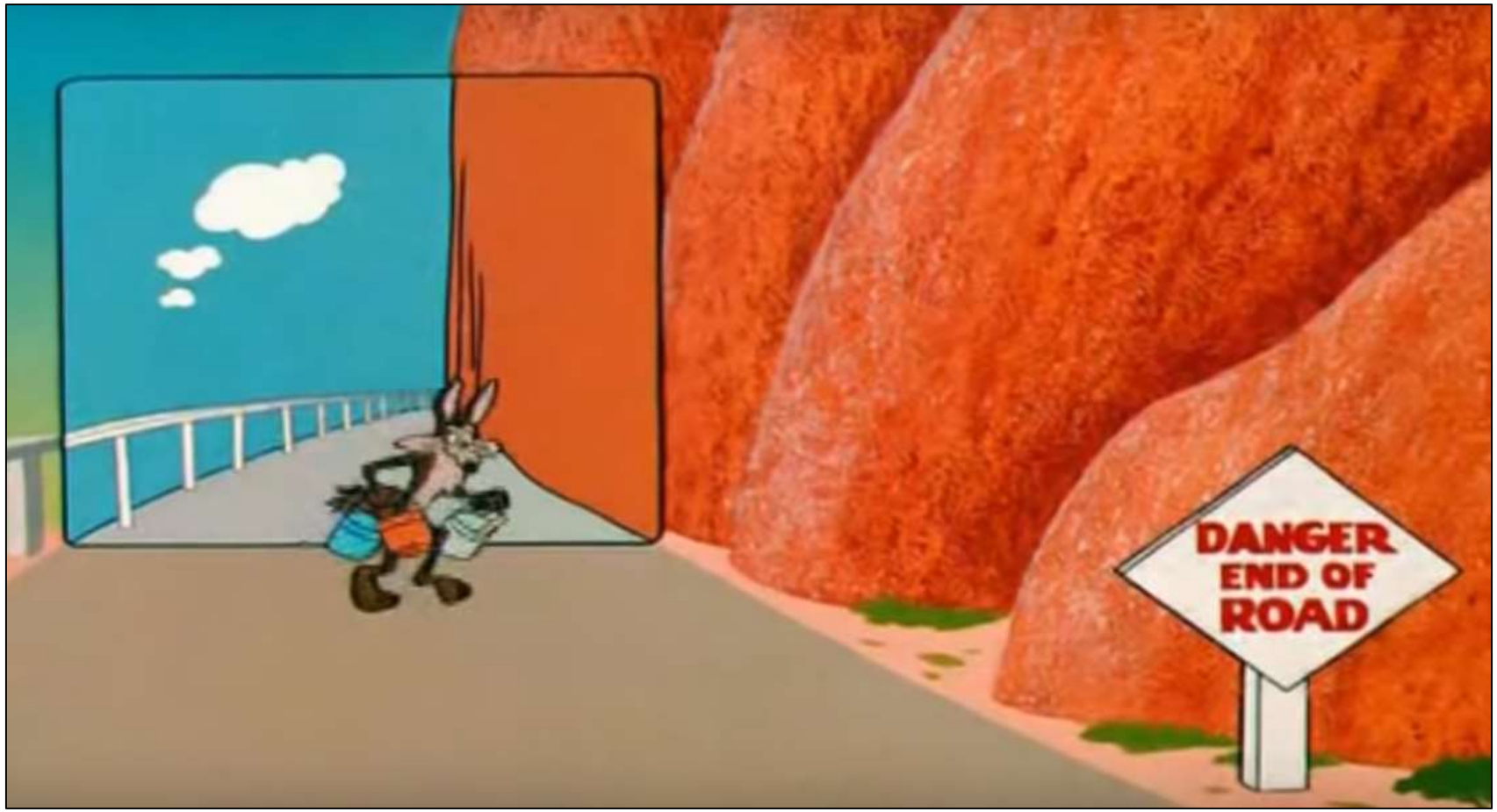
Reunión de Operadores de Redes México
Cd. de México
Agosto 2019

