Wolf in Sheep's Clothing: Evaluating Security Risks of the Undelegated Record on DNS Hosting Services

Author: Fenglu Zhang, Yunyi Zhang, Baojun Liu, Eihal Alowaisheq, Lingyun Ying, Xiang Li, Zaifeng Zhang, Ying Liu, Haixin Duan, Min Zhang

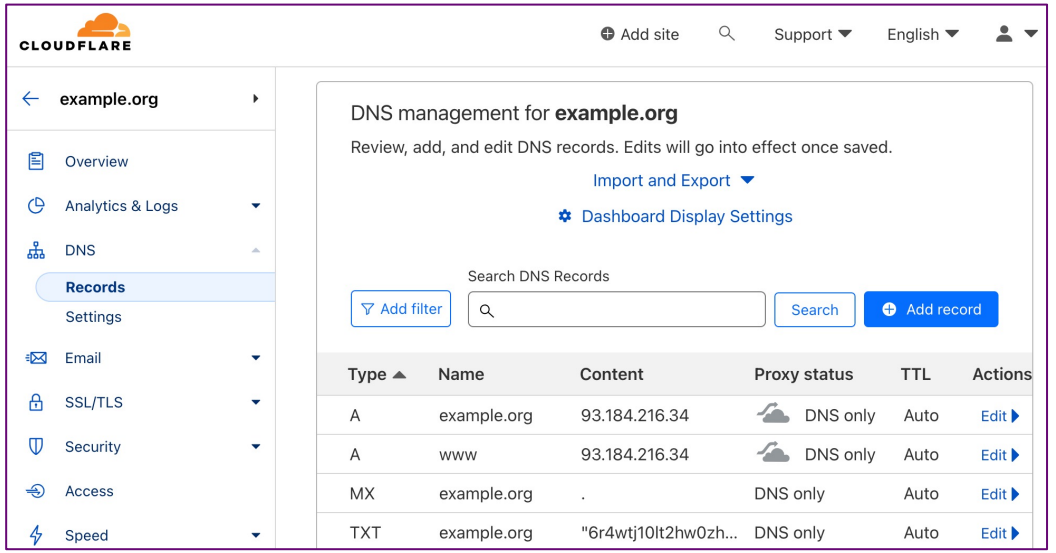
Takeaway

This research reveals an attack that has been overlooked by mainstream DNS hosting providers but is abused at a large scale.

DNS hosting services

- Provide infrastructure to handle the DNS query for hosted domains
- Lower the threshold to maintain and manage a domain

