Exploring the Discovery Process of Fresh IPv6 Prefixes: An Analysis of Scanning Behavior in Darknet and Honeynet

Liang Zhao Ⓐ, zhaoliang@nii.ac.jp
Satoru Kobayashi Ⓑ, sat@okayama-u.ac.jp
Kensuke Fukuda Ⓐ Ⓒ, kensuke@nii.ac.jp

Ⓐ

SOKENDAI

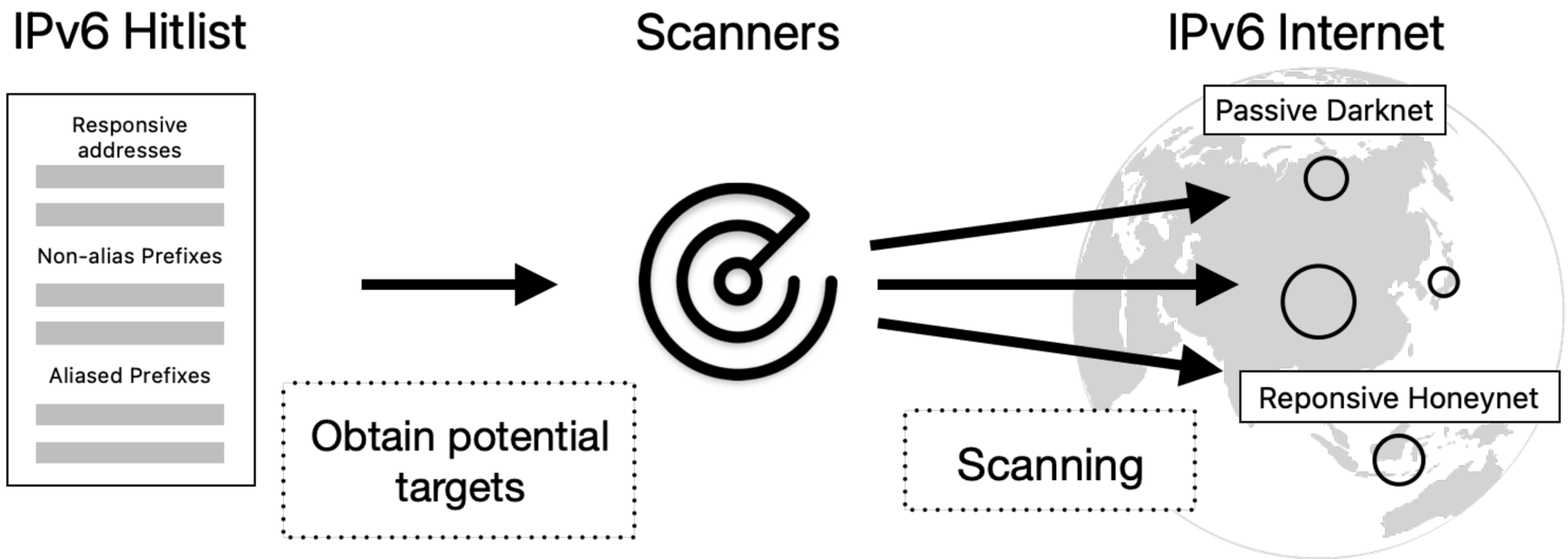
Ⓑ

岡山大学
OKAYAMA UNIVERSITY

Ⓒ

NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
National Institute of Informatics

Background

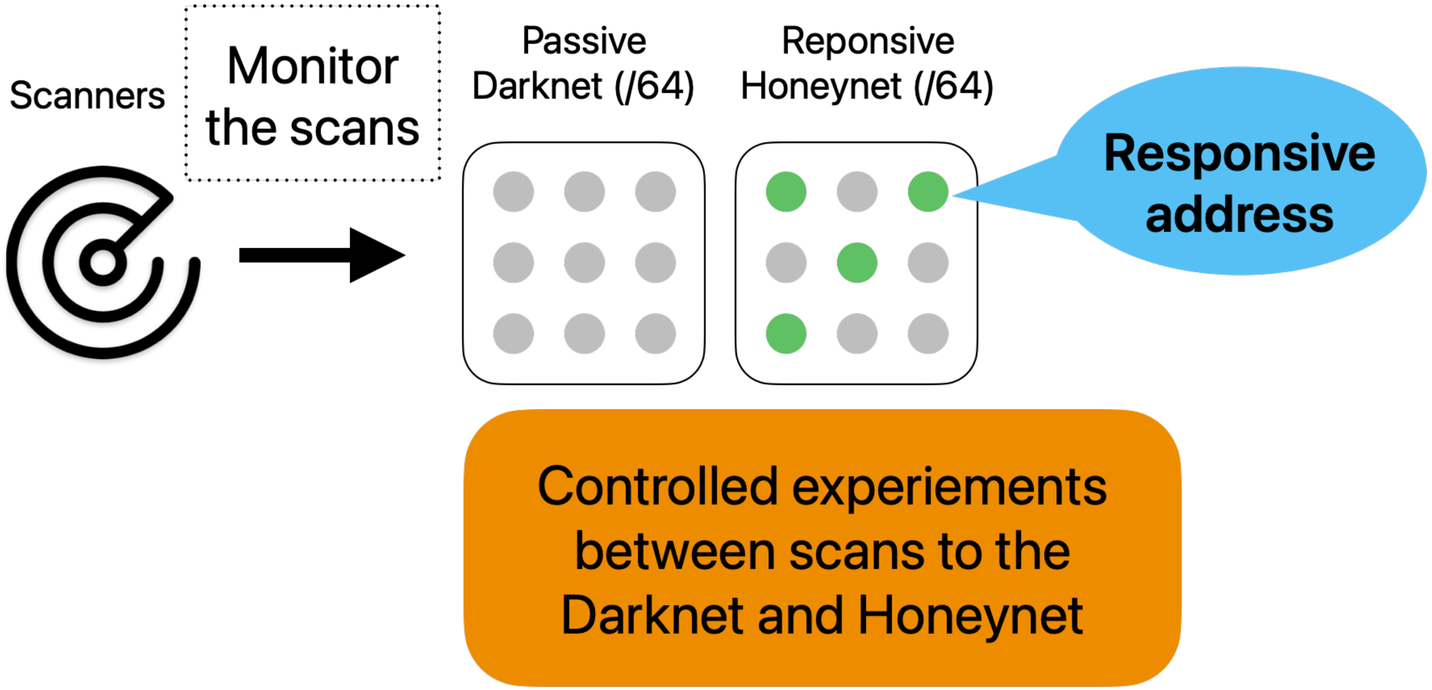


- How do scanners discover fresh prefixes (newly deployed, newly assigned, or previously unused) and what are their intentions?