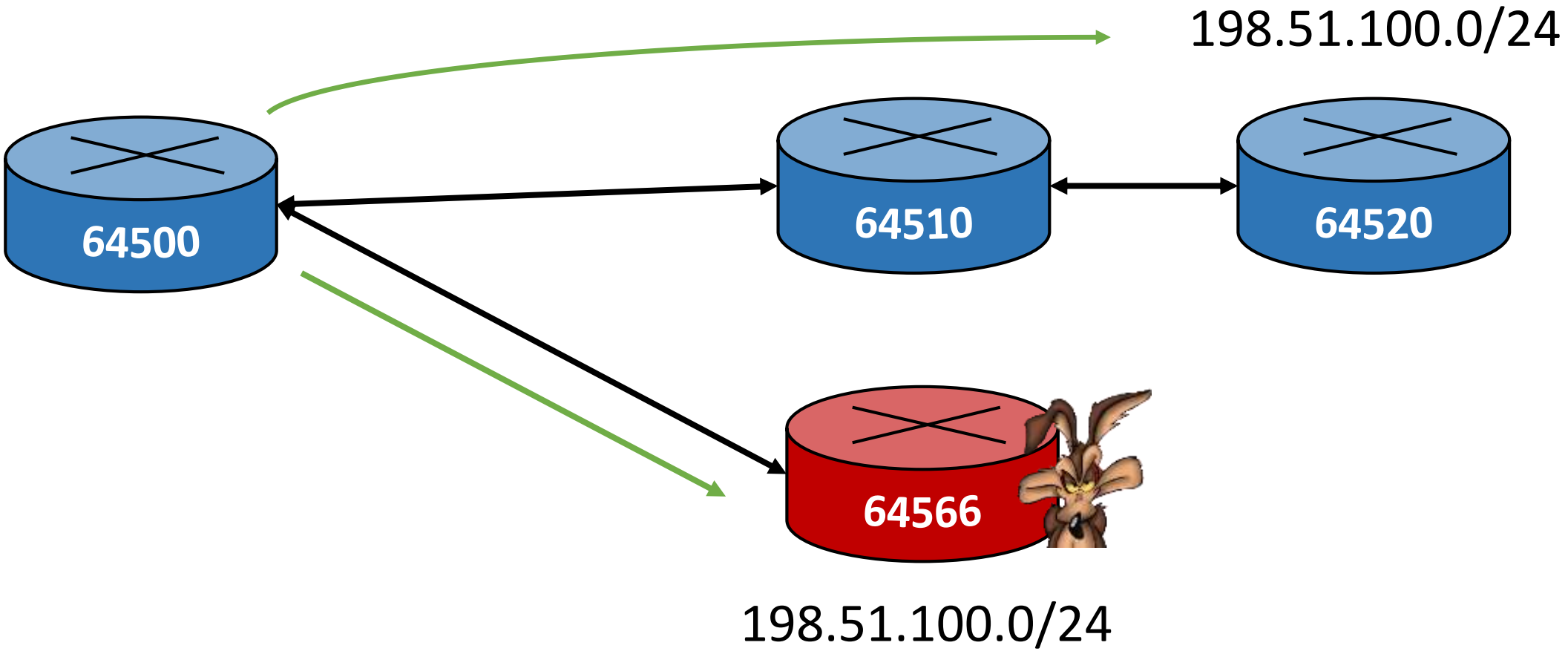
¿Cuál es el problema?

¿Cuál es el problema?

¿Cuál es el problema?

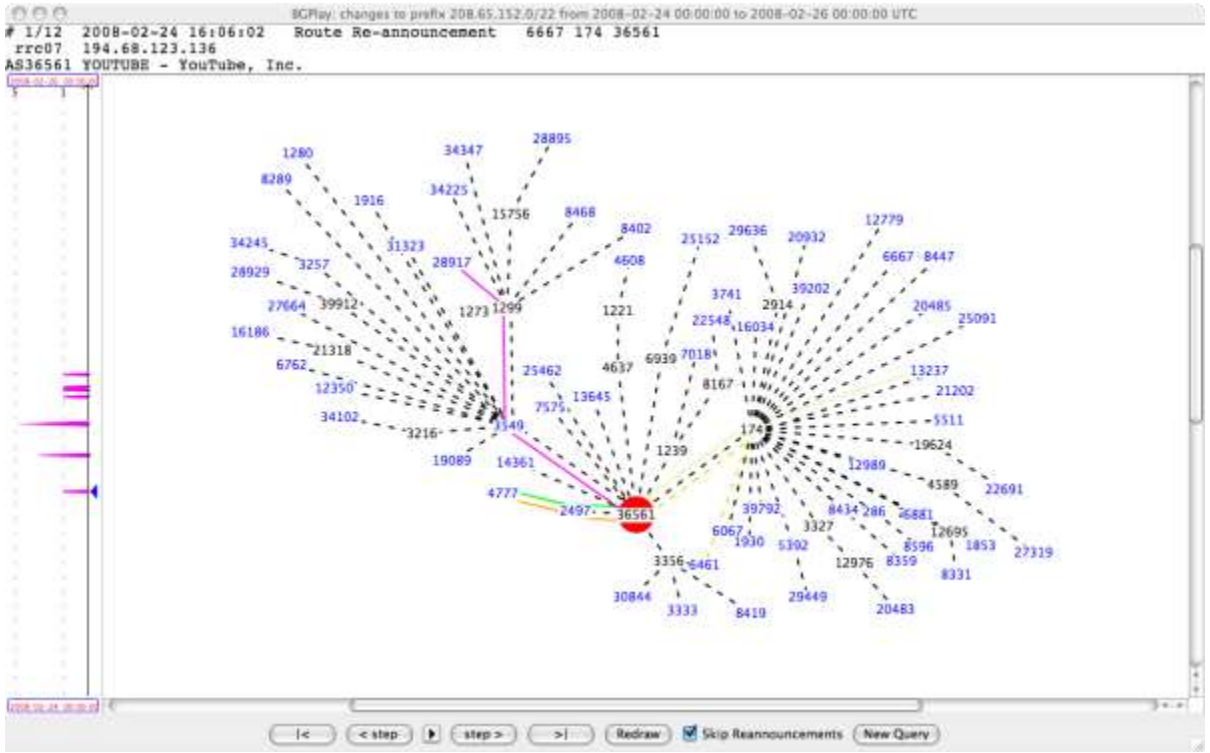


Secuestro de rutas (BGP hijacking)



