Herramientas para visualizar información de enrutamiento

Conocer y detectar incidentes de ruteo

Contexto - Proyecto FORT

Iniciativa conjunta de LACNIC y NIC.MX.

Objetivos:

- ➔ Potenciar el despliegue de RPKI.
- ➔ Detectar y prevenir secuestros de rutas.
- ➔ Desarrollar herramientas afines.

`fortproject.net`

Contexto - Proyecto FORT

- ➔ Validador RPKI de código abierto.
- ➔ Permite validar la información de enrutamiento BGP.
- ➔ https://github.com/NICMx/FORT-validator

Contexto - Proyecto FORT

- ➔ Recolecta y unifica datos sobre incidentes de ruteo.
- ➔ Expone esta información:
  - facilitando la identificación y clasificación.
  - con diferentes niveles de complejidad /para diferentes perfiles de usuarios.

Contexto - Monitoreo FORT

- ¿Cómo recolectar los datos?
- ¿Cómo detectar secuestros?
- ¿Cómo integrar RPKI a toda esta información?

BGPStream - Presentación

- ➔ Framework de código abierto que permite el análisis histórico y en tiempo real de datos BGP.
- ➔ Desarrollado por CAIDA (Center for Applied Internet Data Analysis).
- ➔ Herramientas: BGPReader, BGPCorsaro.
- ➔ APIs: libBGPStream (C), PyBGPStream (Python) , Broker.

BGPReader - Presentación

Permite recolectar datos BGP de numerosas fuentes llamados colectores.

Permite consultar los datos filtrando por:

- proveedor (proyecto y colector) - (Route Views, RIPE RIS)
- tipo de datos - (ribs, updates)
- rango de fechas - Unix epoch
- ASN de origen / prefijo

BGPReader - Instalación y ejecución

- ➔ Instalación sencilla, guía paso a paso según S.O.
- ➔ Ejemplo:

Obtener toda la información BGP para un día específico de los prefijos de LACNIC de la fuente rrc00.

```
bgpreader -d broker -p ris -c rrc00 -t ribs -w $(date +%s
--date='Jun 23, 2018 0:00utc'),$(date +%s --date='Jun 23,
2018 23:59utc') -k 2001:1200::/23 -k 2800::/12 | tee
ipv6_lacnic_visible_20180623.csv
```

