ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

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

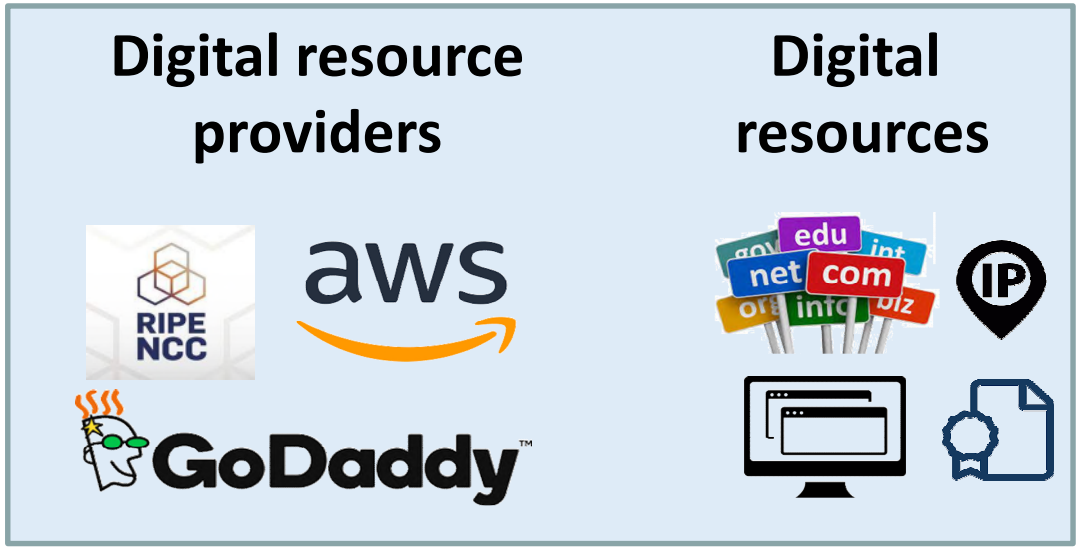
Tianxiang Dai

German National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Germany

Overview

- Digital resources and providers
- Taking over resource holders’ accounts
- Vulnerable customers
- Vulnerable resources
- Potential resource manipulations
- Countermeasures

Digital resources and providers

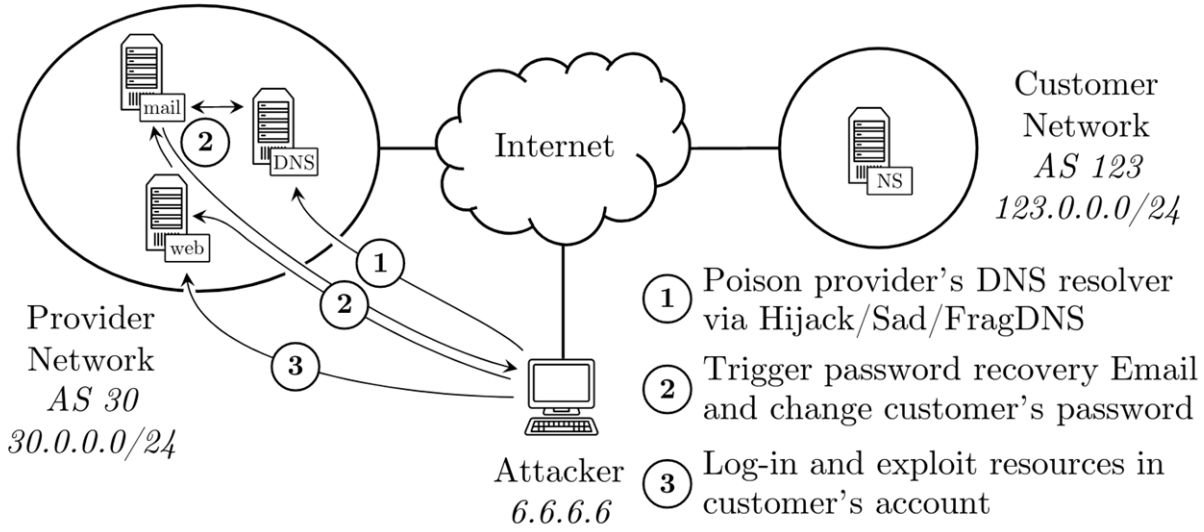


Access via SSO accounts

Resource	Provider Dataset		Total
IP	RIR	ARIN, RIPE, etc.	5
Domain	Registrar	GoDaddy, Alibaba, etc.	11
Computing	Cloud	AWS, Azure, etc.	14
Certificate	CA	Sectigo, DigiCert, etc.	5