YouTube Hijacking: A RIPE NCC RIS case study

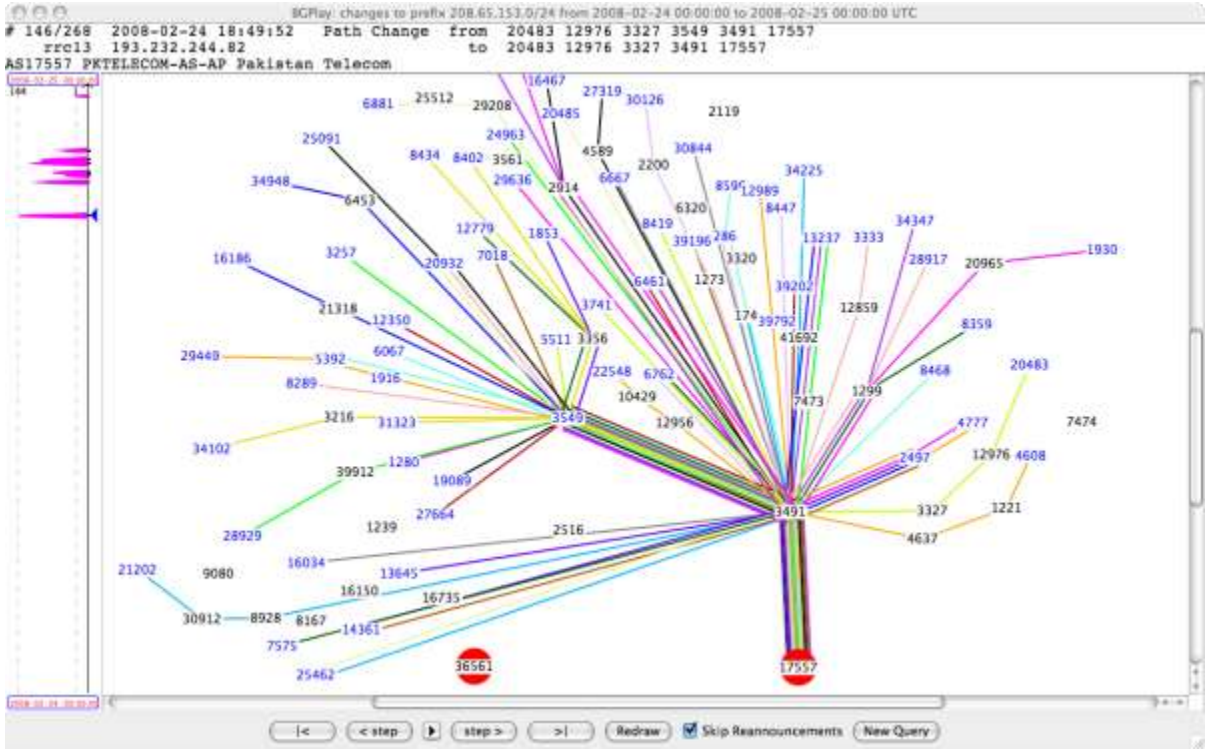
1. ASN 36561 (YouTube) anuncia 208.65.152.0/22



Fuente: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

YouTube Hijacking: A RIPE NCC RIS case study

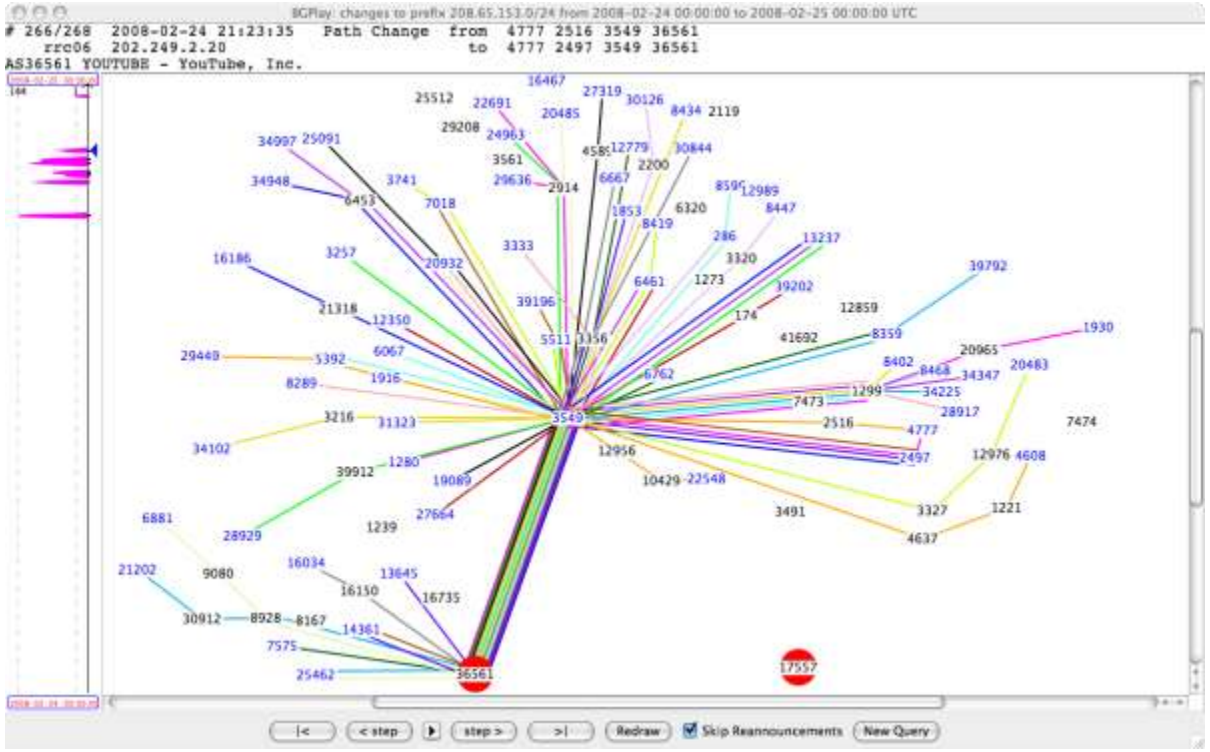
1. ASN 36561 (YouTube) anuncia 208.65.152.0/22
2. ASN 17557 (Pakistan Telecom) anuncia 208.65.153.0/24



