# Abuse of the IPv4 Transfer Markets

Vasileios Giotsas, *Ioana Livadariu*, Petros Gigis

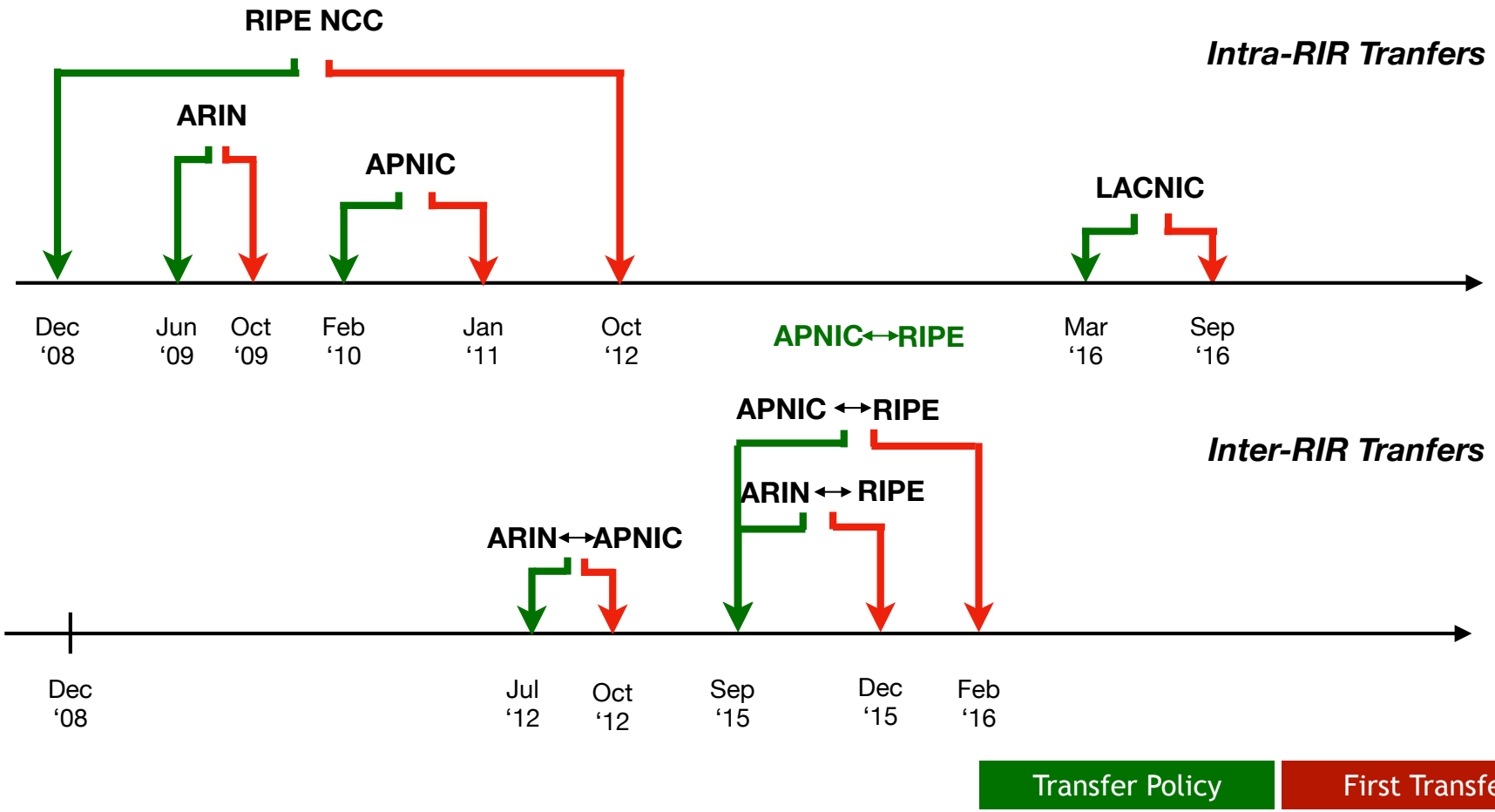
**AIMS 2020**

simulamet

Simula Metropolitan Center for Digital Engineering AS

