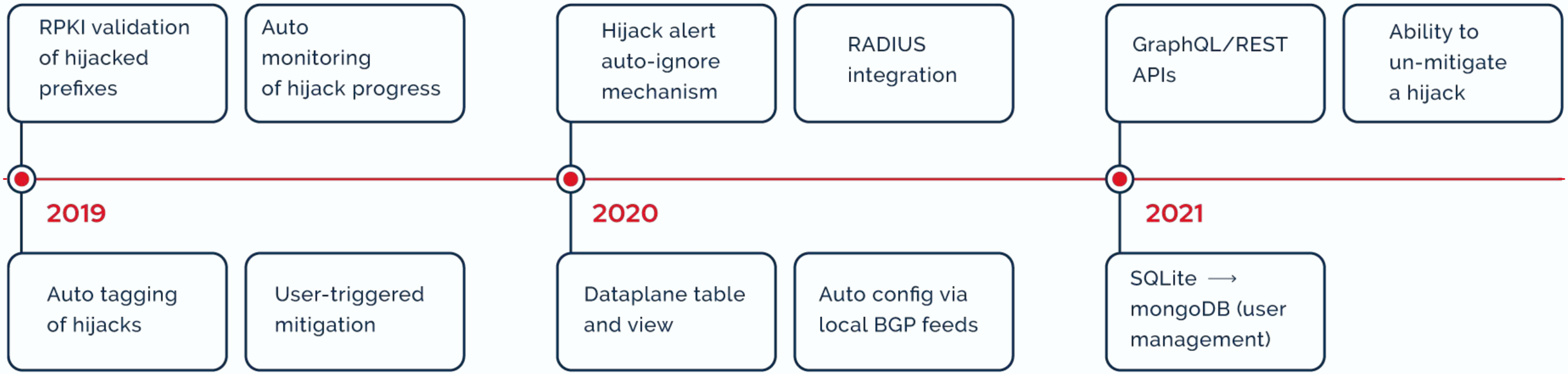
Configuration
(Yaml)

Code BGP

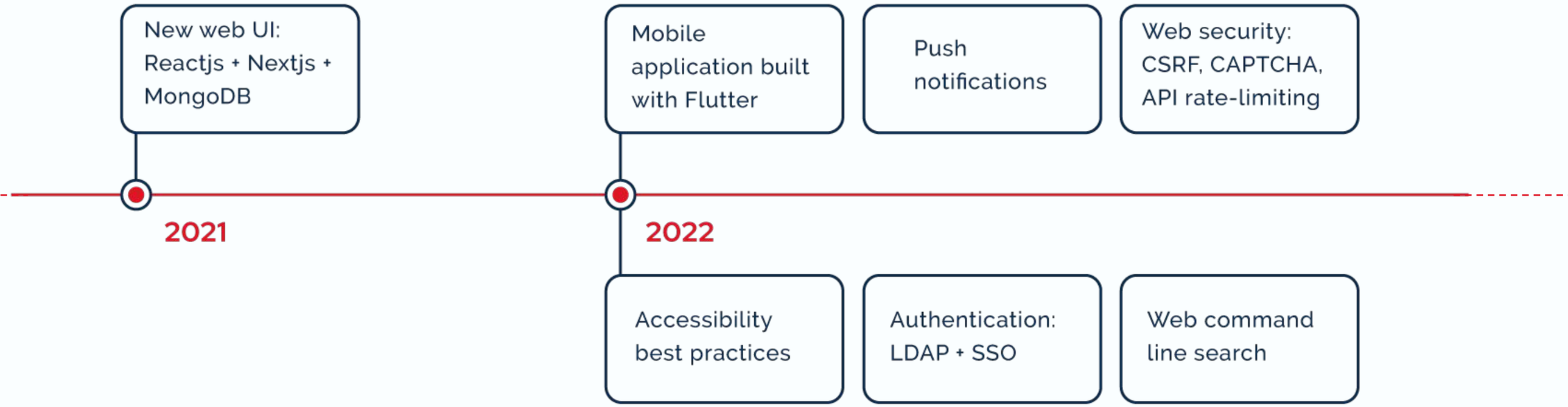
Software stack

Scalable & extendable design based on state-of-the-art technologies (microservices, etc.)

