

Technical Means to Mitigate DNS Abuse

Hongtao Li

China Internet Network Information Center (CNNIC)

September, 2024



中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

DNS Abuse **Detecting**: Challenges & Our Solutions

AI-based Deep Fake Technologies

Adversarial Attack to Avoid Detecting

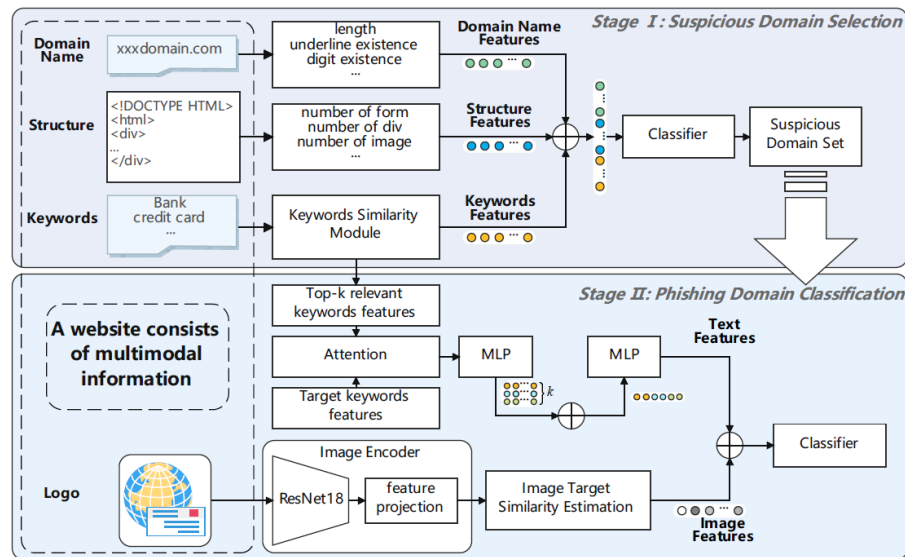
Demand for Large-scale Efficiency

Demand for Global Fast Tracking

Regulation for Abuse Data Sharing

Multi-stakeholders Approach

Two-stages Detecting Scheme: "Fast Filtering + Adversarial Learning"



The average uptime of abused domain names decreases from **12** days to less than **4** days.
Over **120k** phishing domains are identified in recent **5** years.

DNS Abuse **Monitoring** : Challenges & Our Solutions

AI-based Deep Fake Technologies

Adversarial Attack to Avoid Detecting

Demand for Large-scale Efficiency

Demand for Global Fast Tracking

Regulation for Abuse Data Sharing

Multi-stakeholders Approach

Large-scale Analysis Based on Graph Computing



The capability of **DNS Abuse monitoring platform** in large-scale DNS Abuse monitoring has been **improved by 15 times** while using the same hardware facilities, and could complete the scanning of over **160 million** domain names in **1,100 TLDs** globally in just **2 weeks**.

DNS Abuse **Handling** : Challenges & Our Solutions

AI-based Deep Fake Technologies

Adversarial Attack to Avoid Detecting

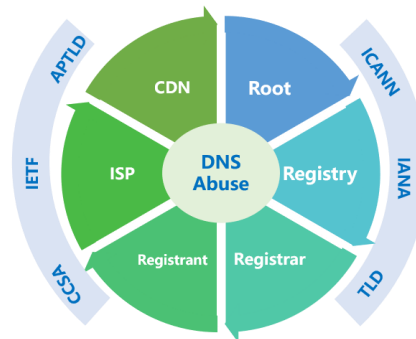
Demand for Large-scale Efficiency

Demand for Global Fast Tracking

Regulation for Abuse Data Sharing

Multi-stakeholders Approach

Data Exchange & Collaborative Standardization



Published **10** domestic standards in DNS Abuse handling, won the **Internet Public Benefit Award** from the Internet Society of China.