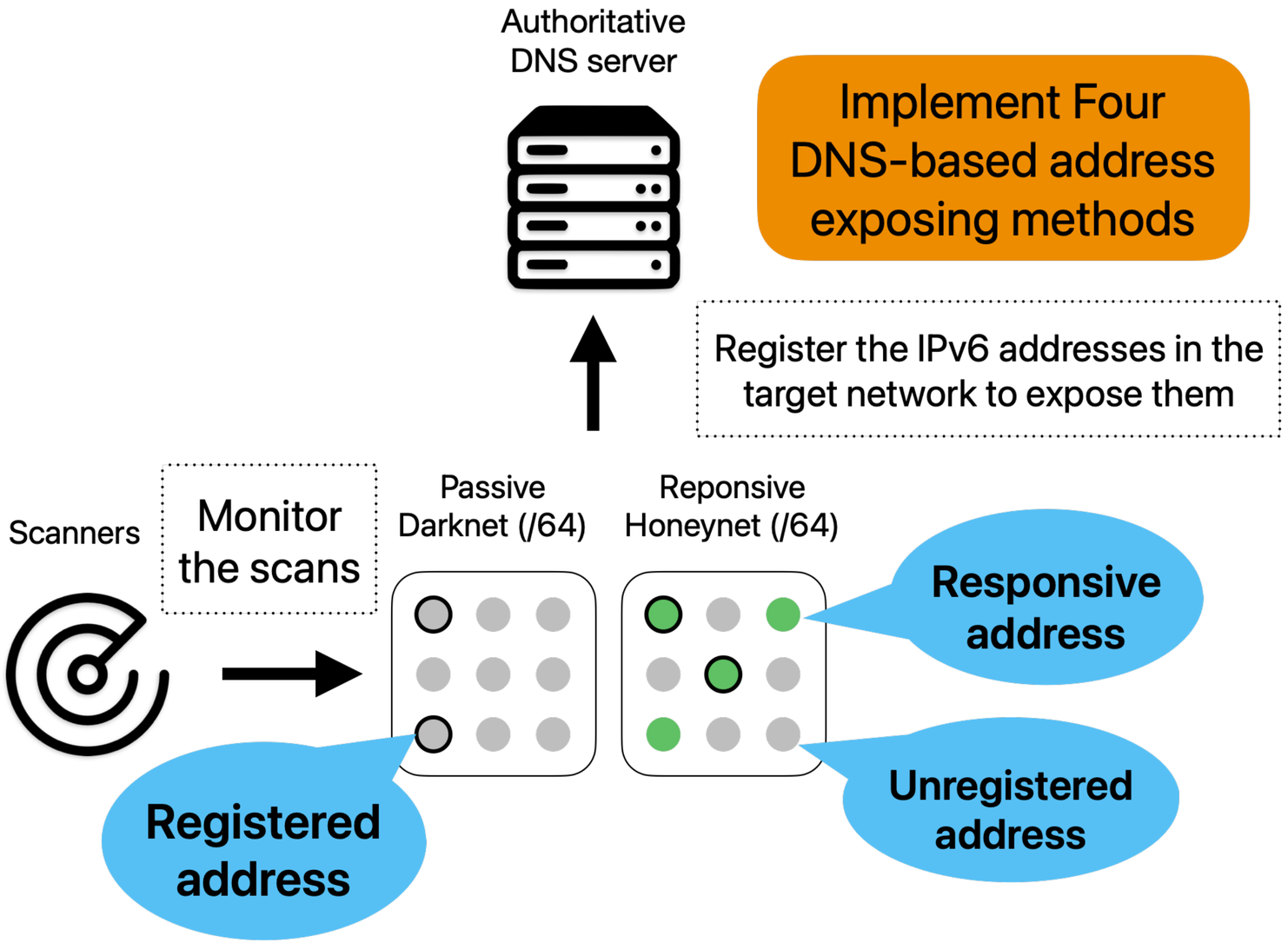
Research Questions

1. How do scanners discover fresh IPv6 prefixes and what is the whole process of it?
2. How does the scanning behavior differ between Darknet and Honeynet?
3. What are the possible intentions of the scanners and how do they obtain the potential targets?

