Leslie Nobile

Leo Vegoda

Address Space & AS Number Hijacking

Leslie Nobile, ARIN
Leo Vegoda, RIPE NCC

EOF, RIPE 48
May 3 & 4, 2004

Overview

- Definition
- Effects & Implications
- Historical Perspective
- Current Status
- Hijackers’ Modus Operandi
- RIR Scope of Activity
- RIR Actions
- Potential Resolutions
- Operators’ Actions

BEWARE
YOU ARE ENTERING
HI-JACK AREA
STOP
500m

What is Hijacking?

“Unauthorised changes made to registration records or objects in the database. The Whois data then inaccurately reflects this false information and gives the illusion that the individual now has some authority over the resources.”

Effects & Implications

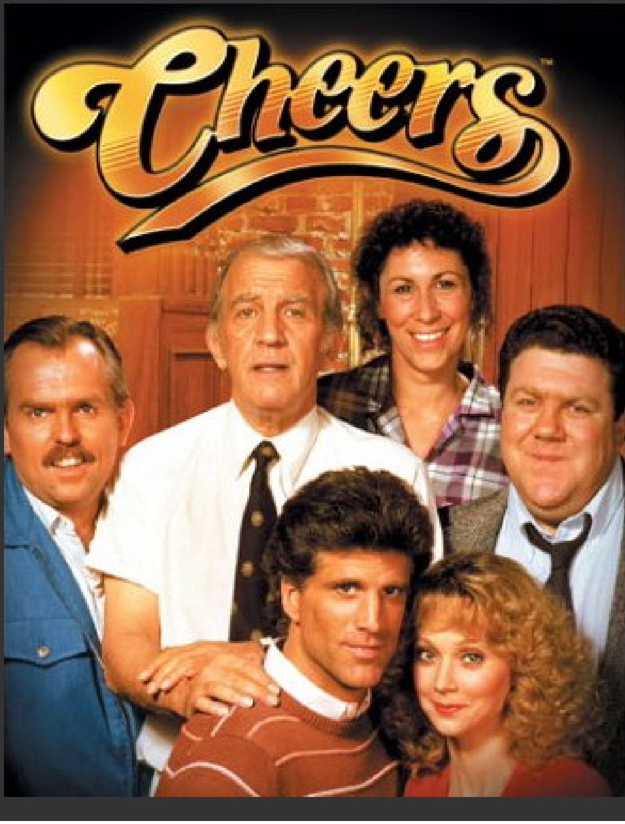
- Operators
  - Can damage your reputation
  - Increases workload
  - Slows response times
  - Increases costs
    - Staffing
    - Time
    - Legal fees
  - May create liability issues

Effects & Implications

- RIRs
  - Can damage your reputation
  - Increases workload
  - Slows response times
  - Increases costs
    - Staffing
    - Time
    - Legal fees
  - May create liability issues

Historical perspective

- The “Cheers”®™ phenomenon
- Where everybody knows your name…



Historical perspective

- Ask and ye shall receive…
- John Postel’s notebook
- IANA, SRI NIC, DoD NIC
- RIRs created
- Internet “Boom” in mid-90’s
- Things start to change…

Historical perspective

- Whois Databases
  - Different systems built from different models
  - Registration -vs- Routing Registries
  - Results:
    - Whois data duplicated between databases
    - Different database authorisation schemas
    - Different change control mechanisms

Now…

- Big business
- Highly commercialised

Current Status

- ARIN

Status	Number	Comment
Opened	162	Reported to or discovered by ARIN
Not Validated	17	No evidence
Closed	133	Reverted to original information Reclaimed by ARIN Returned to ARIN by original registrant
Pending	12	Under investigation

Categories

Category	Number of Records
Legacy Class A	1
Legacy Class B	52
Legacy Class C	64
ARIN Direct Assignments or Allocations	10
Autonomous Systems	18

Current Status

- RIPE NCC

Status	Number	Comment
Opened	6	Reported to or discovered by the RIPE NCC
Not Validated	2	No evidence
Closed	3	Reverted to original information, or De-registered by the RIPE NCC, or Returned to the RIPE NCC by original registrant
Pending	1	Cases remain open

Categories

Category	Number of Records
Legacy Class A	0
Legacy Class B	0
Legacy Class C	0
PI Assignments	4
Autonomous Systems	4