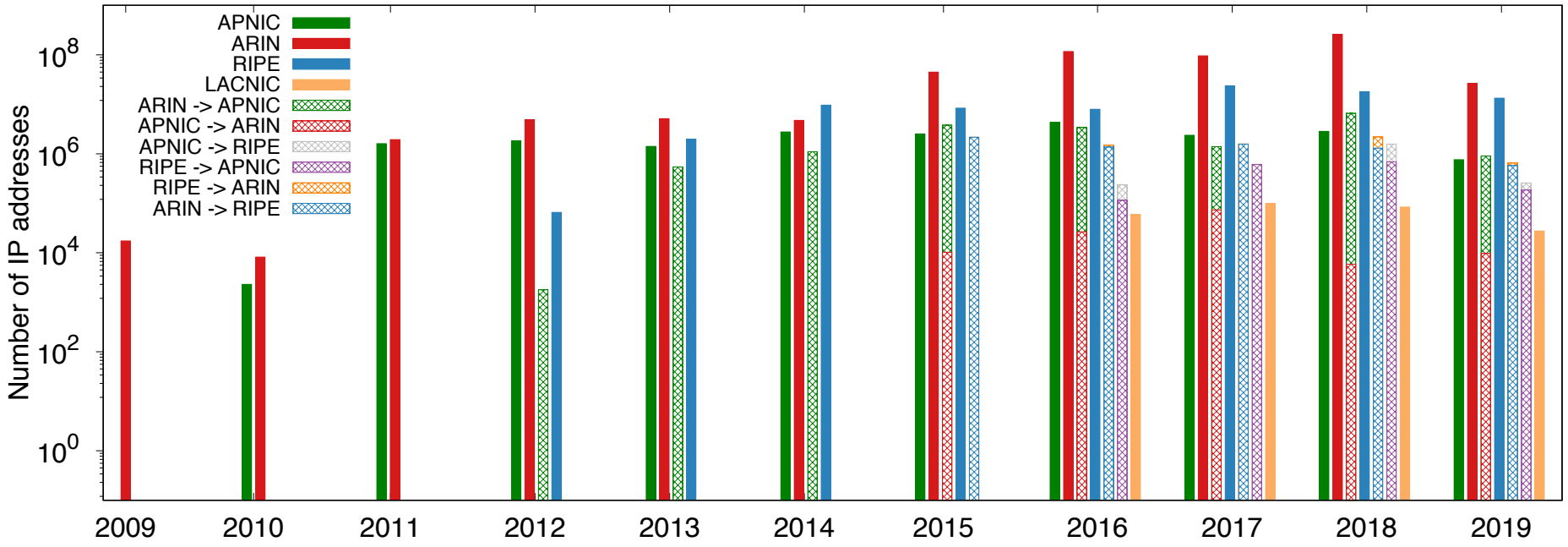
# IPv4 Transfers

IPv4 address transactions that occur between organisations



# Transfer markets: viable source of IPv4 space

Transfer market size is increasing (number of transactions and IP addresses)