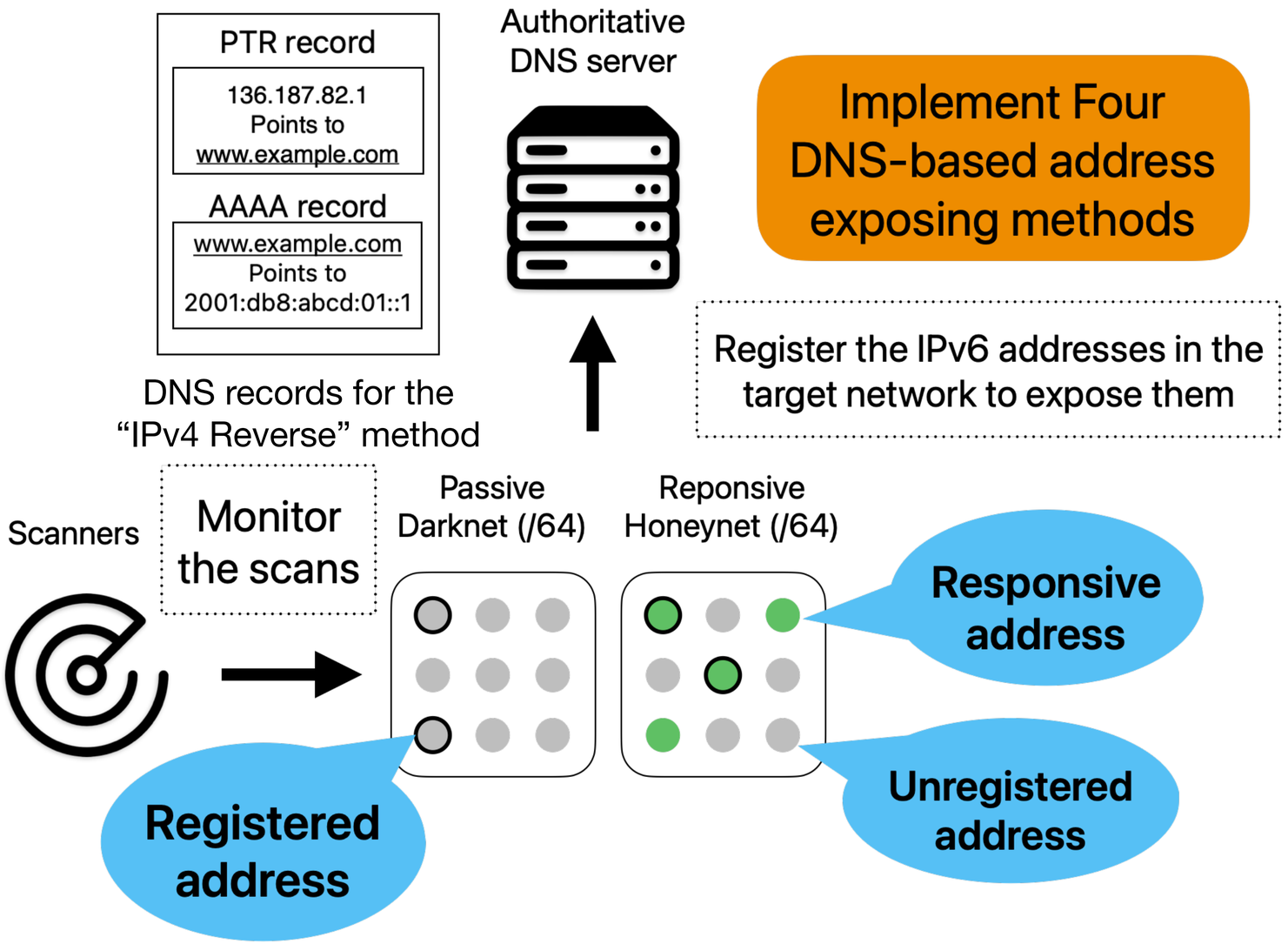
Method


Scanners
Monitor the scans
Passive Darknet (/64)
Reponsive Honeynet (/64)
Responsive address
Controlled experiements between scans to the Darknet and Honeynet

Method

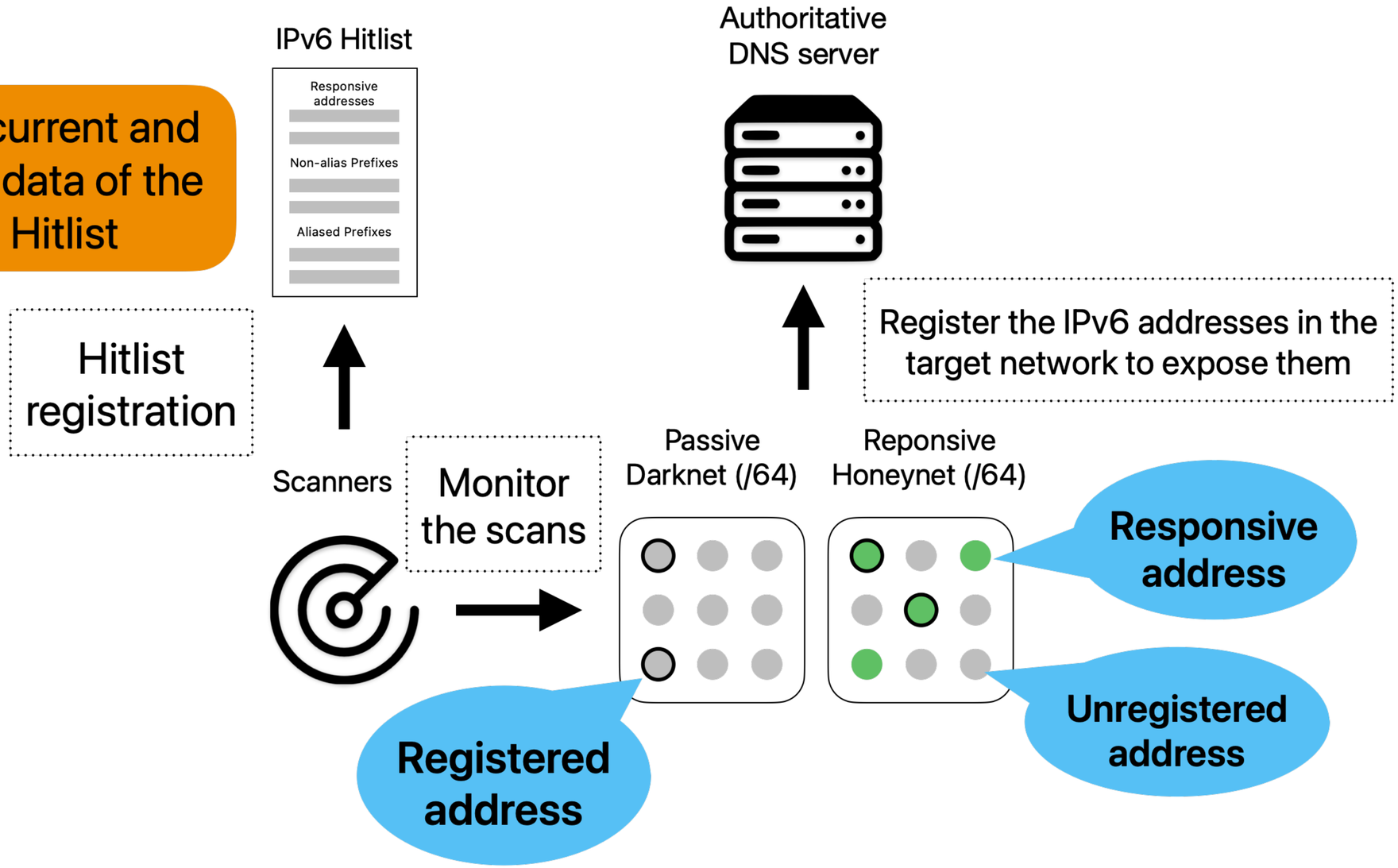

Authoritative
DNS server
Implement Four
DNS-based address
exposing methods
Register the IPv6 addresses in the
target network to expose them
Scanners
Monitor
the scans
Passive
Darknet (/64)
Reponsive
Honeynet (/64)
Responsive
address
Unregistered
address
Registered
address