Fuente: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

YouTube Hijacking: A RIPE NCC RIS case study

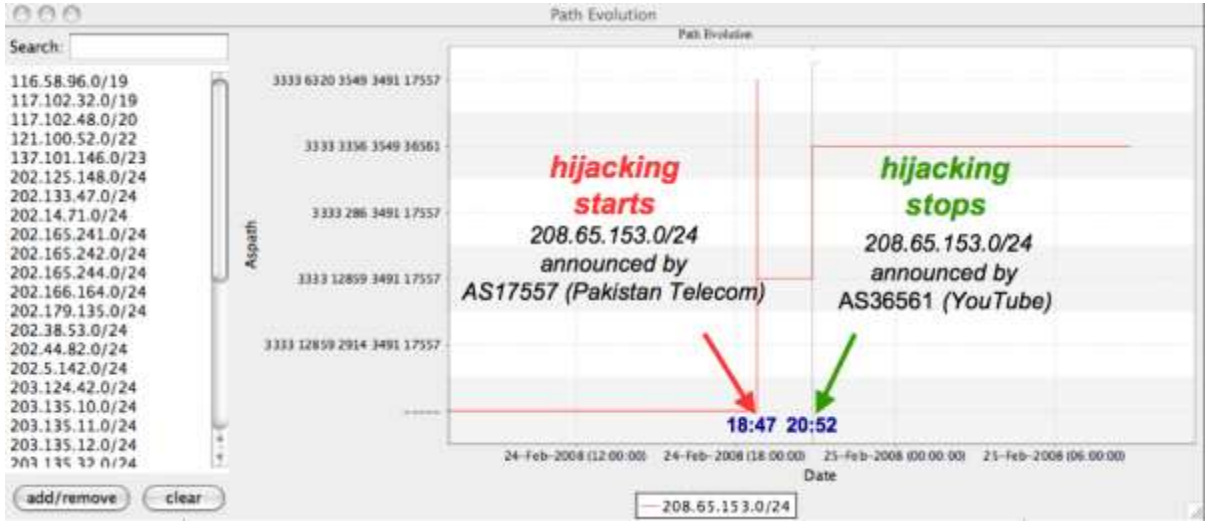
1. ASN 36561 (YouTube) anuncia 208.65.152.0/22
2. ASN 17557 (Pakistan Telecom) anuncia 208.65.153.0/24
3. ASN 36561 (YouTube) anuncia 208.65.153.0/24 y ASN 17557 (Pakistan Telecom) retira el anuncio



Fuente: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

YouTube Hijacking: A RIPE NCC RIS case study

1. ASN 36561 (YouTube) anuncia 208.65.152.0/22
2. ASN 17557 (Pakistan Telecom) anuncia 208.65.153.0/24
3. ASN 36561 (YouTube) anuncia 208.65.153.0/24 y ASN 17557 (Pakistan Telecom) retira el anuncio



Fuente: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Otros incidentes

- **Febrero 2014.** Un ISP en Canadá es utilizado para secuestrar rutas y en 22 incidentes entre febrero y mayo, hackers logran robar una fuerte cantidad en cripto-moneda en sesiones de 30 segundos cada una.

- **Marzo 2017.** SECW Telecom en Brazil secuestro prefijos de Cloudflare, Google y BancoBrazil causando problemas de acceso a estos servicios en la región.

- **Abril 2017.** Una gran parte del tráfico perteneciente a MasterCard, Visa y otras instituciones financieras fueron brevemente ruteadas a través de Russian telecom.

Fuentes: https://www.wired.com/2014/08/isp-bitcoin-theft/
https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

Secuestro de rutas

¿Cómo evitar que otros anuncien mis bloques de IP como suyos?

¡Firmando mis recursos digitalmente!

