

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



Lfteris Manassakis

COO & co-founder | Code BGP

 leftieris@codebgp.com

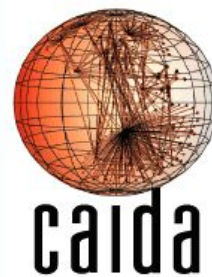
 [Lfteris Manassakis](#)

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



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



Your BGP routers

RIS live
BGPstream

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)

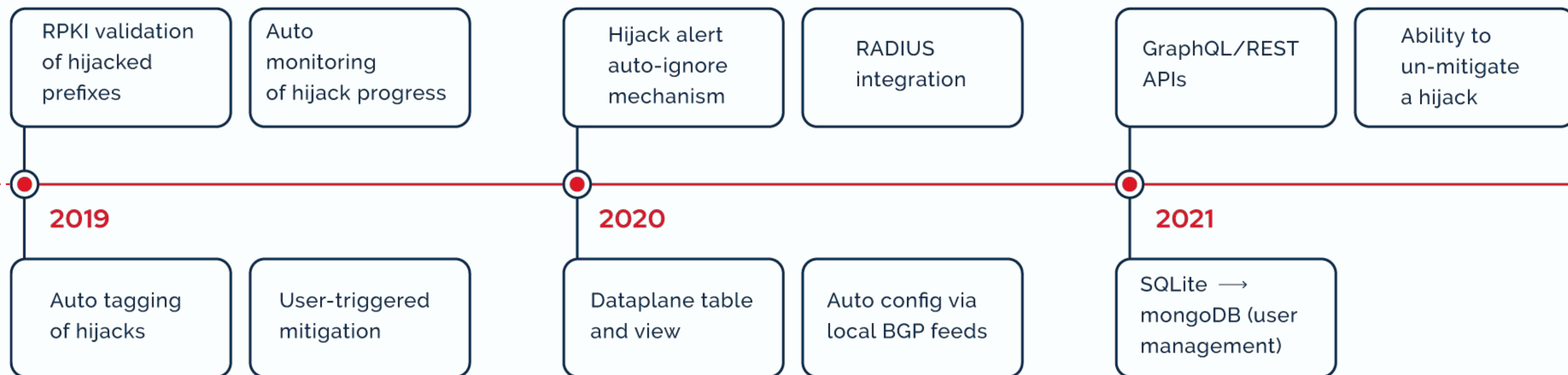


Software stack

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



New features (Backend)



New features (Mobile & Frontend)

New web UI:
Reactjs + Nextjs +
MongoDB



2021

Mobile
application built
with Flutter



2022

Push
notifications

Web security:
CSRF, CAPTCHA,
API rate-limiting

Accessibility
best practices

Authentication:
LDAP + SSO

Web command
line search

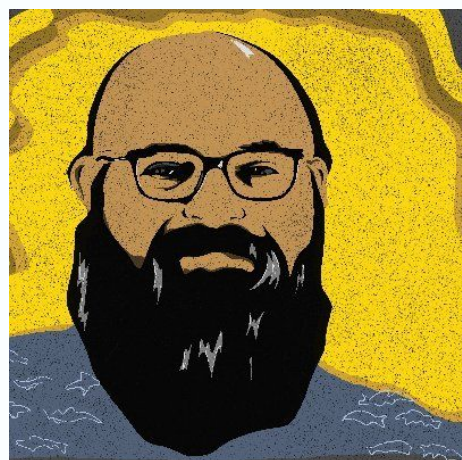
Future Work - RoadMap

- 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

The logo for ARTEMIS, featuring a stylized red 'A' followed by the word 'ARTEMIS' in white, all set against a dark blue background.

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.bgp.artemis.org/>

Live Demo:

- OS Working Group
- Wednesday, October 26

The screenshot shows the Artemis dashboard interface. At the top, there is a navigation bar with the Artemis logo and links for Dashboard, BGP Updates, Hijacks, Admin, Actions, About, and Logout. The main header includes the title 'Dashboard' and a 'Live Update' toggle switch which is currently turned on. Below the header, there is an 'Activity' section with a welcome message for the user 'lefteris@codebgp.com'. The main content area is titled 'Ongoing, Non-Dormant Hijacks' and features a 'DOWNLOAD TABLE' button and a 'Show 10 entries' dropdown. A table displays a list of hijacks with columns for Last Update, Time Detected, Hijacked Prefix, Matched Prefix, Type, Hijacked AS, RPKI, # Peers Seen, # ASes Infected, Ack, and More. The table contains 8 rows of data, each with a 'View' link in the 'More' column.

Last Update	Time Detected	Hijacked Prefix	Matched Prefix	Type	Hijacked AS	RPKI	# Peers Seen	# ASes Infected	Ack	More
Today 11:35:56	2022-9-5 12:21:23	2a12:bc0:2::/48	2a12:bc0:2::/48	E 1 -	57578	VD	51	53		View
Today 11:35:56	2022-9-4 19:43:13	2a12:bc0:1::/48	2a12:bc0:1::/48	E 1 -	57578	VD	73	78		View
Today 11:35:56	2022-9-5 14:18:24	2a12:bc0::/48	2a12:bc0::/48	E 1 -	57578	VD	36	36		View
Today 11:26:52	2022-9-2 19:30:43	2a12:bc0:2::/48	2a12:bc0:2::/48	E 1 -	57695	VD	189	209		View
Today 11:26:52	2022-9-2 19:30:43	2a12:bc0:1::/48	2a12:bc0:1::/48	E 1 -	57695	VD	189	209		View
Today 10:36:52	2022-9-2 19:29:07	212.46.55.0/24	212.46.55.0/24	E 1 -	57578	VD	56	64		View
Today 02:14:29	2022-9-2 19:31:29	2a12:bc0:2::/48	2a12:bc0:2::/48	E 1 -	917	VD	12	17		View

Questions



 lfteris@codebgp.com

 bgpartemis.org

 bgpartemis.slack.com/