Method

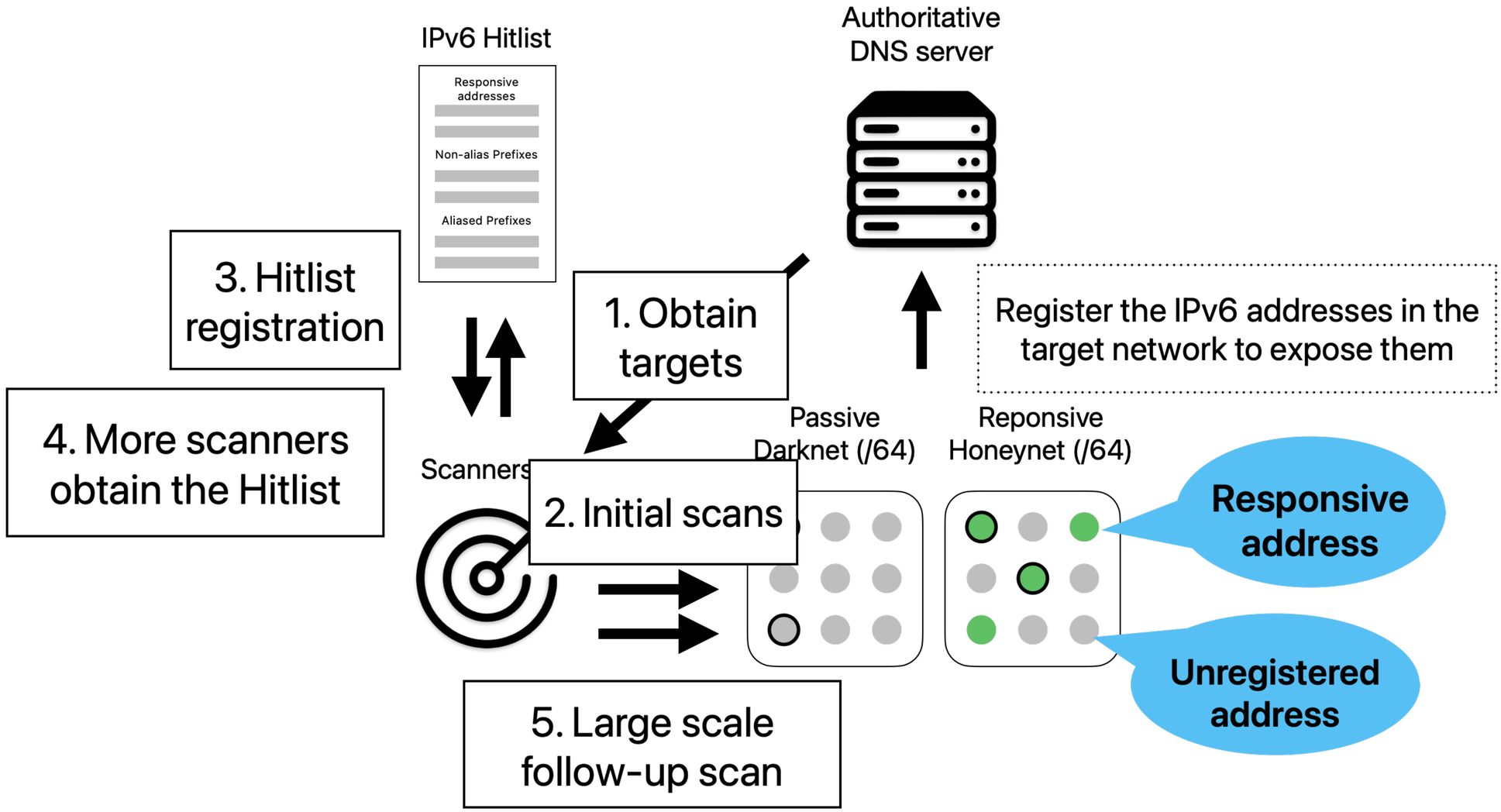

PTR record
136.187.82.1
Points to
www.example.com
AAAA record
www.example.com
Points to
2001:db8:abcd:01::1
Authoritative
DNS server
Implement Four
DNS-based address
exposing methods
Register the IPv6 addresses in the
target network to expose them
DNS records for the
“IPv4 Reverse” method
Scanners
Monitor
the scans
Passive
Darknet (/64)
Reponsive
Honeynet (/64)
Responsive
address
Unregistered
address
Registered
address