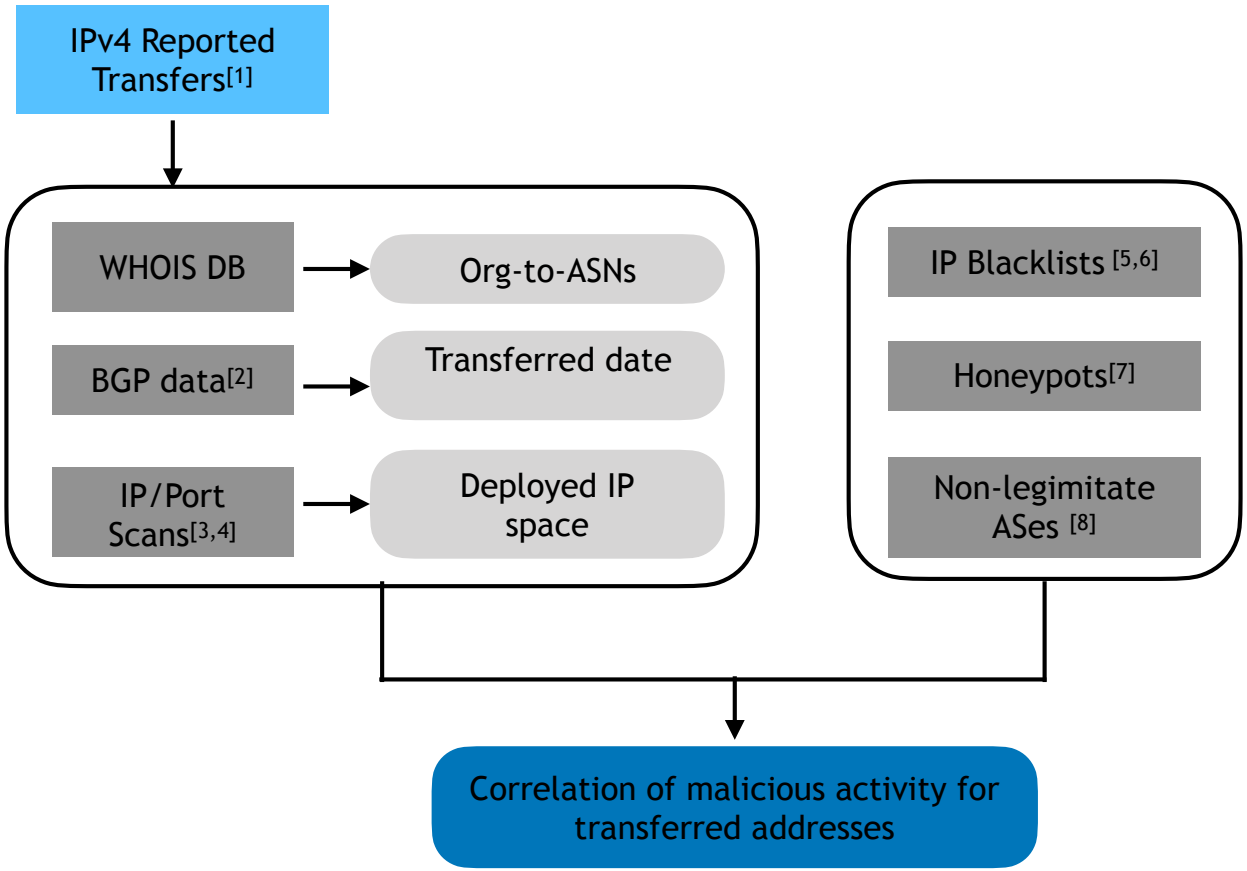
# Overview

*Do IPv4 transfer markets pose an opportunity for malicious actors?*

1. Compile and process the IPv4 transferred addresses
    - Usage of the IP address space
    - Participants on the IPv4 transfer market

2. Analyze the IP addresses against a dataset of malicious activities
    - Blacklisted IP addresses
    - Blacklisting timing

