The Hijackers Guide To The Galaxy: Off-path Taking Over Internet Resources

Tianxiang Dai, Philipp Jeitner, Haya Shulman, Michael Waidner

German National Research Center for Applied Cybersecurity ATHENE
Technical University of Darmstadt
Fraunhofer Institute for Secure Information Technology SIT
Overview

➢ Digital resources and providers
➢ Taking over resource holders’ accounts
➢ Vulnerable customers
➢ Potential resource manipulations
➢ Vulnerable resources
➢ Countermeasures & Conclusions
Digital resources and providers

Provider datasets

RIRs
- AFRINIC
- APNIC
- ARIN
- LACNIC
- RIPE

Registrars
- Godaddy
- Namecheap
- NetworkSolutions
- enom
- name.com
- Alibaba
- Amazon
- Gandi
- Namesilo
- Google
- OVH

Cloud (IaaS)
- Amazon
- Azure
- Alibaba
- Google
- IBM
- Tencent
- Oracle
- DigitalOcean
- Linode
- IONOS
- Hostwinds
- OVHCloud
- Vultr
- CloudSigma

Certificate Authorities
- IdenTrust
- DigiCert
- Sectigo
- GoDaddy
- GlobalSign

Customers datasets

- 75% of customers of RIRs (Local ISPs)
- 100K-top Alexa
Attacking providers

Taking over accounts from off-path

- Take over accounts via password recovery:
  - Poison DNS cache for victim domain
  - Trigger password recovery for victim domain
  - Reset password and take over account

How to poison cache?
- On-path lookup interception
- Off-path:
  - BGP prefix hijacks
  - Side channels
  - IP fragmentation

<table>
<thead>
<tr>
<th>Vulnerable providers</th>
<th>BGP sub-prefix</th>
<th>Side-channel</th>
<th>Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIRs</td>
<td>5/5</td>
<td>0/4</td>
<td>3/5</td>
</tr>
<tr>
<td>Registrars</td>
<td>11/11</td>
<td>0/9</td>
<td>11/11</td>
</tr>
<tr>
<td>Cloud providers</td>
<td>11/14</td>
<td>4/13</td>
<td>14/14</td>
</tr>
<tr>
<td>CAs</td>
<td>5/5</td>
<td>0/2</td>
<td>5/5</td>
</tr>
<tr>
<td>Total providers</td>
<td>27/30</td>
<td>4/24</td>
<td>28/30</td>
</tr>
</tbody>
</table>
Vulnerable Customers

- Accessibility of customers’ account details
  - 75% of ASes have email addresses listed in WHOIS
  - 11% of Alexa 100K domains
  - Account identifiers can also often be guessed

- Nameserver configuration:
  - 11-56% of accounts vulnerable

How to poison cache?
- On-path lookup interception
- Off-path:
  - BGP prefix hijacks
  - Side channels
  - IP fragmentation
Manipulation of resources under providers

Test case: attacks via SSO account of LIR under RIPE NCC

- **RPKI manipulation: create/remove/modify ROAs**
  - Disrupt propagation of BGP announcements
  - Expose to BGP hijacking

- **RIPE DB manipulation**
  - Allows impersonation of LIR representatives
  - Refused BGP peerings, dropped routers, degradation of connectivity

- **User, role and contact management**
  - Create new users (admin/operator)
  - Modify LIR contacts/details
  - Terminate LIR membership
  - Modify LIR organisation, address, VAT

- **Transfer of IPv4 resources**
  - Sell resources to a third party

---

**Additional Validation**

<table>
<thead>
<tr>
<th>Attack</th>
<th>RIRs Registers</th>
<th>Labs</th>
<th>CAs</th>
<th>Outcome / Attacker use</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPKI manipulation</td>
<td>✅ ✅ ✅ ✗ permanent control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Changing the account details</td>
<td>✅ ✅ ✅ ✗ permanent control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPs Close the account permanently</td>
<td>✅ ✅ ✅ ✗ DoS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Disabling Email alerts</td>
<td>✅ ✅ ✅ ✗ remain stealthy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRs Resource transfer</td>
<td>✅ ✅ ✅ ✗ permanent control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Resource return / deletion</td>
<td>✅ ✅ ✅ ✗ DoS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAs Purchase new resources</td>
<td>✅ ✅ ✅ ✗ financial Damage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Control / Modify Resources</td>
<td>✅ ✅ ✅ ✗ facilitates hijacking</td>
<td>Whois DB VNMs</td>
<td>NS records</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✅ ✅ ✅ ✗ various</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>✅ ✅ ✅ ✗ traffic hijacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Create new ROAs/certificates</td>
<td>✅ ✅ ✅ ✗ facilitates hijacking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Create invalid ROAs</td>
<td>✅ ✅ ✅ ✗ DoS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Revoke certificates</td>
<td>✅ ✅ ✅ ✗ DoS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv4 Transfers per week:

- ARIN
- RIPE
- APNIC

Object in RIPE Database

- **IPv4 Transfer**
  - Offering party details
  - Receiving party details

RIPE DB manipulation

- Terminate membership

IPv4 Transfers per week:
How many resources are vulnerable?

<table>
<thead>
<tr>
<th>Resource</th>
<th>BGP hijack</th>
<th>Side-Channel</th>
<th>Fragmentation</th>
<th>Any Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 addresses</td>
<td>81%</td>
<td>30%</td>
<td>51%</td>
<td>93%</td>
</tr>
<tr>
<td>Domains</td>
<td>47%</td>
<td>10%</td>
<td>27%</td>
<td>65%</td>
</tr>
</tbody>
</table>
Recommendations for countermeasures

Taking over accounts

**Problems**
Easy access to infrastructure, account details are public

**Countermeasures**
- ✓ Hide public account details
- ✓ Separate system for high-privilege accounts
  - ✓ CAPTCHAs
  - ✓ DNSSEC

Manipulating resources

**Problems**
Modifications are easy, stealthy and fast

**Countermeasures**
- ✓ 2-Factor authentication
- ✓ Account notifications
- ✓ Account access restrictions
- ✓ Manual review/waiting time for transactions
Conclusions

- Resource databases are poorly protected
  - adversaries can take over the accounts and can manipulate them

- Attacks against accounts are practical
  - Large fraction of providers and customers are potentially vulnerable to off-path attacks
  - Even interesting for on-path attackers (nation adversaries, etc.)

- Fixes exist, but are not enforced
  - Strict authentication might drive customers away?
Thank You!

Philipp Jeitner, TU Darmstadt/Fraunhofer SIT
philipp.jeitner@sit.fraunhofer.de