Method

Analyze current and historical data of the TUM Hitlist

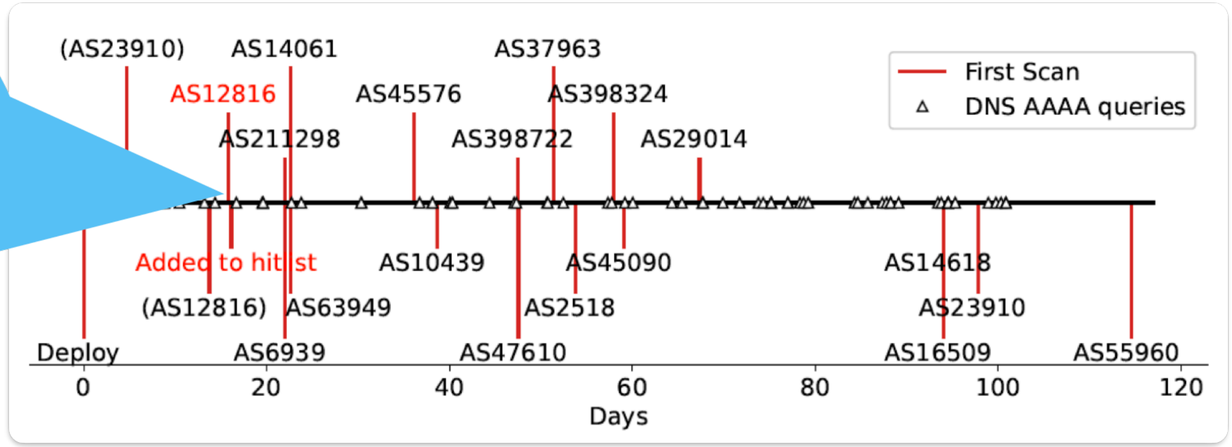


Result (RQ 1): Discovery Process of Fresh Prefixes



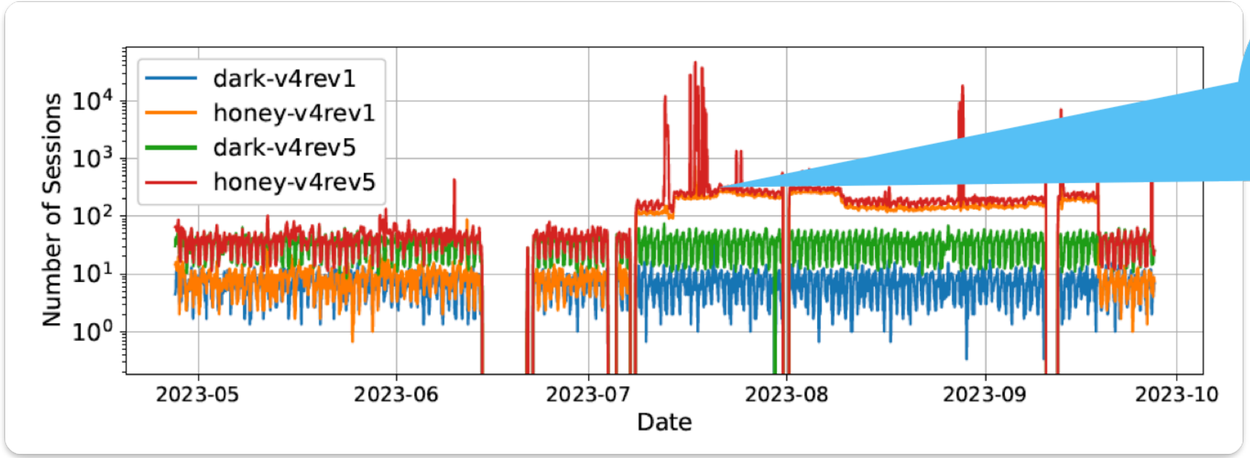
Result (RQ 1): Scans over time

Added to Hitlist around 17 days after deployment



Arrival sequence of the initial scan from each AS in the Honeynet

33M packets from 116 ASes and 18.8K unique IPs

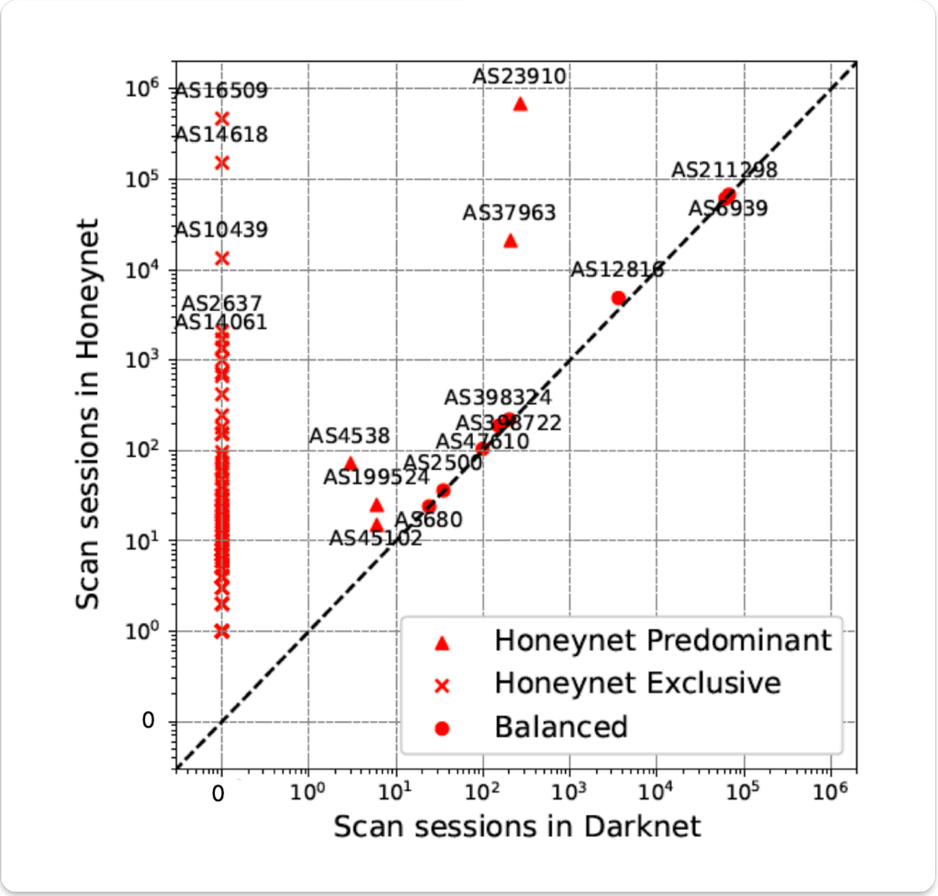


Large scale scan campaigns targeting the Honeynet

Scans over time in the Darknet and Honeynet

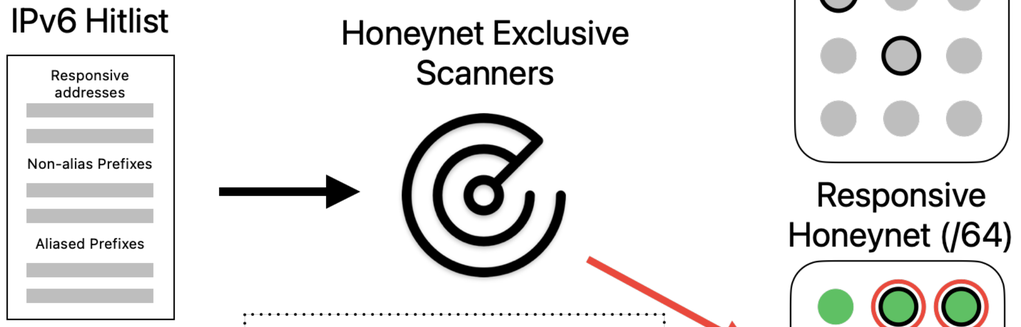
Result (RQ 2): Scanner Types by Targets

- Three types of scanners according to the respective ratio of scans to Darknet and Honeynet
  - Honeynet Exclusive
  - Balanced
  - Honeynet Predominant



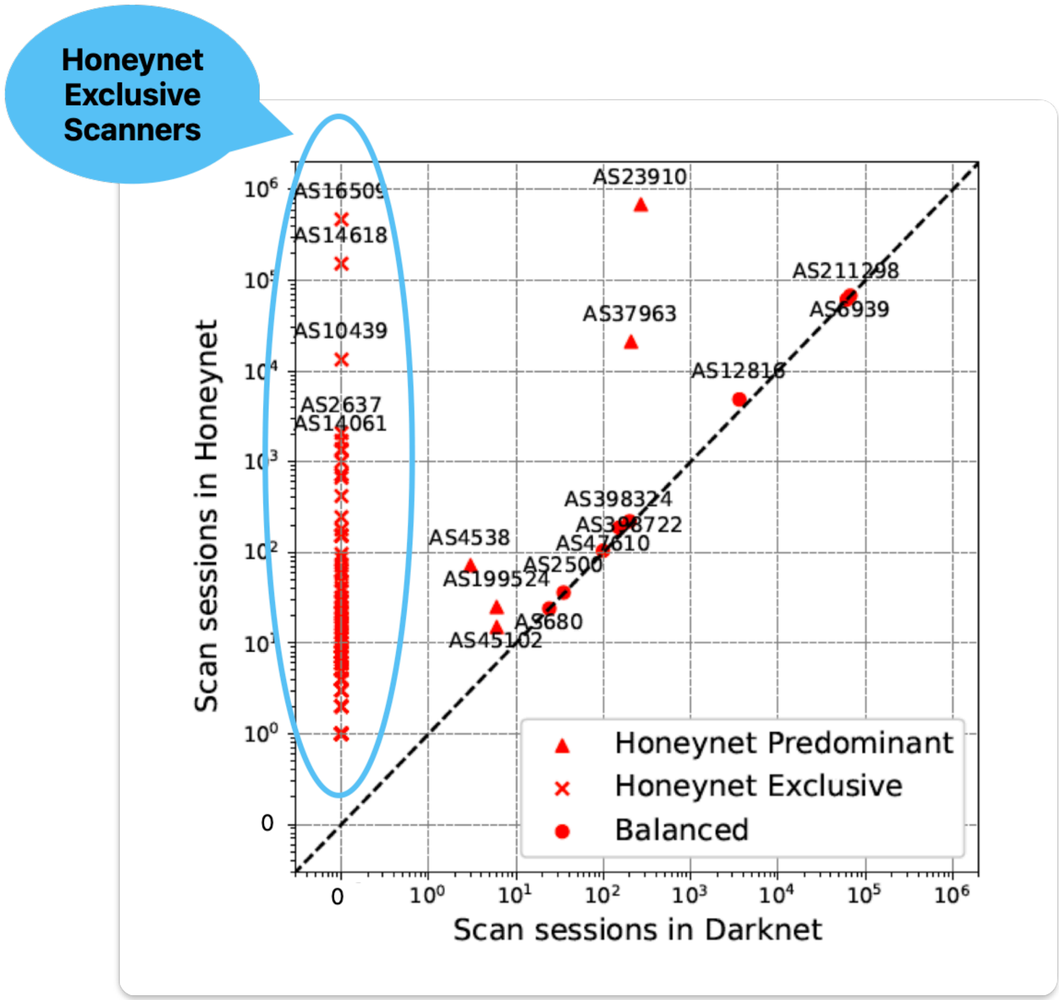
Scans to the Darknet and Honeynet from ASes