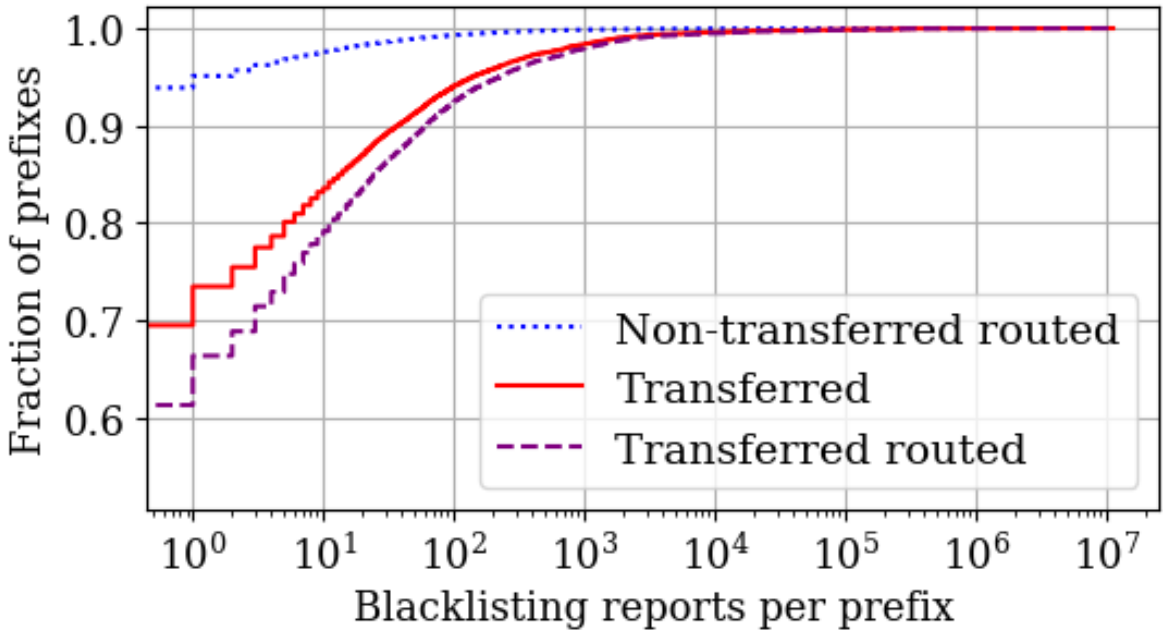
# Datasets




[1] RIRs, IPv4 reported transfers
[2] Routeviews and RIPE RIS
[3] USC/ISC LANDER project, https://www.isi.edu/~johnh/PAPERS/Heidemann09b.html
[4] RAPID7's project Sonar, TCP and UDP scans, https://opendata.rapid7.com/
[5] Zhao *et al.*, A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists, AsiaCCS 2019
[6] UCEPROTECT: Network Project, http://www.uceprotect.net/en/
[7] Badpackets (https://badpackets.net/botnet-c2-detections/), BinaryEdge (https://www.binaryedge.io/data.html)
[8] Testart *et al.*,Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table, IMC 2019

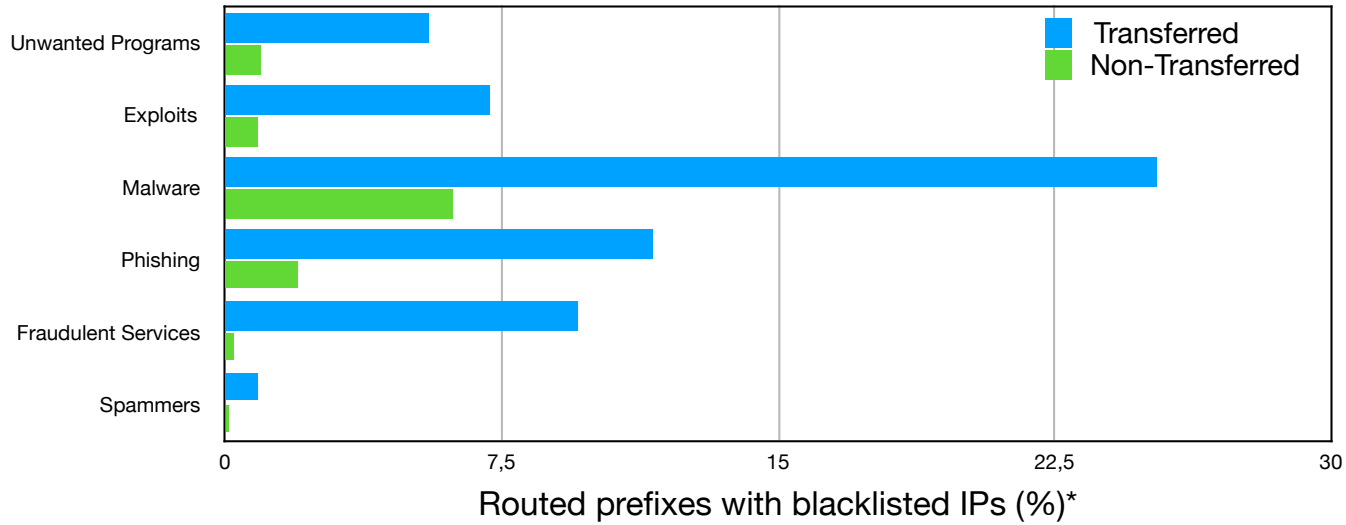
# Significant percentage of the transferred prefixes appears blacklisted