Some vendors of DNS hosting services



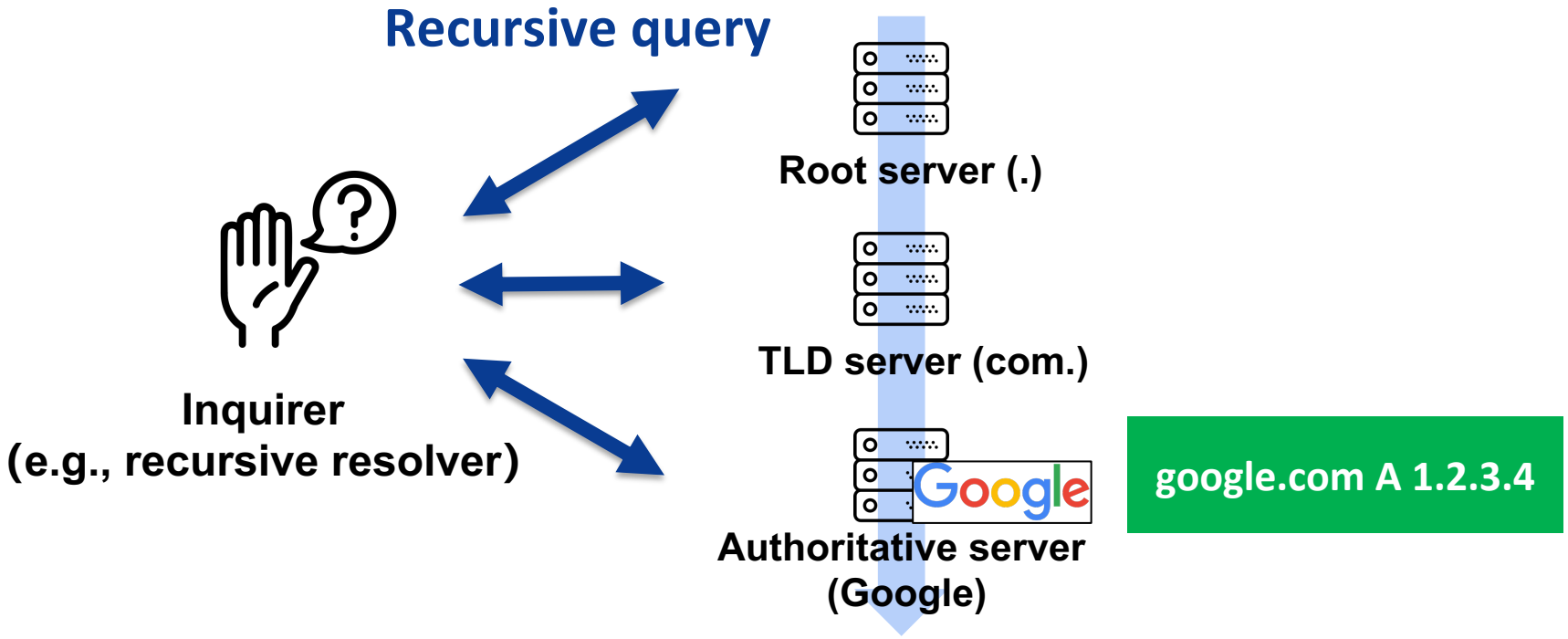
The user-friendly UI provided by a DNS hosting service

Undelegated record (UR)

- To further enhance the user experience, providers **do not verify ownership** and provide domain resolution directly, leading to the issue of **undelegated records (UR)**.

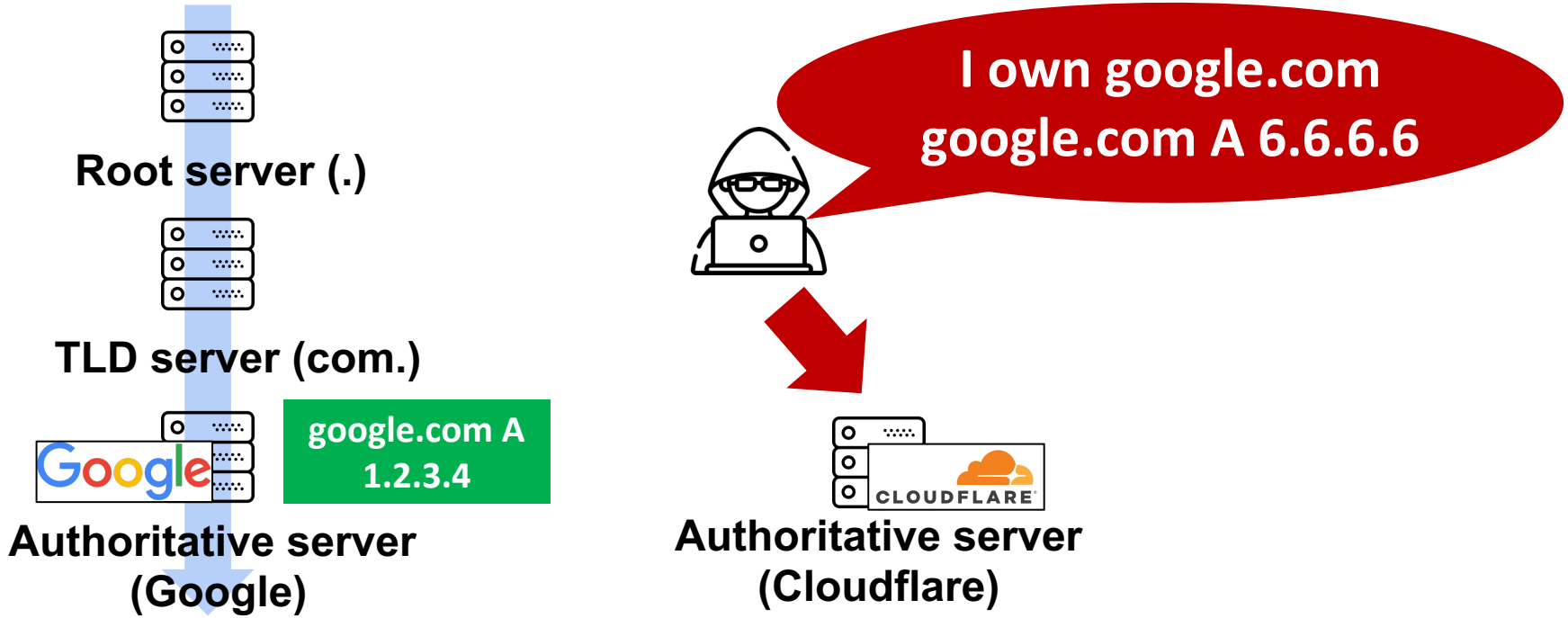
Undelegated record (UR)