New features (Backend)



New features (Mobile & Frontend)



Future Work - RoadMap

- A command-line installation script that guides the user through setup
- Convert ARTEMIS to a Progressive Web Application (PWA)
- Add support for SAML2.0 authentication
- Build a lightweight version of ARTEMIS, ARTEMIS-Lite
  - A static web page
  - The application logic will run on the client-side
  - Will leverage WebAssembly to increase performance
- Extract and visualize container analytics with Telegraf and Grafana
  - Make remote debugging and user support more efficient
- Automate cloud deployment with “infrastructure as code” tools

ARTEMIS Users

- We are aware of ~25 organizations
- Support ~70 users in Slack workspace: bgpartemis.slack.com
- Deploy ARTEMIS: https://bgpartemis.org/

"ARTEMIS is a **fantastic** replacement for BGPmon.
All around it seems like **an incredibly well-built tool** and
I use it in prod all the time"

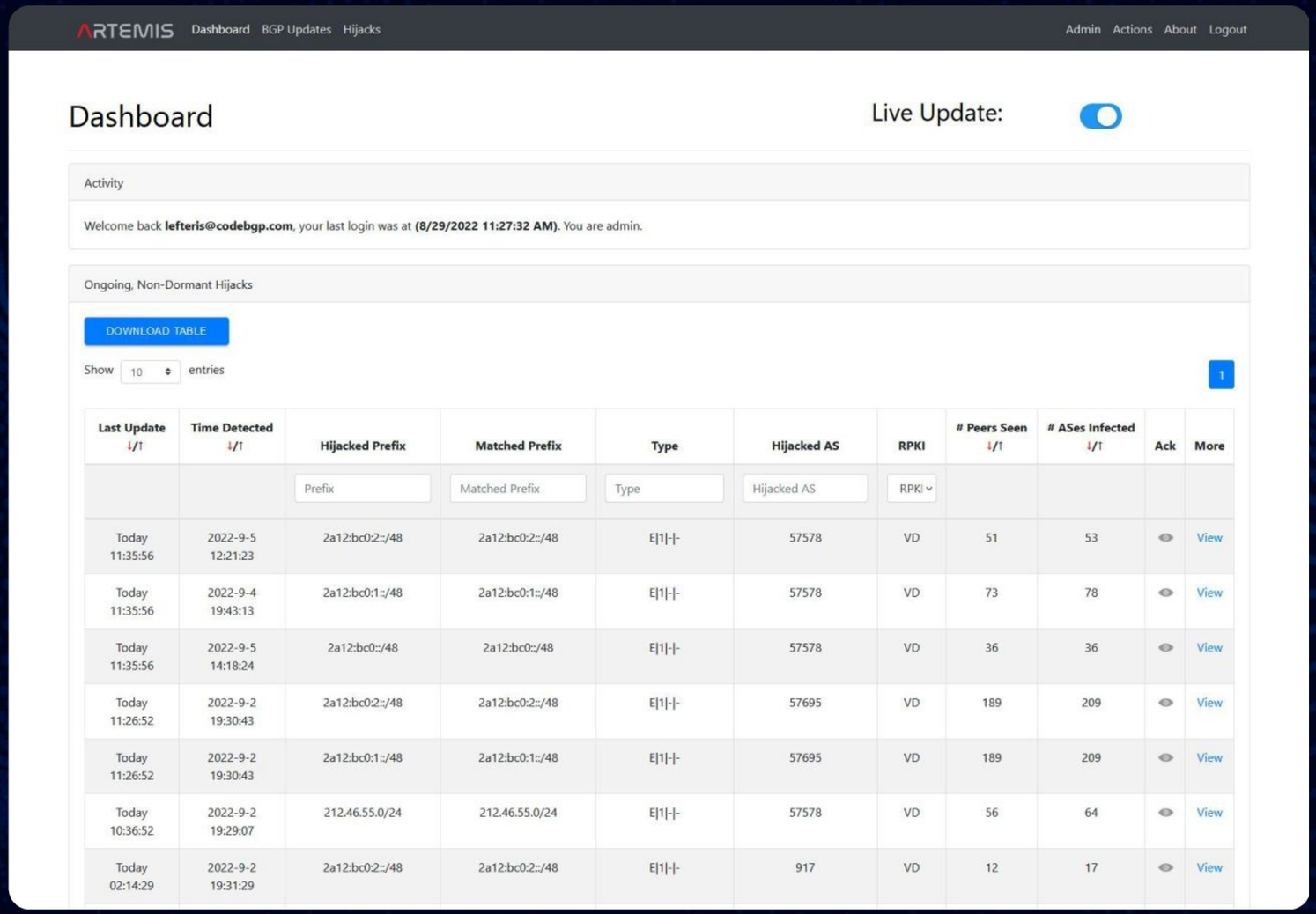
Chris Cummings
Network Engineer & modem.show podcast host

Demo

Try it:
https://demo.bgpartemis.org/

Live Demo:

- OS Working Group
- Wednesday, October 26



Questions

lefteris@codebgp.com

bgpartemis.org

bgpartemis.slack.com/