IPv4 Hijacking: Our Experience

Mirjam Kühne, Ivo Dijkhuis

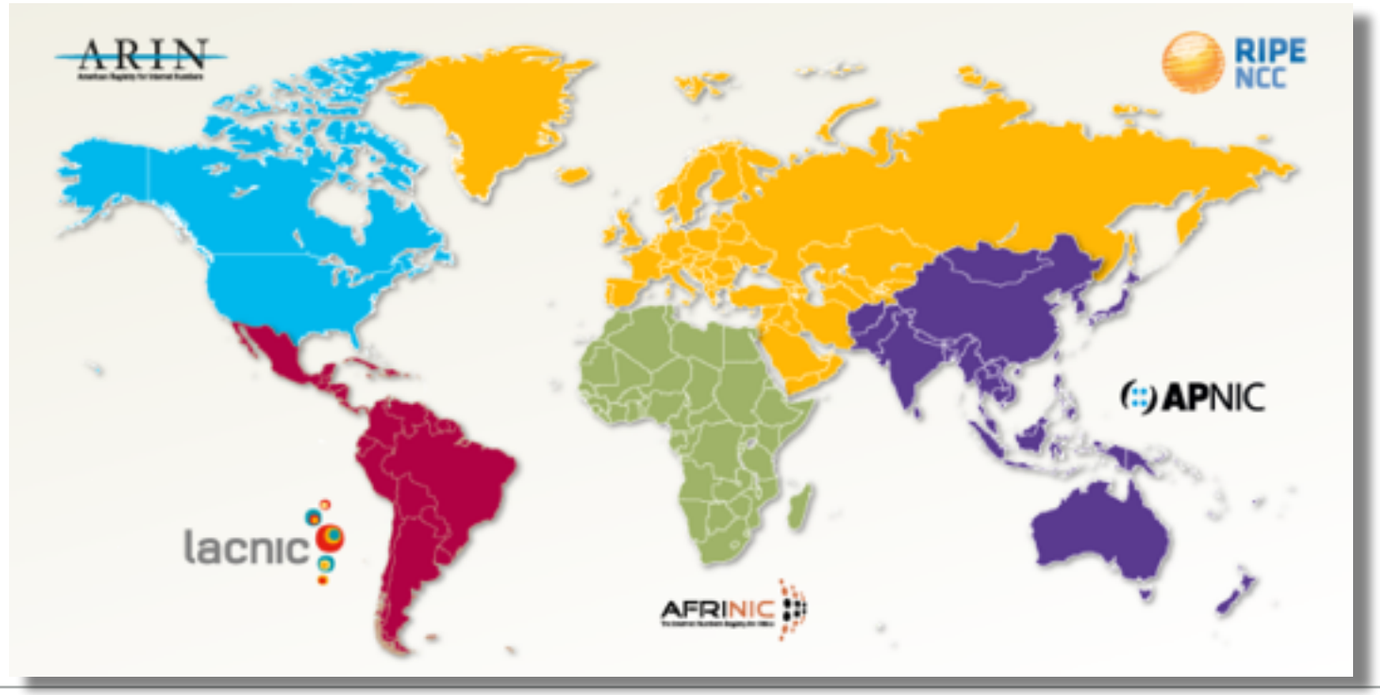
TF-CSIRT 43 | Rome - Italy | 18 September 2014

Overview

- Introduction to the RIPE NCC
- Our definition of hijacking
- Common approaches we observe
- Investigations and interventions
- Common difficulties and typical responses
- What you can do

Introduction to the RIPE NCC

- Not-for-profit, independent membership association
  - Neutral and impartial
  - Established in Amsterdam in 1992
  - Provides open community platform
- Over 10,000 members in 76 countries
- Bottom-up industry self regulation



RIPE NCC

RIPE NCC Activities

- Distribute IP addresses and AS numbers
- Support policy development in the RIPE NCC service region (Europe, Middle East, parts of central Asia)
- Maintain RIPE registry (RIPE whois Database)
- Resource certification (RPKI)
- Training Courses
- Tools and measurements
  - RIPE Atlas, RIPEstat

Our Definition of Hijacking

"Taking control of *issued* Internet number resources under false pretences"

- IPv4 addresses get re-registered to hijackers or another (innocent) organisation
- IPv4 addresses have economic value due to IPv4 scarcity

Background Information

- 12 September 2012: the RIPE NCC starts allocating from the last /8
- The RIPE NCC sees an increase in hijackings of **apparently** unused and/or abandoned addresses
- Hijacks found so far
  - **227 cases investigated, 19 hijacks found, 6 ongoing**
  - Often cases get resolved before they turn into hijack
- Most hijacking cases involve organisations we don't have a business relationship with (PI, legacy)

When Do We Investigate?

- A resource holder sends us a complaint or abuse report
- An experienced staff member notices something out of the ordinary
- Follow-up from existing investigations: one case often leads to another

Common Approaches Hijackers Use

- Research company histories and provide paper trails to demonstrate changes in business structure
- Conduct BGP test announcements to check if addresses are unused
- Re-register expired domain names to make email change requests look legitimate
- Copy websites, with identical pages hosted on (almost) identical domain names

Common Approaches Hijackers Use

- Forged documentation
  - Faked IDs
  - Faked company registration papers
  - Forged signatures of real people on contracts
  - Forged stamps and signatures of notaries and resource holders

How Do We Investigate?

- We check changes in company structure
  - Public records
  - National chamber of commerce registries
- We contact former and current resource holders (where possible)
  - Contact notaries found on documentation
  - Phone calls, emails and faxes
  - Using other contact information beyond what was provided

What Do We Do?

- Allowing time to support claim to the address space
- Reverting all changes immediately
- Resources are de-registered if no legitimate holder found
- Where member involvement in the hijacking case can be proven
    - Closure of member account and de-registration of IP resources
- Reporting to authorities where appropriate

Common Difficulties

- The resource holder expects immediate action while we need to investigate carefully
- It can be difficult to find and contact the resource holder in question
- No effective penalty and lots to gain for the hijacker:
  - They can open a new RIPE NCC member account
  - No high costs involved
  - No blacklists, no fine

What You Can Do

- Protect your resources against hijacking by making sure your RIPE Database objects and contact information are up to date
- If acquiring resources, ensure you are in contact with the legitimate holder or representative
- If you need help, or think your resources may have been hijacked, contact: reg-review@ripe.net

https://www.ripe.net/lir-services/resource-management/address-hijacking-in-the-ripe-ncc-service-region

Questions?