Result (RQ 3): Honeynet Exclusive Scanners



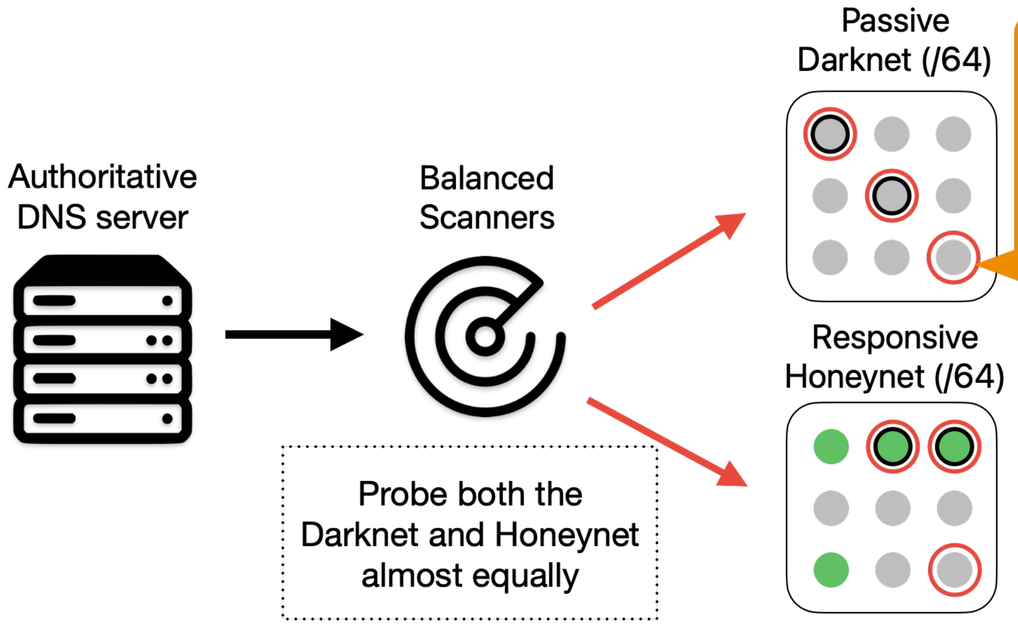
Target obtained: from the Hitlist

Intention: Exploiting the responsive targets



Scans to the Darknet and Honeynet from ASes

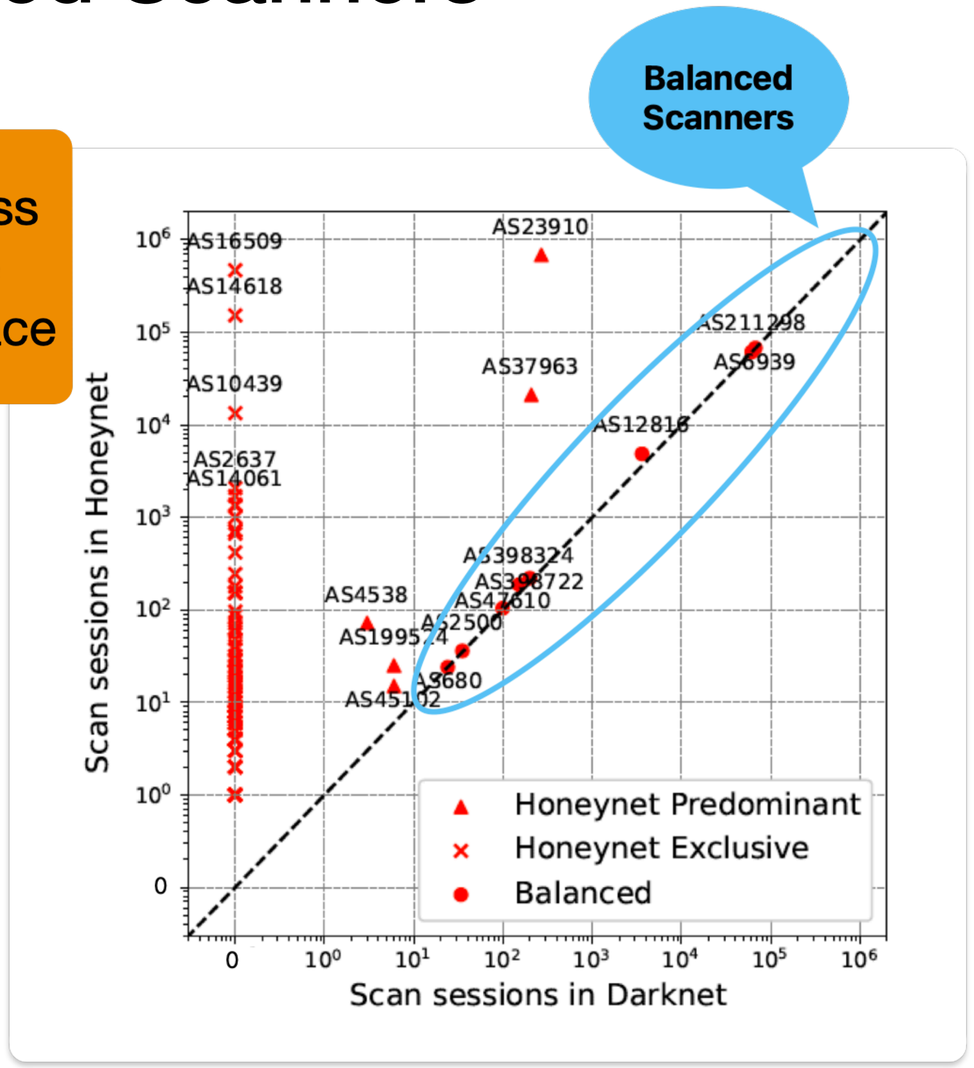
Result (RQ 3): Balanced Scanners



Probe across the whole network space

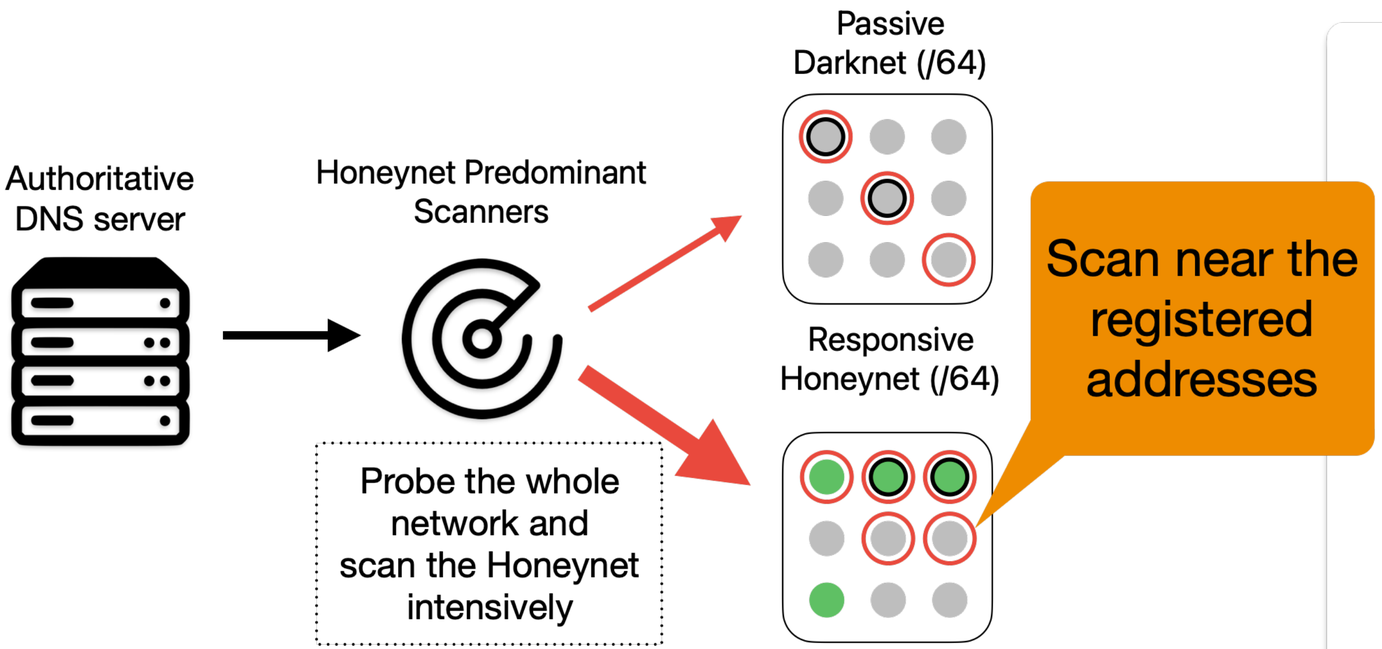