Hijackers’ Modus Operandi

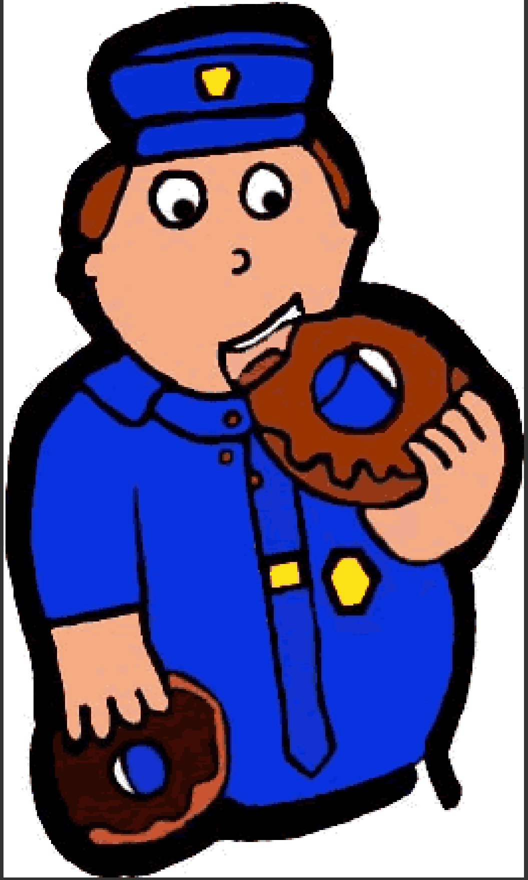
- Target legacy blocks in particular
- Ensure that blocks are not routed
- Search Whois for out of date contact information
- Check whether the domain has expired
  - if it’s expired, hijacker registers the domain
  - if it’s not expired, they register a similar domain
- Many of them register a company or incorporate using the name of the original registrant

RIR Scope

- Stewardship of Internet Number Resources
- Provide a public registry for the community to maintain
- Neutral and impartial
- Bottom up, consensus based policy development process

Out of RIR Scope

- Cannot guarantee routability
- Cannot police the network



RIR Actions

ARIN Actions

- Developed counter-hijacking procedures
- Research and document all reported or discovered hijackings
- Introduction of X.509 auth scheme
- Developed new database “status” attribute to lock down records
- Co-operating with law enforcement agencies

RIPE NCC Actions

- Created reporting address <reg-review@ripe.net>
- Increased vigilance
- Take control of hijacked registrations
- Changes to request forms
- Introduction of Organisation objects
- A multitude of auth schemes
  - Deprecation of NONE auth scheme
  - Introduction of X.509 auth scheme
  - Introduction of MD5-PW auth scheme
  - LIR Portal tools

RIR Co-ordination Actions

- Exchange information
- Analyse cases together
- Devise methodologies together
- Monitor and participate in “hijacked” mailing list

What Aren’t We Doing?

- Reporting all incidents to law enforcement agencies
- Disclosing investigation details to the general public

Potential Resolutions

- Processes and Procedures
  - Require more stringent verification data
  - Revise service agreements
  - Display Whois historical “change log”

Potential Resolutions

- Database
  - Stronger validation software
  - Bi-Annual Whois data validation (Re-Registration)
  - More stringent Authentication, Authorisation and Accountability

Potential Resolutions

- Legacy Records
  - Separate registration database for all legacy records
  - Update Options:
    - No updates permitted without joining an RIR, **OR**
    - Validated updates within the *RLR to NS and contact records, on a fee-for-service basis
  - Legacy space holders encouraged to move their records into the RIR system over time

***RLR – “Registry of Legacy Resources”**

Considerations

- Legacy records
  - Pre-RIR contractual relationship?
  - Legal obligations?
  - Should maintenance fees be charged?
  - Criteria to determine user legitimacy?

What Is the Reality?

- Not all operators are aware of the problem
- Not all operators know they are vulnerable
- Most operators have registrations in an RIR database
- Registration data is provided by you
- The database is maintained by the RIRs

What Can You Do?

- Ensure Organisation, contact & registration data are accurate and up to date
  - Your customers’ records as well as your own

Questions?