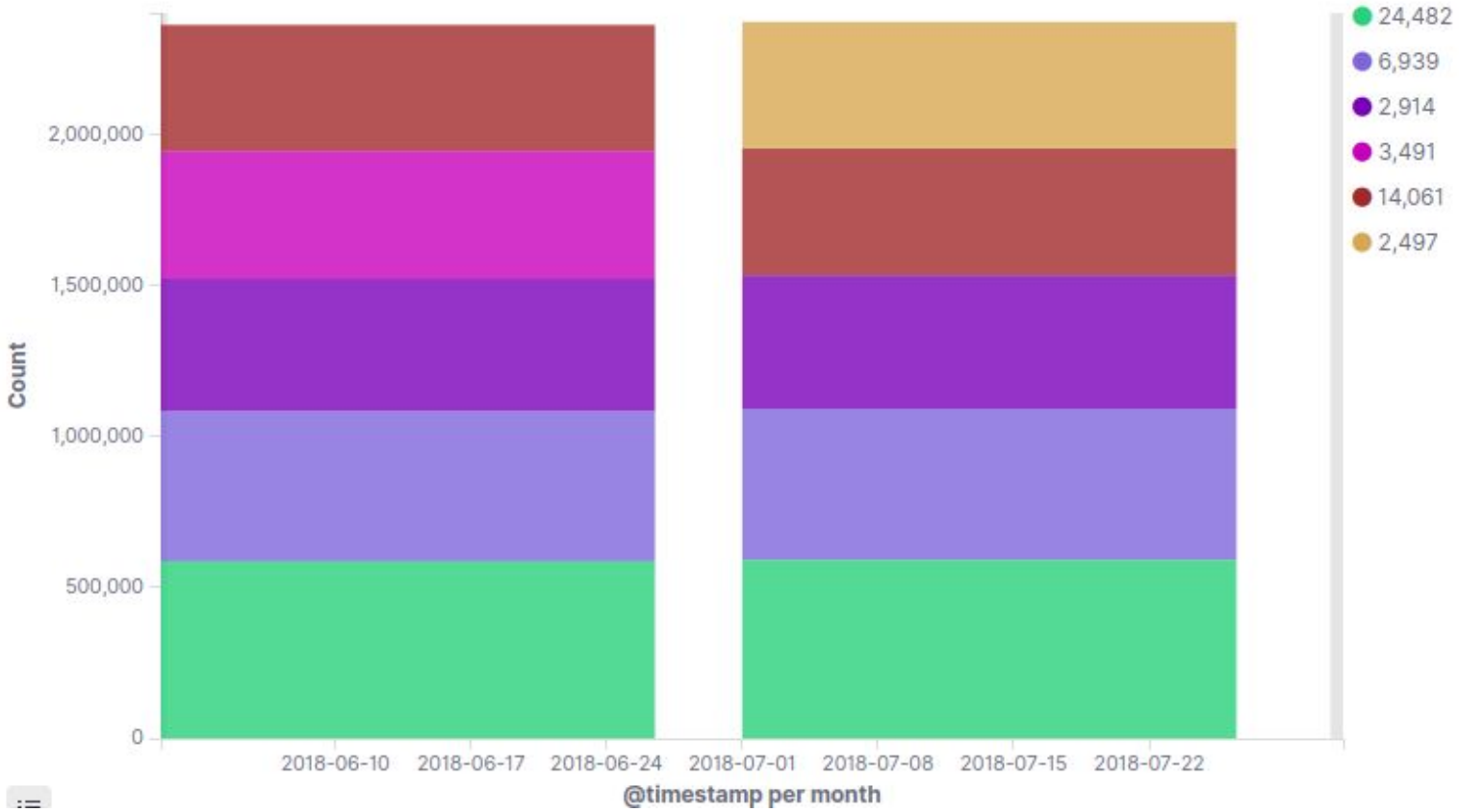
BGPReader - Ejemplos de uso

Obtener toda la información BGP para un día específico de los prefijos de LACNIC.

```
bgpreader -d singlefile -o $FILEFILTER -t ribs
-w $INIDATEFILTER,$FINDATEFILTER -k $LACNICPREIXFILTER |
tee $OUTPUTFILE
```

BGPReader - Resultados

BGPReader - Resultados



BGPReader - Problemas

- ➔ Enormes cantidades de datos a procesar.
- ➔ Varios colectores y diferentes accesos.
- ➔ Tiempos de respuesta lentos y variables.
- ➔ Pocos ejemplos en la documentación.

BGPReader - Soluciones

- ➔ Conocer mejor las fuentes para obtener los datos directamente.
- ➔ Descargar los datos y luego procesarlos localmente:
  - mayor control en los tiempos de ejecución.
  - mayor velocidad de procesamiento.
- ➔ Pruebas locales para experimentar parámetros y chequear datos.

ARTEMIS - Presentación

Herramienta de código abierto contra ataques de secuestro de prefijos BGP.

Desarrollada por el grupo INSPIRE y CAIDA.

Permite a un AS monitorear, detectar y mitigar eventos de secuestro en tiempo real.

Utiliza BGPStream.

ARTEMIS - Instalación y ejecución

- ➔ Instalación sencilla, guía de pasos (wiki).
- ➔ Requerimientos:
  - CPU: 4 cores / RAM: 4+ GB / HDD: 100 GB
  - Internet / Ubuntu Linux 16.04+ / docker
- ➔ Configuración:
  - variables de entorno (por seguridad principalmente).
  - ARTEMIS: fuentes, prefijos, ASNs y reglas.
- ➔ Luego se ejecuta docker-compose y accedemos a la web.