Target obtained: from the DNS server

Intention: Network reconnaissance for research purpose



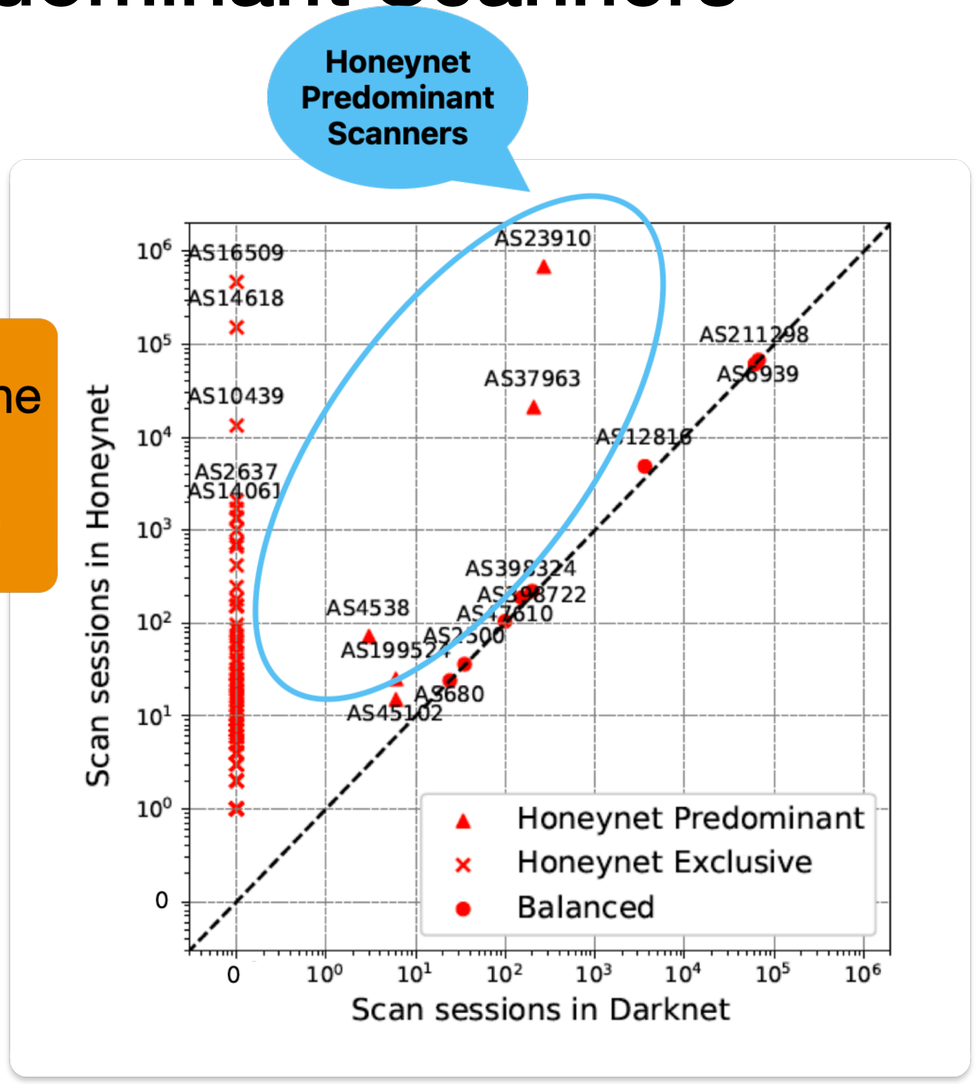
Scans to the Darknet and Honeynet from ASes

Result (RQ 3): Honeynet Predominant Scanners



Target obtained: from the DNS server & through network reconnaissance by themselves

Intention: Exploiting the responsive targets & searching for new responsive targets