Resource Public Key Infrastructure (RPKI)

RPKI

RFC	Nombre
3779	X.509 Extensions for IP Addresses and AS Identifiers
6480	An Infrastructure to Support Secure Internet Routing
6481	A Profile for Resource Certificate Repository Structure
6482	A Profile for Route Origin Authorizations (ROAs)
6483	Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)
6486	Manifests for the Resource Public Key Infrastructure (RPKI)
6487	A Profile for X.509 PKIX Resource Certificates
6488	Signed Object Template for the Resource Public Key Infrastructure (RPKI)
7730	Resource Public Key Infrastructure (RPKI) Trust Anchor Locator
8360	Resource Public Key Infrastructure (RPKI) Validation Reconsidered

entre otros…

Route Origin Authorizations (ROA)

ROA

ASN: 60504

Puede ser origen para el bloque: 198.51.100.0/24

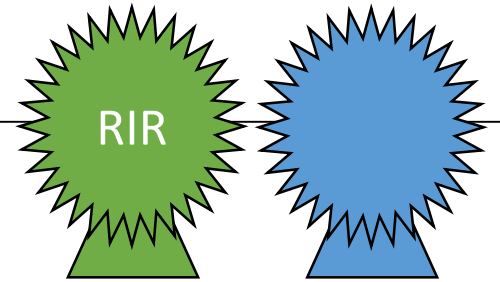
Certificado

Mi nombre:

Ejemplo ISP, SA de CV

Mis recursos:

- [ASN] 60504
- [IP] 198.51.100.0/24



Repositorios

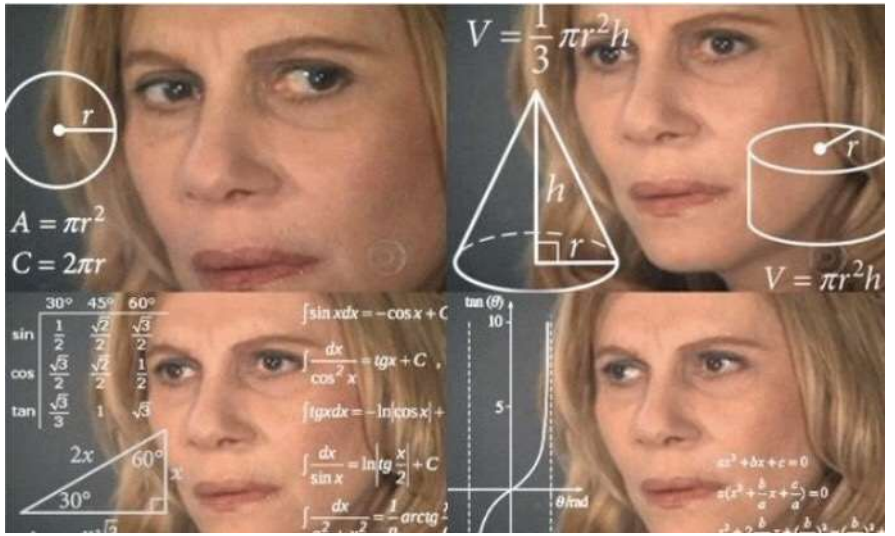
RIR	# de Archivos	# de ROA	Tamaño
AFRINIC	~ 1,000	~ 360	2.9 MB
APNIC	~ 11,160	~ 3,340	35.9 MB
ARIN	~ 7,030	~ 5,000	17.3 MB
LACNIC	~ 6,320	~ 2,440	15.6 MB
RIPE	~ 36,820	~ 10,940	132.1 MB
Total	**~ 62,330**	**~ 22,080**	**203.8 MB**

Fecha: 26 de julio, 2019

Validación de origen de rutas

Ok, certificados, firmas digitales y ROAs se utilizan para distinguir entre información verdadera y falsa…

¿Pero cómo le paso toda esta información a mi ruteador?



Validación de origen de rutas

AFRINIC

APNIC

ARIN
American Registry for Internet Numbers

lacnic

RIPE NCC

Validador RPKI

- Descarga la información de los TAL
- Valida criptográficamente la información
- Transmite la información validada a los ruteadores

Validación de origen de rutas

Descripción

- Implementación de RPKI Relying Party (Validador y Servidor RTR)
- Código Abierto y de libre uso
- Soporte para Linux y BSD
- Desarrollado en C