ARTEMIS - Ejemplos de uso

Monitoreo de prefijos de LACNIC para 2 AS en particular:

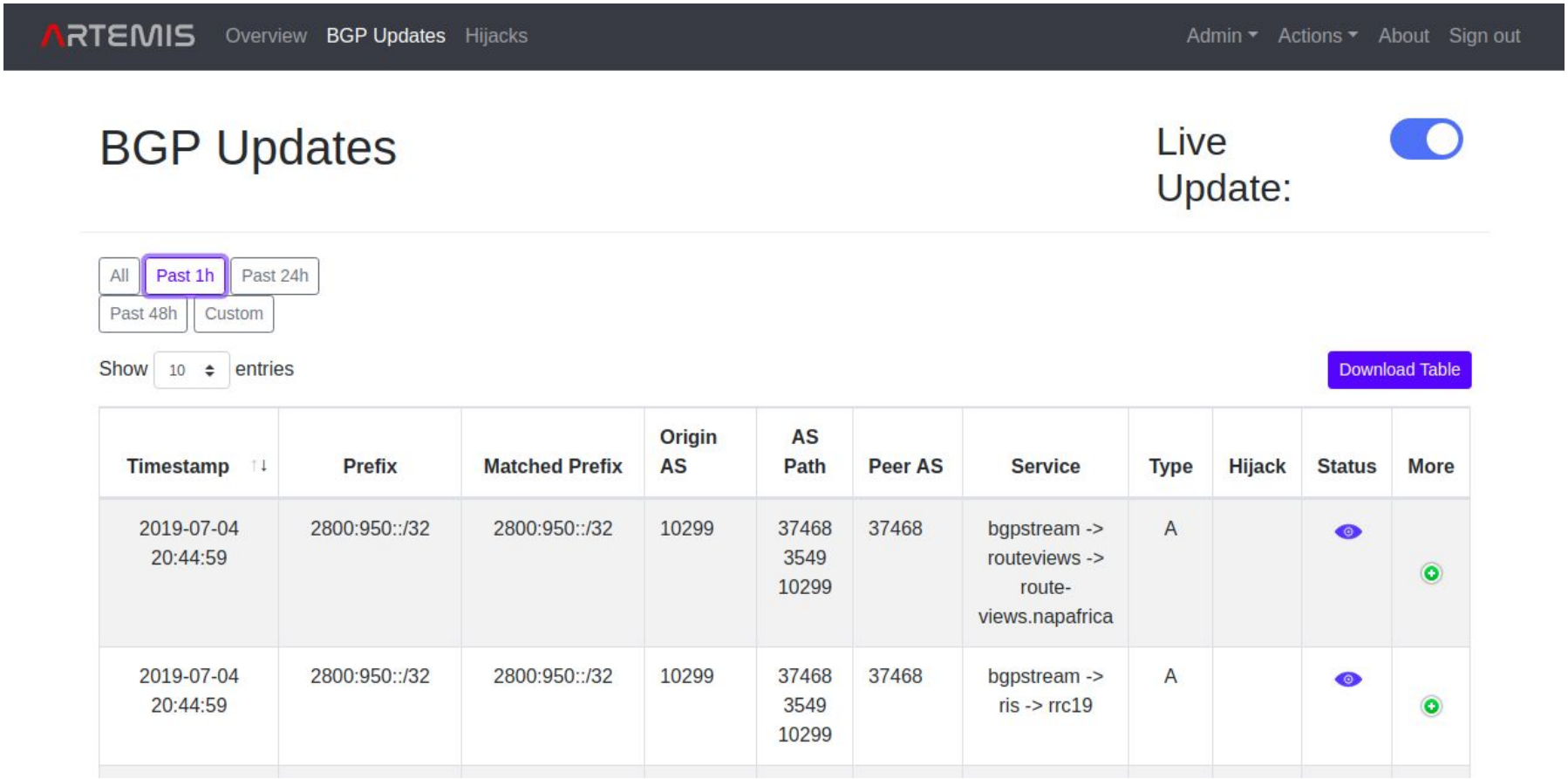
```
prefixes:
    AS28000_prefixes: &AS28000_prefixes
      - 2001:13c7:7001::/48
      - 200.7.87.0/24
      - ...

    Mi_AS_prefixes: &Mi_AS_prefixes
      - 200.10.60.0/23^23-24
      - 2800:620::/32^32-64
      - ..
```