- To further enhance the user experience, providers even **do not verify ownership** and provide domain resolution directly, leading to the issue of **undelegated records (UR)**.



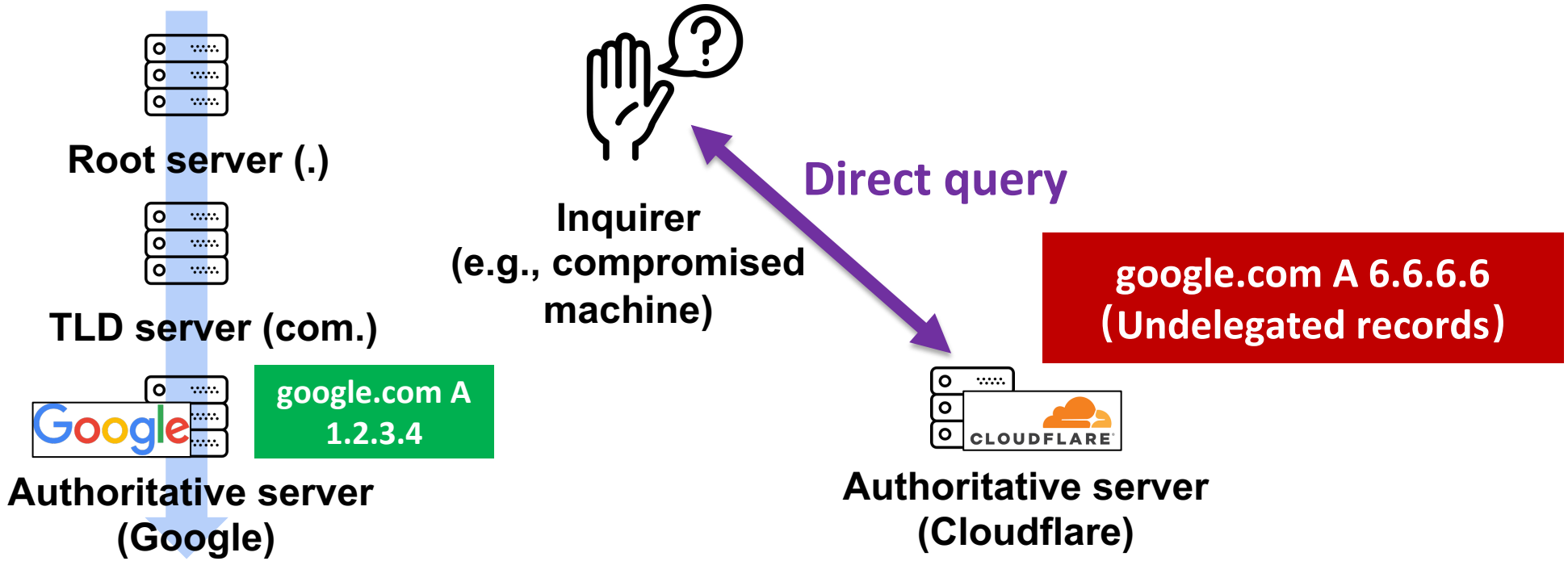
Undelegated record (UR)