Scans to the Darknet and Honeynet from ASes

Conclusion

- Process of fresh prefix discovery

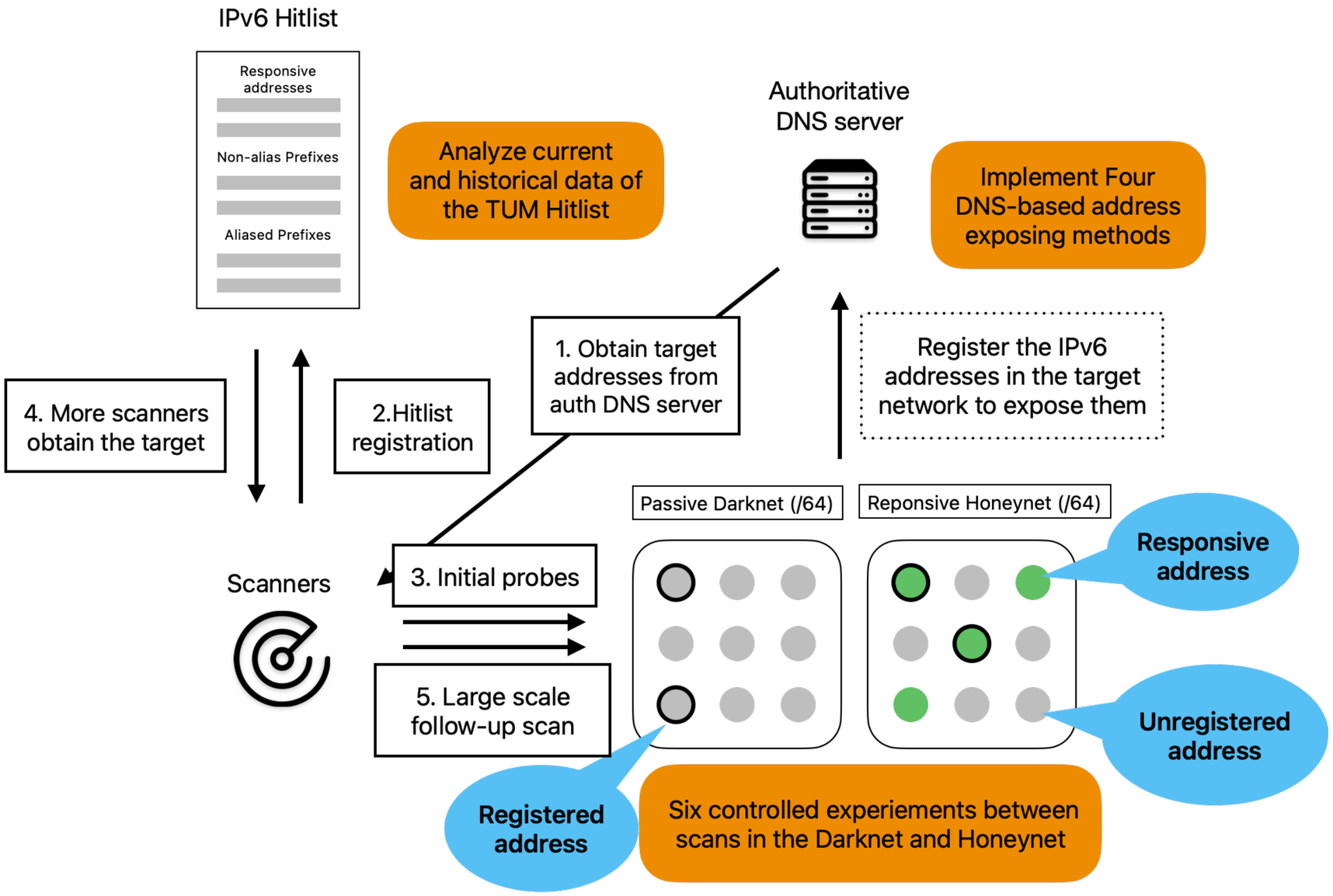
  1) Address exposing 2) Initial probing 3) Hitlist registration 4) Large-scale scan campaigns

- Intention and method to obtain targets with three scanner types

Scanner Type	Target obtained from	Intention
Honeynet Exclusive	Public Hitlist	Exploiting responsive targets
Balanced	DNS queries	Network reconnaissance for research purpose
Honeynet Predominant	DNS queries, Network reconnaissance	Exploiting responsive targets, Searching for new targets

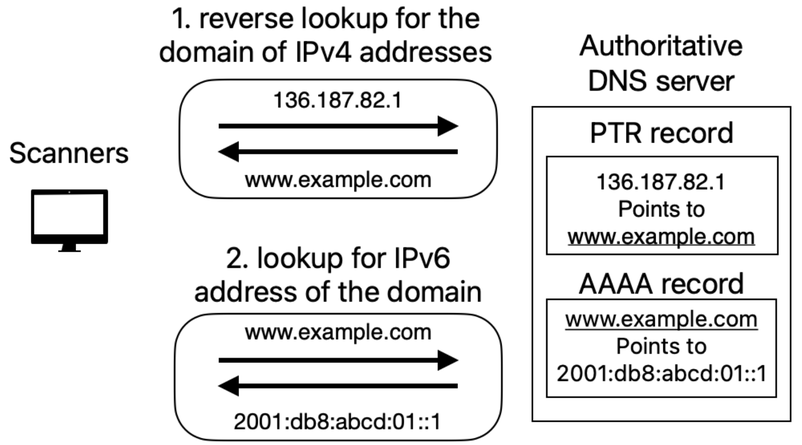
Backups

Method


IPv6 Hitlist
Responsive addresses
Non-alias Prefixes
Aliased Prefixes
Analyze current and historical data of the TUM Hitlist
Authoritative DNS server
Implement Four DNS-based address exposing methods
1. Obtain target addresses from auth DNS server
Register the IPv6 addresses in the target network to expose them
4. More scanners obtain the target
2.Hitlist registration
Passive Darknet (/64)
Reponsive Honeynet (/64)
Responsive address
Scanners
3. Initial probes
5. Large scale follow-up scan
Unregistered address
Registered address
Six controlled experiements between scans in the Darknet and Honeynet

Scan attraction methods

- IPv4 Reverse: associate domains with both IPv4 and IPv6 addresses for the scanners performing IPv4 reverse lookups to discover.
- IPv6 Enumeration: register PTR records of random IPv6 address to be collected by scanners exploiting "denial of existence" semantics of the DNS (NXDOMAIN).
- Special IPv6 Address: register PTR records of special addresses embedded with well-known ports (e.g., 2001:db8::80), or words (e.g., 2001:db8::cafe).
- Popular Service Name: register IPv6 address to domain names with popular service names (e.g., admin, web) to be collected by domain name reconnaissance tools.



IPv4 reverse address exposing method

Related works

- Scan detection: Richter et al. [1] investigated the large-scale IPv6 scanning activities based on firewall logs captured at a major CDN.
  - Their work focuses more on already existing scan activities in the broad internet space.
  - We focus on newly attracted scans in a specific target network.
- Scan attraction: Tanveer et al. [2] propose to attract potential IPv6 scans by direct/indirect scan attraction methods.
  - Our DNS-based methods are similar with the ones in [2], which are proven to be effective in attracting scanners.
  - We did a more thorough and focused analysis of the scans attracted by DNS-based methods.