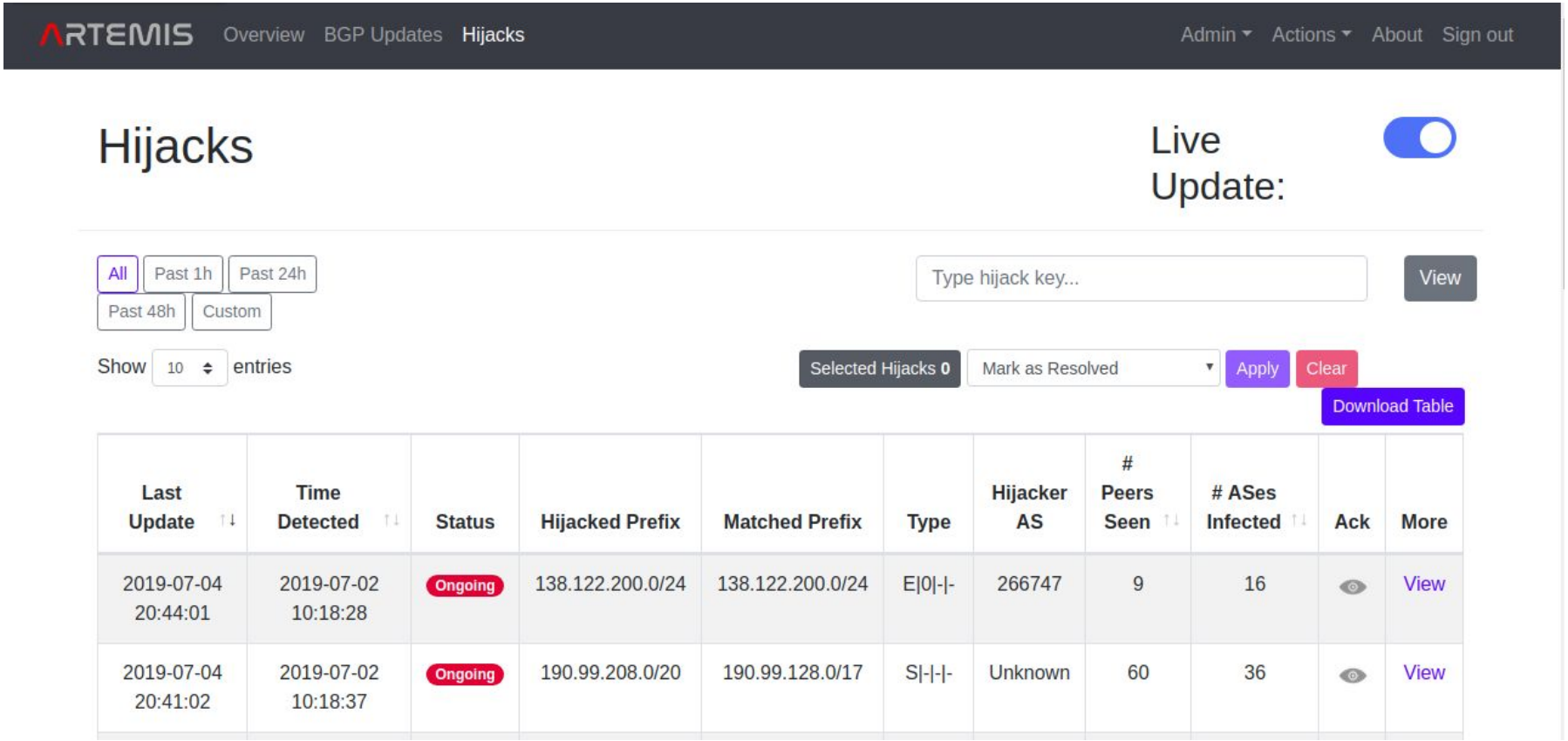
```
rules:
- prefixes:
    - *AS28000_prefixes
  origin_asns:
    - *AS28000

- prefixes:
    - *Mi_AS_prefixes
  origin_asns:
    - *Mi_AS
```

ARTEMIS - Ejemplos de uso



ARTEMIS - Ejemplos de uso



Monitoreo FORT

Recolección de upd BGP -> BGPStream.

Clasificación según ROV -> Validador FORT + rtrclient.

Clasificación y detección de incidentes -> heurísticas (quizás ARTEMIS).

Agregar información: ASRank, GeoLite2.

Monitoreo FORT

Con esta información integrada podemos:

- ➔ Exponer incidentes de ruteo.
- ➔ Documentar incidentes de forma periódica.
- ➔ Proveer información sobre seguridad de ruteo para tomadores de decisiones técnicos y no-técnicos.

Muchas gracias

Gerardo Pias

gerardo.pias@matesoft.com.uy