- To further enhance the user experience, providers **do not verify ownership** and provide domain resolution directly, leading to the issue of **undelegated records (UR)**.



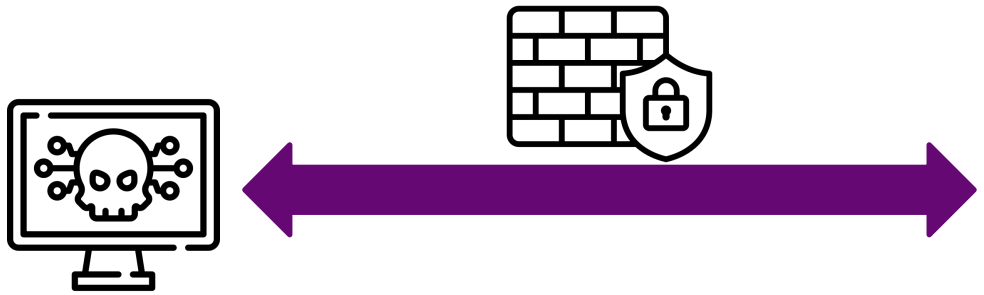
Undelegated record (UR)

- To further enhance the user experience, providers **do not verify ownership** and provide domain resolution directly, leading to the issue of **undelegated records (UR)**.



The attack of UR

- **Objective:** a compromised machine is **protected** by defense mechanisms (e.g., firewall or IDS) and **requires information from the attacker** (e.g., IP addresses of C2 server or the following command)
- **Challenge:** **bypassing** the defense mechanisms

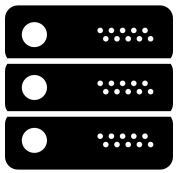


Information from the attacker:
- **IP addresses of C2 server**
- **command from the attacker**

The attack of UR

- **Objective:** a compromised machine is **protected** by defense mechanisms (e.g., firewall or IDS) and **requires information from the attacker** (e.g., IP addresses of C2 server or the following command)
- **Challenge:** **bypassing** the defense mechanisms

Information from the attacker:
- **IP addresses of C2 server**
- **command from the attacker**