Estado

- Actual: Beta al público
- Sep-2019: Versión 1.0

Código fuente:
https://github.com/NICMx/FORT-validator

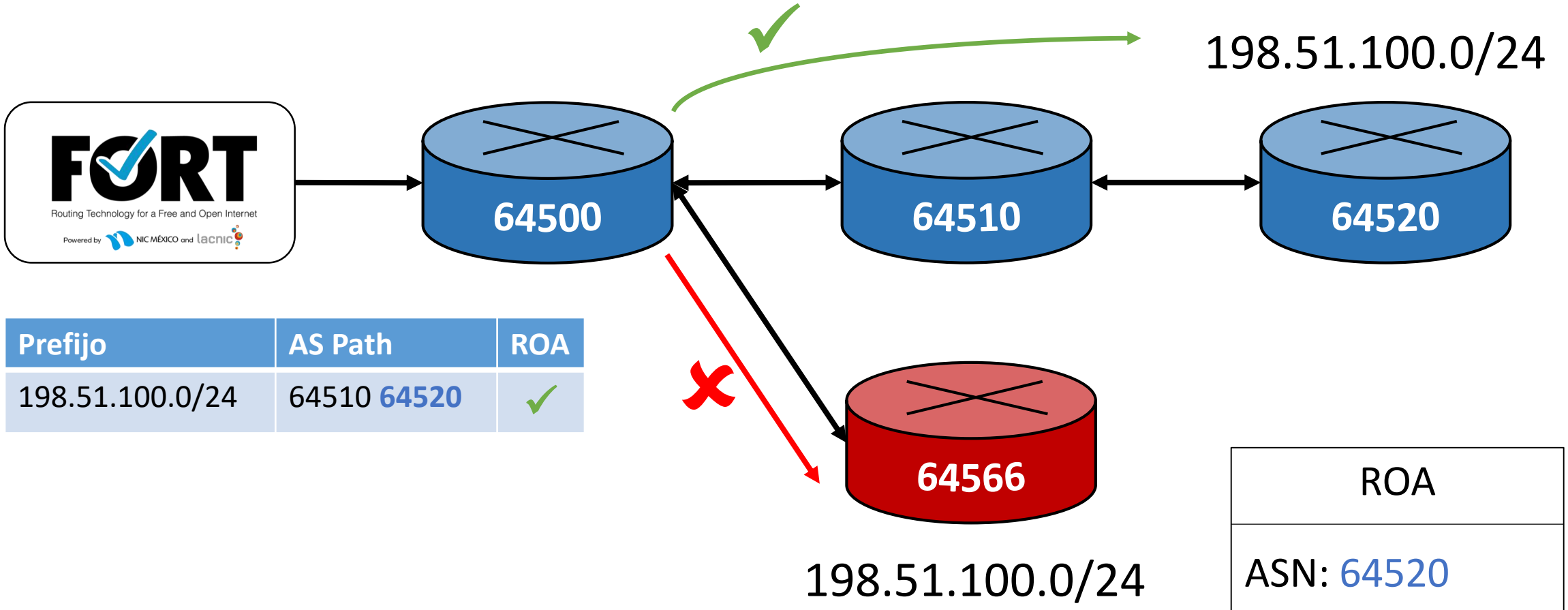
Validación de origen de rutas

Ruteadores con soporte RPKI-RTR

- Hardware
  - Cisco IOS 15.2 o superior, también Cisco IOS/XR desde 4.3.2
  - Juniper Junos 12.2 o superior
  - Nokia R12.0R4 o superior, ejecutando en 7210 SAS, 7750 SR, 7950 XRS y VSR
- Software
  - BIRD
  - FRRouting
  - GoBGP
  - OpenBGPD
  - VyOS

Fuente: https://rpki.readthedocs.io/en/latest/rpki/router-support.html

Validación de origen de rutas



Prefijo	AS Path	ROA
198.51.100.0/24	64510 64520	✓

ROA
ASN: 64520 IP: 198.51.100.0/24

FORT-Validator: Testing

- Debian-Based
  - Debian 10 — Passed
  - Ubuntu 18.04.2 LTS — Passed
- BSD-Based
  - FreeBSD 12.0 — Passed
  - OpenBSD 6.5 — Failed
- RedHat-Based
  - CentOS 7 — Failed
  - Fedora 30 — Passed
- Slackware-Based
  - Slackware (current) — Passed
  - OpenSUSE Leap 15.1 — Passed

Nota: Correcciones listas y se encuentran en testing.

Instalación de FORT-Validator

1. Instalar las dependencias:
   a. jansson
   b. libcrypto (LibreSSL o OpenSSL)
   c. rsync
   d. compilador C
2. Descargar el código de github
3. Compilar e instalar

Instalación de FORT-Validator

1. Instalar dependencias

```
# apt install autoconf automake build-essential libjansson-dev libssl-dev pkg-config rsync
```

2. Descargar el código de github

```
$ wget https://github.com/NICMx/FORT-validator/releases/download/v0.0.2/fort-0.0.2.tar.gz
$ tar xvzf fort-0.0.2.tar.gz
$ cd fort-0.0.2/
```

Nota:
Indica que el comando necesita permisos de administrador para ejecutarse.

debian

Instalación de FORT-Validator

3. Compilar e instalar

```
$ ./configure
$ make
# make install
```

Nota:
Indica que el comando necesita permisos de administrador para ejecutarse.

```
Debian GNU/Linux 10 debian tty1

debian login: jcano
Password:
Last login: Tue Aug  6 09:37:37 CDT 2019 on tty1
Linux debian 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jcano@debian:~$ _
```

¿Qué son los TALs y dónde los consigo?

- Un Trust Anchor Locator (TAL) apunta al certificado digital raíz de un RIR para validar los objetos en su repositorio
- Es necesario contar con los 5 archivos TAL para poder utilizar FORT-Validator
- Estos archivos se pueden encontrar en las páginas web de los 5 RIRs
  - AFRINIC https://afrinic.net
  - APNIC https://apnic.net
  - ARIN https://arin.net
  - LACNIC https://lacnic.net
  - RIPE https://ripe.net

¿Qué son los TALs y dónde los consigo?

```
rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqZEzhYK0+PtDOPfub/KR
c3MeWx3neXx4/wbnJWGbNAtbYqXg3uU5J4HFzPgk/VIppgSKAhlO0H60DRP48by9
gr5/yDHu2KXhOmnMg46sYsUIpfgtBS9+VtrqWziJfb+pkGtuOWeTnj6zBmBNZKK+
5AlMCW1WPhrylIcB+XSZx8tk9GS/3SMQ+YfMVwwAyYjsex14Uzto4GjONALE5oh1
M3+glRQduD6vzSwOD+WahMbc9vCOTED+2McLHRKgNaQf0YJ9a1jG9oJIvDkKXEqd
fqDRktwyoD74cV57bW3tBAexB7GglITbInyQAsmdngtfg2LUMrcROHHP86QPZINj
DQIDAQAB
```