Resource	Customer Dataset
IP	75% of customers of RIRs (ISPs / LIRs)
Domain & Certificate	Alexa Top-100K domains

Attacking providers



Taking over accounts from off-path via password recovery

Off-path DNS cache poisoning

- BGP prefix hijacking
- Side channel
- IP fragmentation

Vulnerable providers	BGP sub-prefix	Side-channel	Frag-ment
RIR	5/5	0/4	3/5
Registrar	11/11	0/9	11/11
Cloud	11/14	4/13	14/14
CA	5/5	0/2	5/5
Total	**27/30**	**4/24**	**28/30**

Vulnerable Customers

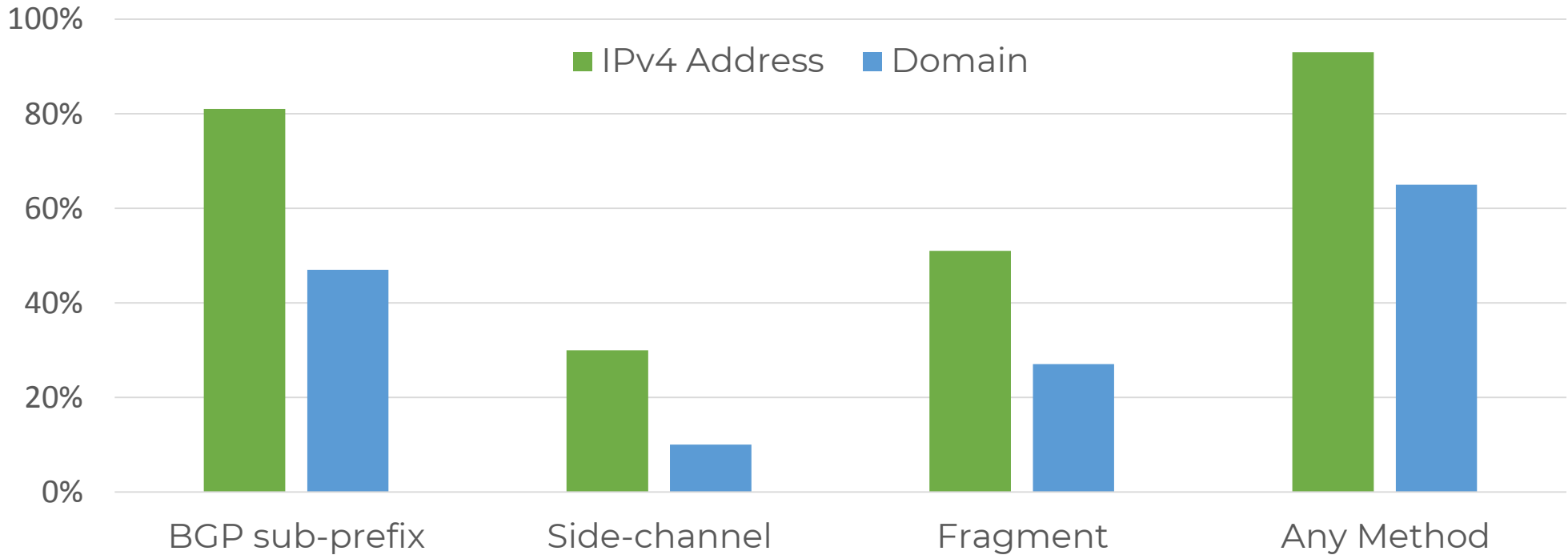
- Accessibility of customers' account details
  - **WHOIS**
    - 75% of ASes
    - 11% of Alexa domains
  - Guessable

Off-path DNS cache poisoning

- BGP prefix hijacking
- Side channel
- IP fragmentation

Vulnerable customers	BGP sub-prefix	Side-channel	Fragment
LIR administrator	56%	11%	17%
Domain owner	45%	10%	21%

Vulnerable Resources



Resource	BGP sub-prefix	Side-channel	Fragment	Any Method
IPv4 address	81%	30%	51%	93%
Domain	47%	10%	27%	65%

Potential resource manipulations

Showcase: 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

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!

Tianxiang Dai, ATHENE Center/Fraunhofer SIT
tianxiang.dai@sit.fraunhofer.de

Tianxiang Dai, Philipp Jeitner, Haya Shulman, and Michael Waidner. "The Hijackers Guide To The Galaxy: Off-Path Taking Over Internet Resources." In 30th {USENIX} Security Symposium ({USENIX} Security 21), pp. 3147-3164. 2021.