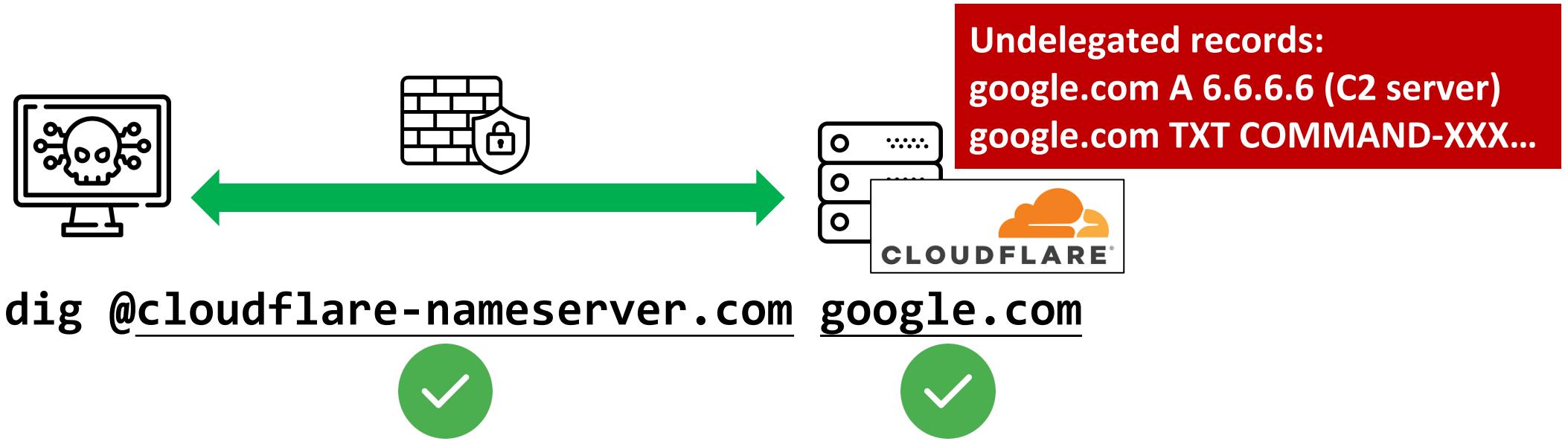


`dig @malicious-nameserver malicious-domain.com`

? ?

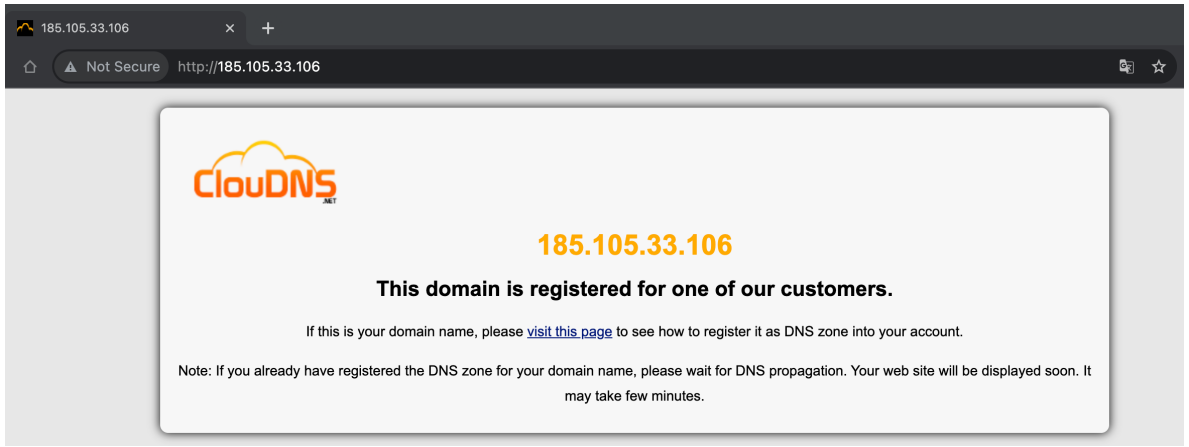
The attack of UR

- **Objective:** a compromised machine is **protected** by defense mechanisms
  (e.g., firewall or IDS) and **requires information from the attacker**
  (e.g., IP addresses of C2 server or the following command)
- **Challenge: bypassing** the defense mechanisms
- **Advantage:** abusing the **reputation of both popular domains and hosting providers**

