IP Address Hijacking

An ARIN Perspective

Ray Plzak
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]**

<table>
<thead>
<tr>
<th>Status</th>
<th>Number</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opened</td>
<td>110</td>
<td>Reported to or Discovered by ARIN</td>
</tr>
<tr>
<td>Not Validated</td>
<td>11</td>
<td>No Evidence</td>
</tr>
<tr>
<td>Closed</td>
<td>84</td>
<td>Reverted to Original Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reclaimed by ARIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Returned to ARIN by Original Registrant</td>
</tr>
<tr>
<td>Pending</td>
<td>15</td>
<td>Under Investigation</td>
</tr>
</tbody>
</table>
## Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Class A</td>
<td>1</td>
</tr>
<tr>
<td>Legacy Class B</td>
<td>48</td>
</tr>
<tr>
<td>Legacy Class C</td>
<td>45</td>
</tr>
<tr>
<td>Direct Allocations</td>
<td>4</td>
</tr>
<tr>
<td>Reassignment</td>
<td>1</td>
</tr>
</tbody>
</table>
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