Blacklisted transferred IPs are distributed across 40% of the routed prefixes.



# Significant percentage of the transferred prefixes appears blacklisted

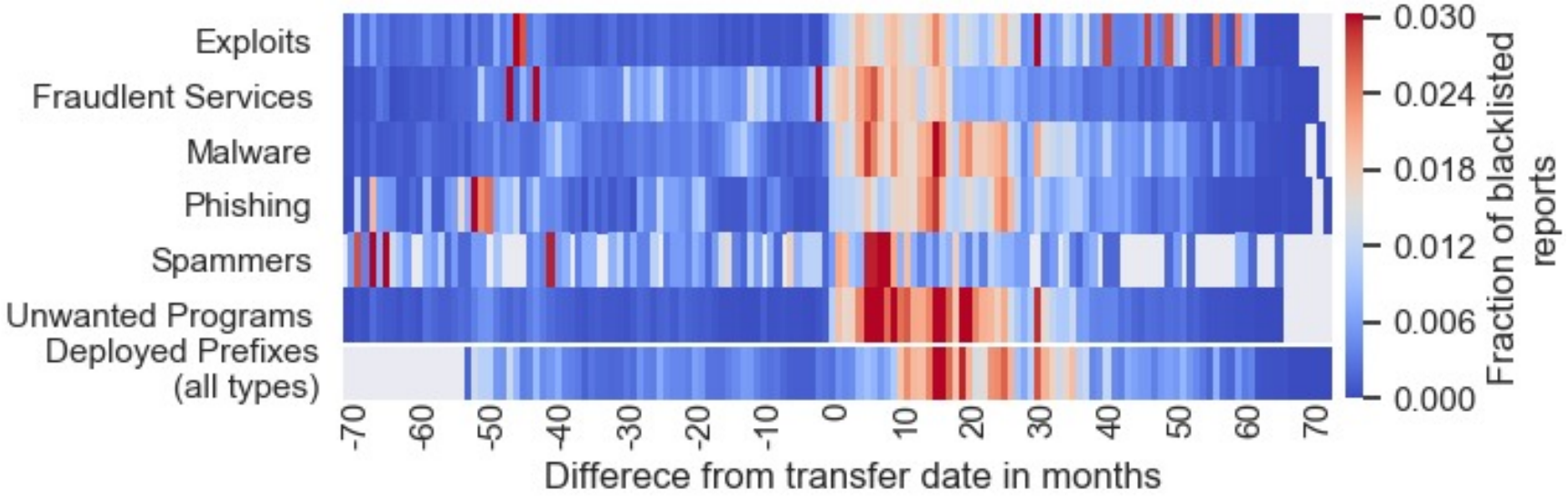
Transferred prefixes are disproportionally represented in the blacklist for every type of malicious activity except spamming




*Zhao *et al.*, A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists, AsiaCCS 2019

# When do the transferred IPs get blacklisted?

- Compare the transfer date with the blacklisting timing
- Buyers are more prone to abuse of the IP space



# Future Work

- Develop predictive techniques for blacklisting based on monitoring the reported IPv4 transfers
- Augment our malicious datasets (IBR, DDoS, Spoofing, Honeypots)
- Investigate non-canonical patterns in the reported transfer (e.g networks are both seller and buyer)