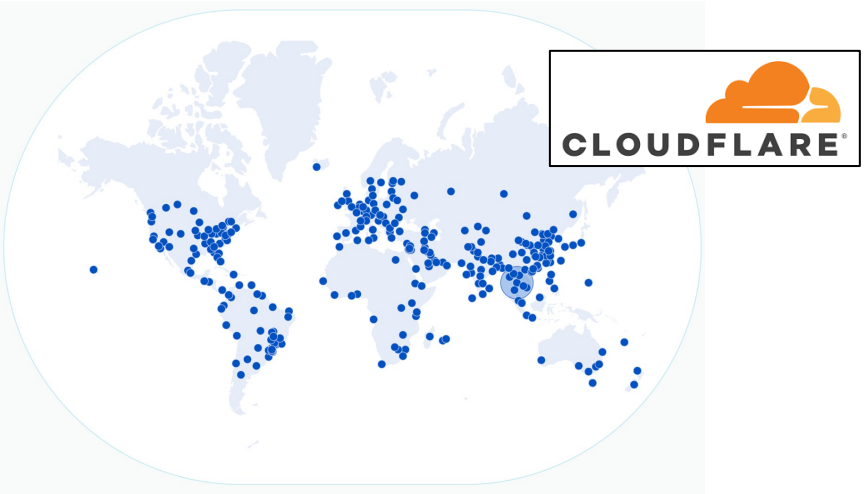


Measurement: main challenge

- How to determine potentially abused URs by **filtering:**
  - **Protective UR:** e.g., to a website with warning information
  - **Correct UR:**
    - Past delegations: switched hosting services but forgot to delete the past records.
    - Misconfigured authoritative servers: conduct recursive queries for a non-authoritative domain.



A warning website provided by a protective UR



Correct URs can be **geo-distributed** while the domain activating CDN

Measurement: methodology

Measurement: methodology

1. Response collection → **2. Determining suspicious record** → **3. Malicious behavior analysis**

- **Collect URs from popular hosting providers**
- **Collect information for further determination**
  - Protective URs: querying a non-authoritative domain (our domain)
  - Correct URs:
    - Leveraging **passive DNS data** to collect past delegations
    - Leveraging **geo-distributed open resolvers** to collect correct URs
      - With information of IP addresses in correct URs: AS, geolocation, HTTP response, TLS certificate

Measurement: methodology

1. Response collection → **2. Determining suspicious record** → **3. Malicious behavior analysis**

- **Exclude existing correct URs and protective URs directly**
- **Exclude extended correct URs by utilizing uniformity**
  - Information of IP addresses in correct URs (AS, geolocation, HTTP response, TLS certificate) for a domain tends to be **uniform**
    - As the **same organization** manages it

Measurement: methodology

1. Response collection → **2. Determining suspicious record** → **3. Malicious behavior analysis**

- **Label a UR if its related IP addresses are malicious**
  - A UR: the IP addresses in the record
  - TXT UR:
    - Embedded in the text of the record
    - The A record sharing the same nameserver and domain
- **Label an IP address by checking**
  - **Threat intelligence**
  - **IDS alert while checking sandbox traffic toward the IP address.**


Measurement: result

- Two measurements: collecting A and TXT URs in Apr and Dec 2022
  - For the top 2,000 Tranco domains
  - From 8,941 nameservers hosting 50+ domains in the top 1M Tranco domains

Measurement: result

- Two measurements: collecting A and TXT URs in Apr and Dec 2022
  - For the top 2,000 Tranco domains
  - From 8,941 nameservers hosting 50+ domains in the top 1M Tranco domains

Table : Overview of suspicious undelegated records (excluding correct and protective records).

Category	# Domain		# Nameserver		# Provider		# Undelegated record		# IP address	
	Total	Malicious	Total	Malicious	Total	Malicious	Total	Malicious	Total	Malicious
A	1,999	1,353 (67.68%)	6,262	4,981 (79.54%)	347	241 (69.45%)	1,366,164	395,095 (28.92%)	5,477	1,329 (24.27%)
TXT	448	221 (49.33%)	3,664	3,234 (88.26%)	102	67 (65.69%)	214,761	6,623 (3.08%)	1,147	273 (23.80%)
Total	1,999	1,369 (68.48%)	6,351	5,048 (79.48%)	347	248 (71.47%)	1,580,925	401,718 (25.41%)	6,346	1,494 (23.54%)

Measurement: result

- Two measurements: collecting A and TXT URs in Apr and Dec 2022
  - For the top 2,000 Tranco domains
  - From 8,941 nameservers hosting 50+ domains in the top 1M Tranco domains

Table : Overview of suspicious undelegated records (excluding correct and protective records).