Usando FORT-Validator

```
fort \
    --tal <archivo o directorio con los TALs> \
    --local-repository <directorio para el cache> \
    --server.address <Dirección del Servidor RTR> \
    --server.port <Puerto del Servidor RTR>
```

```
jcano@debian:~/fort$
```

Archivo de configuración

```
{
    "tal": "/tmp/tal/test.tal",
    "local-repository": "/tmp/repository",
    "mode": "server",

    “server”: {
            “address”: “192.0.2.1”,
            “port”: “323”
      },
      …
}
```

Desempeño de FORT

OS: Ubuntu Server 18.04.2 LTS

Hardware: Raspberry Pi3 B+ (Cortex-A53 (ARMv8) 64-bit SoC@1.2GHz | 1 GB RAM)

FORT

Routing Technology for a Free and Open Internet

Powered by NIC MÉXICO and lacnic

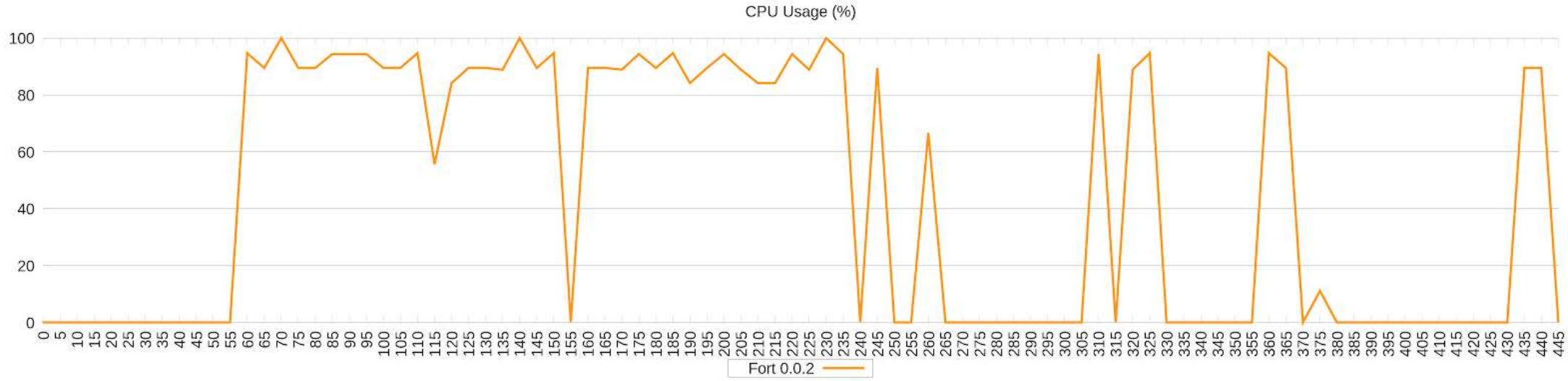
ubuntu

FORT en Raspberry Pi3 B+

Modo: Standalone

OS: Ubuntu Server 18.04.2 LTS (Preinstalled Ubuntu Server ARM64)

Hardware: Raspberry Pi3 B+ (Cortex-A53 (ARMv8) 64-bit SoC@1.2GHz | 1 GB RAM)

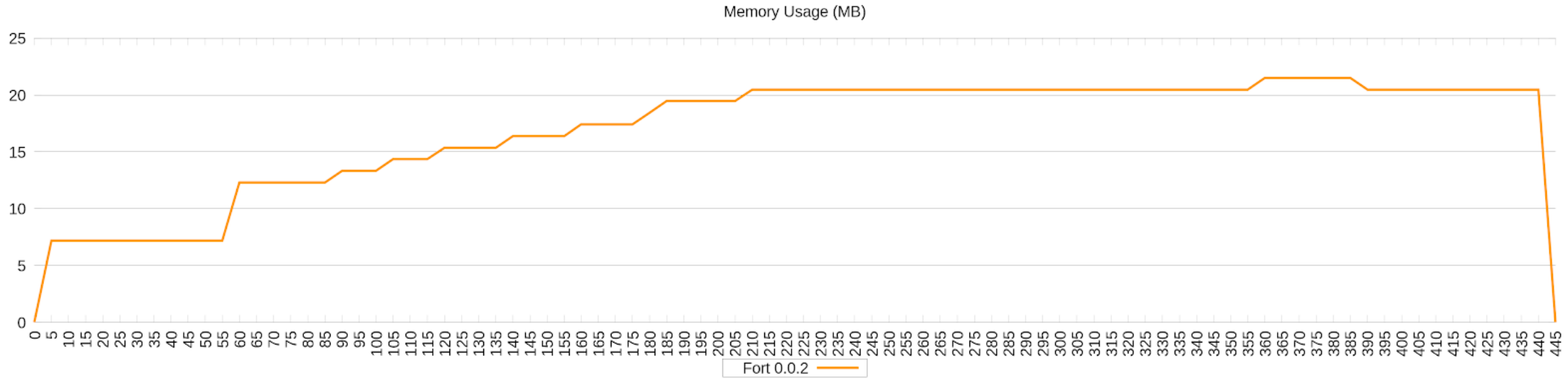


FORT en Raspberry Pi3 B+

Modo: Standalone

OS: Ubuntu Server 18.04.2 LTS (Preinstalled Ubuntu Server ARM64)

