IP Address Hijacking

What is Hijacking?

Individuals targeting mainly legacy IP address blocks to make unauthorized changes to registration records in WHOIS. The WHOIS data then inaccurately reflects this false information and gives the illusion that the individual now has some authority over the resource records. Affected resources include IP addresses as well as AS numbers.

Effects / Implications

- Misleads Network Operators
- Compromises WHOIS Database
- Creates Liability Issues
- Increased Workload
- Slower Response Times
- Increased Costs
  - **Staffing**
  - **Legal Fees**

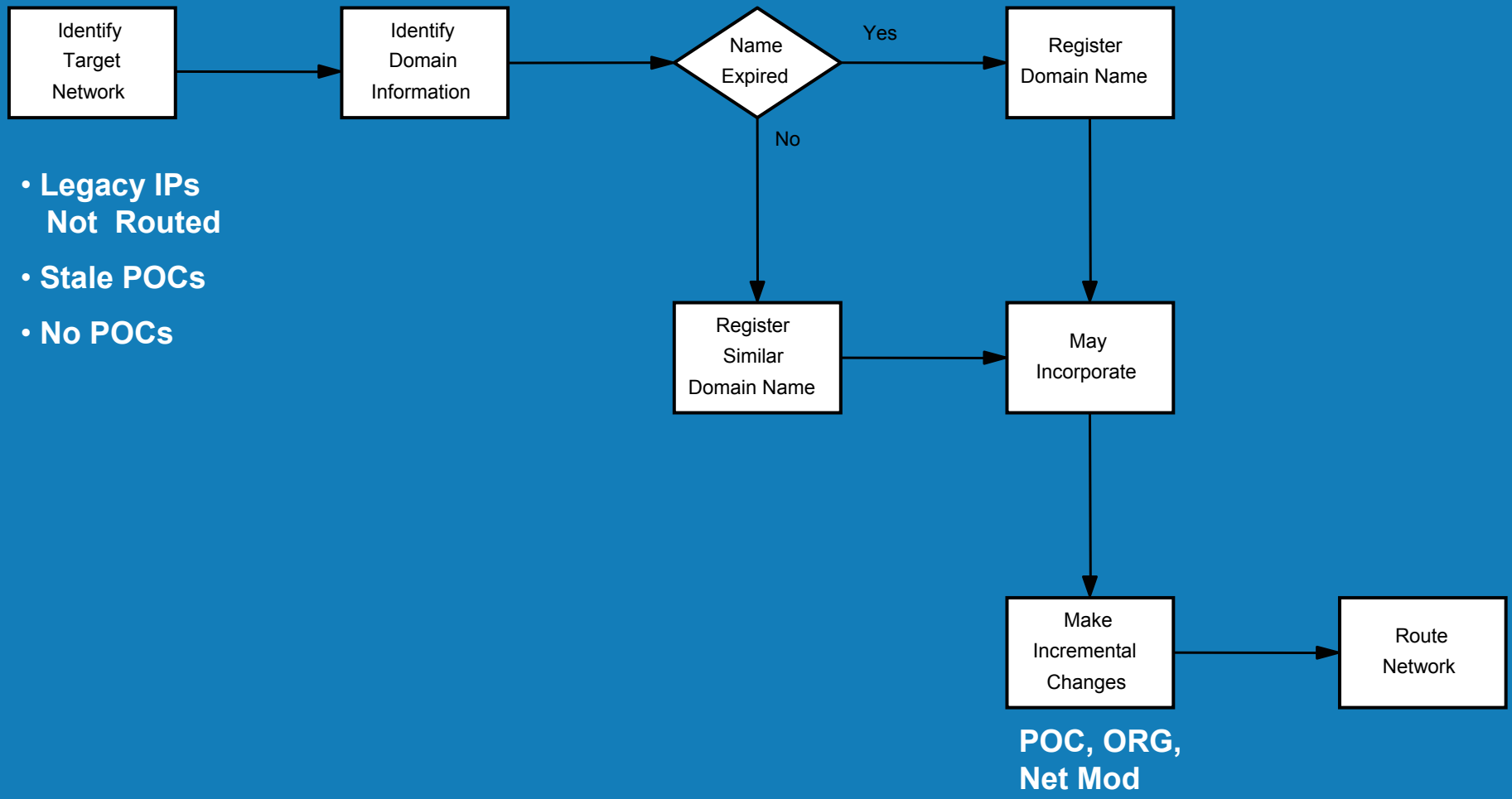
Current Status
[APR – OCT 03]

Status	Number	Comment
Opened	110	Reported to or Discovered by ARIN
Not Validated	11	No Evidence
Closed	84	Reverted to Original Information Reclaimed by ARIN Returned to ARIN by Original Registrant
Pending	15	Under Investigation

Categories

Category	Number of Records
Legacy Class A	1
Legacy Class B	48
Legacy Class C	45
Direct Allocations	4
Reassignment	1

Typical Hijacking Modus Operandi



- Legacy IPs Not Routed
- Stale POCs
- No POCs

What is ARIN Doing?

- Identified patterns used by hijackers to uncover unauthorized database changes
- Monitor “hijacked” list
- Research every reported or discovered hijacking
- Document and track every case
- Working with law enforcement agencies
- Developed/modified processes and procedures
- Developed new database “status” attribute that can lock down records
- RIR Coordination

What is ARIN Not Doing?

- Reporting All Incidents to Law Enforcement Agencies
- Disclosing Investigation Details to the General Public

Possible Actions

- Processes and Procedures
- Database
- Legacy Records

Possible Actions
Processes and Procedures

- **Require Additional Verification Information**
  - Tax ID
  - Raised Seal Corporation Documents
- **Pursue Legal Options**
- **Revise the Registration Services Agreement**
  - Add AUP Clause
  - Strengthen Transfer Clause
- **Display WHOIS Historical "change log"**

Possible Actions
Database

- Stronger Validation Software
- Bi-Annual WHOIS data Validation
  [Re-Registration]
- More Stringent Authentication, Authorization, and Accountability

Possible Actions
Legacy Records

"Registry of Legacy Resources (RLR)"

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

Possible Actions
Legacy Records

Considerations

- Pre-RIR Contractual Relationship
- Legal Obligations
- Maintenance Fees
- Criteria to Determine User Legitimacy

What Can You Do?

- **Ensure ORG & Resource Records are Updated**
  - Your Records
  - Your Customer's Records
- **Use Stronger Authentication When Available**

Thank You