Category	# Domain		# Nameserver		# Provider		# Undelegated record		# IP address	
	Total	Malicious	Total	Malicious	Total	Malicious	Total	Malicious	Total	Malicious
A	1,999	1,353 (67.68%)	6,262	4,981 (79.54%)	347	241 (69.45%)	1,366,164	395,095 (28.92%)	5,477	1,329 (24.27%)
TXT	448	221 (49.33%)	3,664	3,234 (88.26%)	102	67 (65.69%)	214,761	6,623 (3.08%)	1,147	273 (23.80%)
Total	1,999	1,369 (68.48%)	6,351	5,048 (79.48%)	347	248 (71.47%)	1,580,925	401,718 (25.41%)	6,346	1,494 (23.54%)

Measurement: result

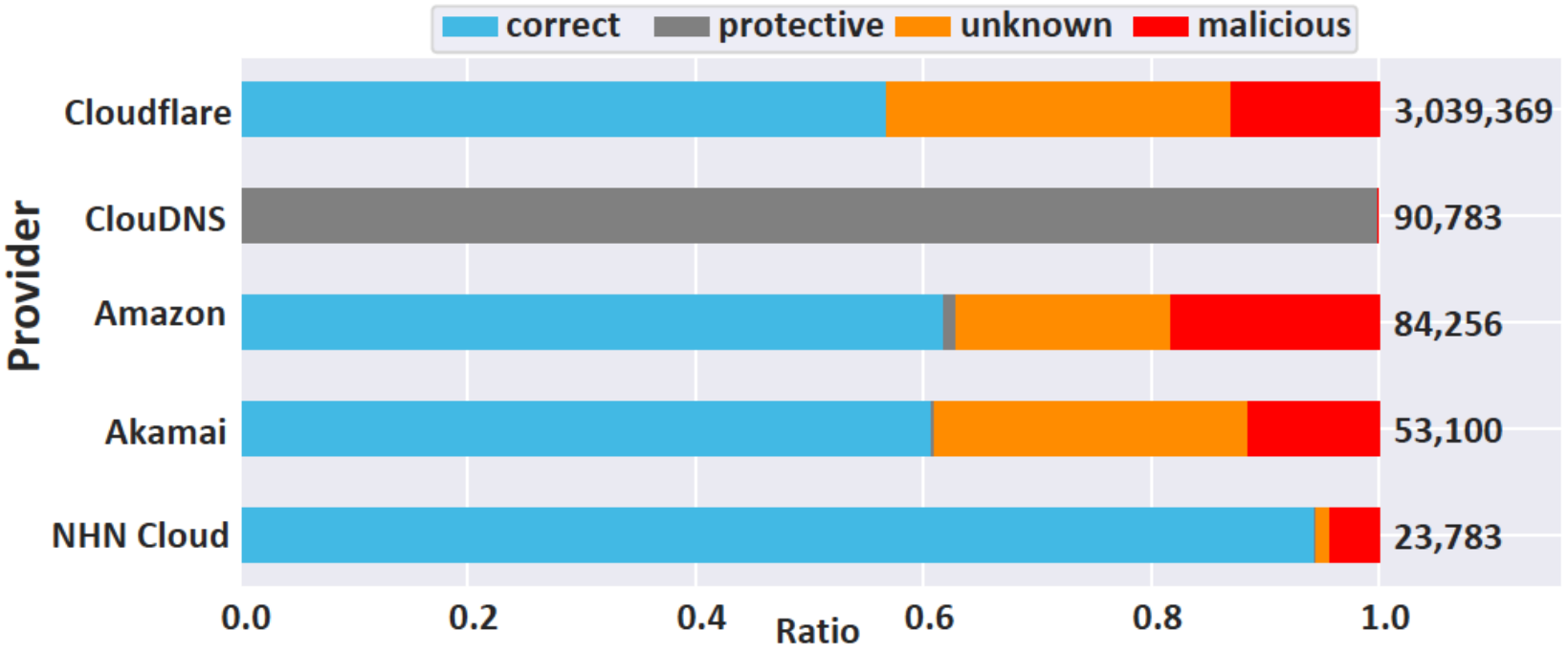


Figure : Categories and proportions of URs among the top five vendors with the most URs.