Hardware: Raspberry Pi3 B+ (Cortex-A53 (ARMv8) 64-bit SoC@1.2GHz | 1 GB RAM)

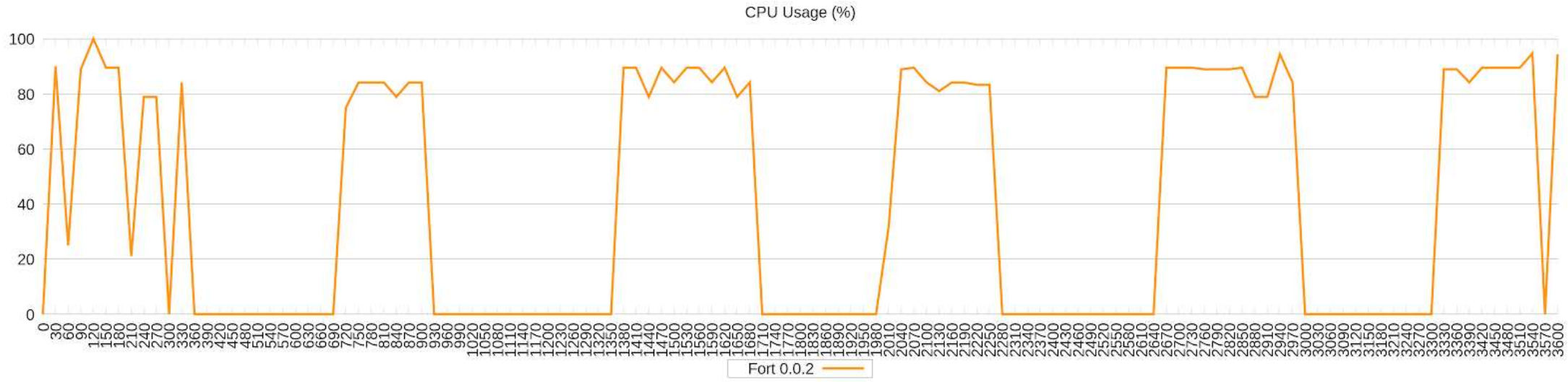


FORT en Raspberry Pi3 B+

Modo: Server

OS: Ubuntu Server 18.04.2 LTS (Preinstalled Ubuntu Server ARM64)

Hardware: Raspberry Pi3 B+ (Cortex-A53 (ARMv8) 64-bit SoC@1.2GHz | 1 GB RAM)

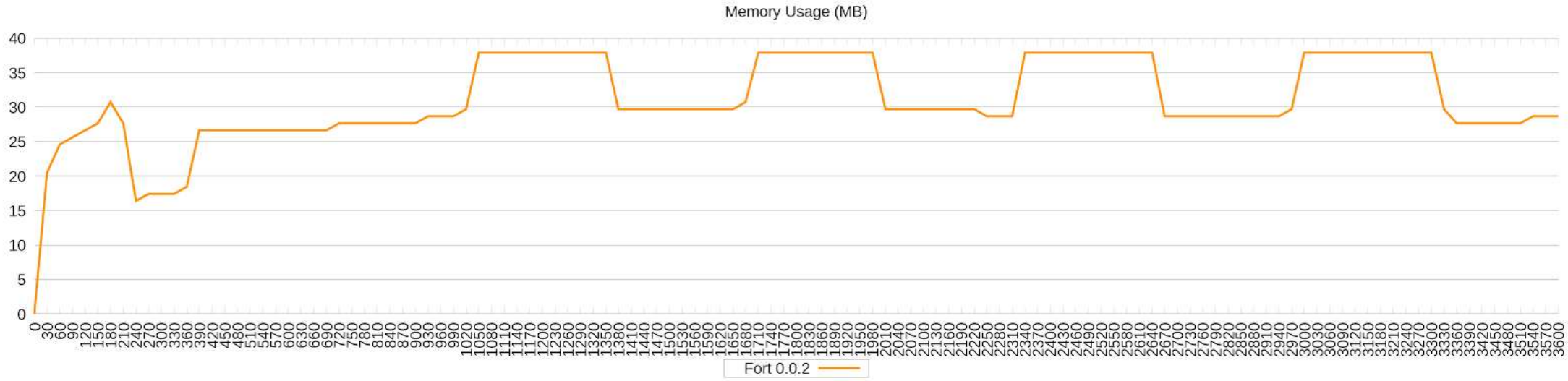


FORT en Raspberry Pi3 B+

Modo: Server

OS: Ubuntu Server 18.04.2 LTS (Preinstalled Ubuntu Server ARM64)

Hardware: Raspberry Pi3 B+ (Cortex-A53 (ARMv8) 64-bit SoC@1.2GHz | 1 GB RAM)



Mas información

- Proyecto FORT

  https://fortproject.net

- FORT-Validator
  - Documentación

    https://nicmx.github.io/FORT-validator

  - Repositorio del código

    https://github.com/NICMx/FORT-validator

¿Preguntas?

¡Muchas Gracias!