Measurement: result

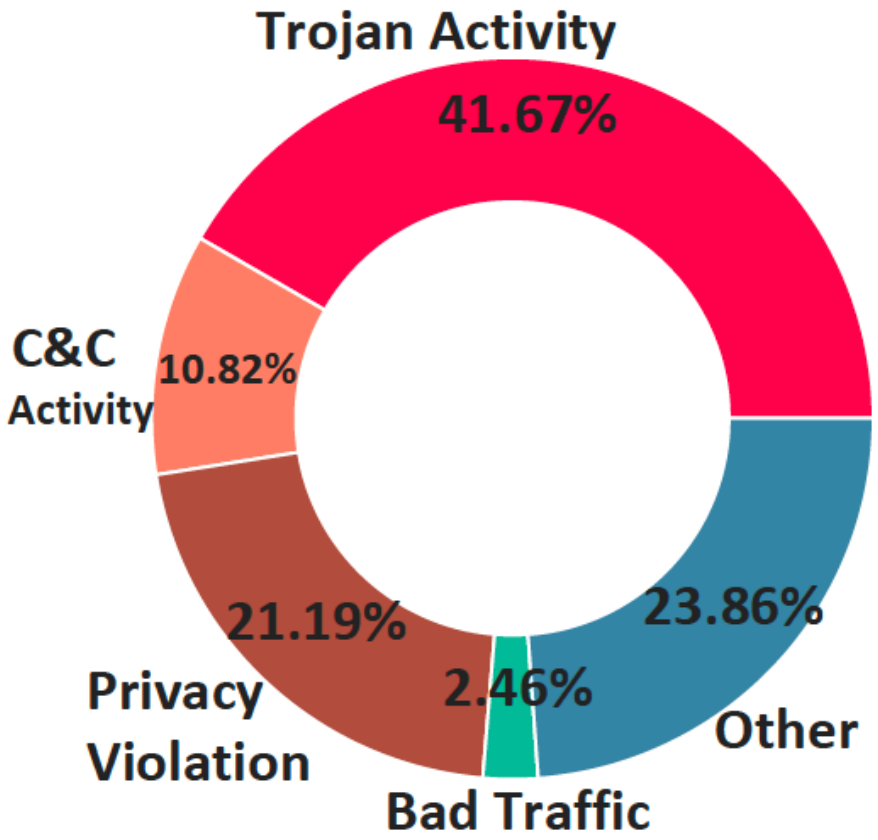


Figure : Malicious activities detected in the traffic toward malicious IP addresses

- **Case 1: Two malware families (Dark.IoT and Specter)** that exploit ClouDNS to obtain C2 servers
- **Case 2:** Masquerading **SPF** records hiding **SMTP-based covert communication**

Mitigation and disclosure

Mitigation

- Verify the ownership of a hosted domain before providing services:
  - Option 1: verify whether the TLD NS records point to the assigned nameservers.
  - Option 2: verify the control of the hosted domain's zone

Disclosure

- We have responsibly disclosed to most of the mentioned providers in this paper.
- Tencent Cloud (DNSPod), Alibaba, Cloudflare, and ClouDNS have taken action to fix this issue.

Conclusion

- We uncover an emerging threat model of covert communication that abuses the **reputations of popular domains and DNS hosting services.**
- We conducted a large-scale measurement and confirmed the URs **are widely exploited in the wild.**
- We provided recommendations for hosting providers to mitigate the revealed threat.

Our code and data are publicly available:
https://github.com/zhangshanfen9/imc-ur

Thanks for listening! Any questions?

zfl23@mails.tsinghua.edu.cn