インターネットトラフィック上の異常を見つける

IPv6ネットワークスキャン検出センサ:

どんな研究？

ネットワークスキャンを検出するセンサを積極的にインターネット上に公開することでネットワークスキャンを誘引する技術を研究しています。

何がわかる？

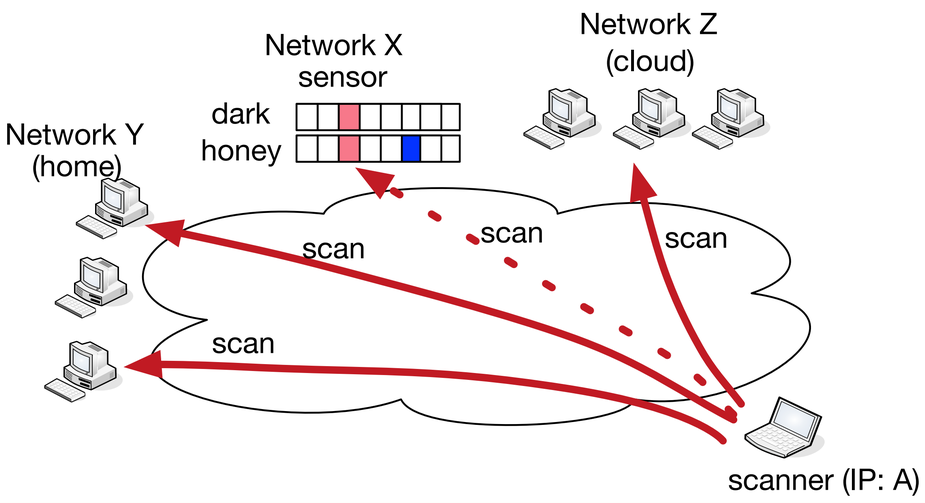
世界中で起きている大規模IPv6ネットワークスキャンを効率良く検出することで、その特徴や傾向を把握しています。

状況設定

- 新たな脆弱性が発見されると，脆弱性を持つホストの探索(スキャン)が始まる
  - 乗っ取られたホストはさらなる被害を引き起こす
- ゴール: IPv6スキャンを行っている送信元を同定したい
- 従来手法:
  - ファイアーウォール(FW)のログを集める (規模拡張性に欠ける)
  - センサネットワークでパケットを集める (パケットが来ない)

研究内容

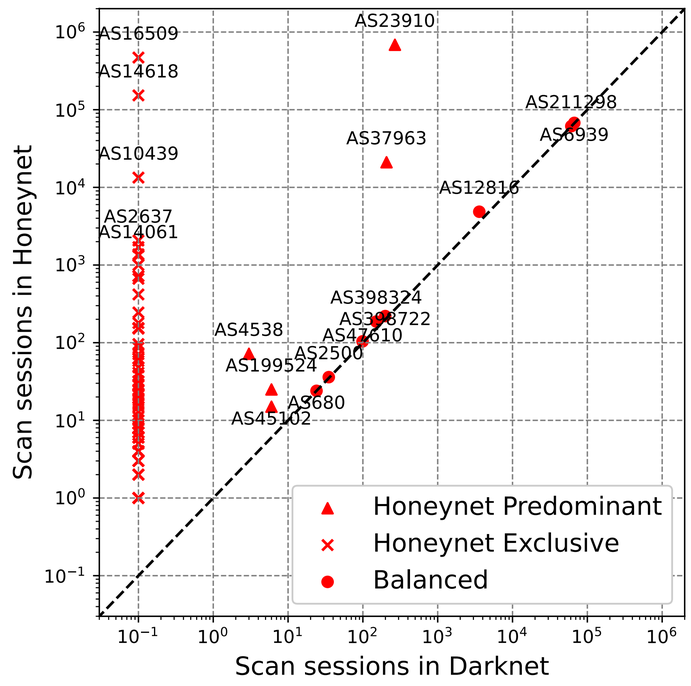
- IPv6スキャン誘引センサの原理
  1. スキャナーはヒットリスト(応答するIPアドレスのリスト)を使用
  2. センサのアドレスを各種手法で公開
  3. ヒットリスト掲載
  4. センサにてスキャンを検出
- 実験環境
  - 2種類のセンサ(dark, honey)
  - 公開手法：5
  - 各センサアドレス空間：/64
  - 観測期間: 2024.04-



- 評価: 公開手法の有用性(IP数)
  - 公開後2週間でリスト掲載

	Darknet	Honeynet
No exposing	5	1
IPv4 reverse	1.7K	2.0K
IPv6 enumeration	2	2
IPv6 special	1	1
IPv6 popular name	4	2

- 評価: スキャンタイプの同定



多くは海外研究機関(米欧中)

- 公開リスト or 自前リスト
- 空間探索 or 応答ホスト探索

“Exploring the Discovery Process of Fresh IPv6 Prefixes” L.Zhao, S.Kobayashi, K.Fukuda, PAM’24

連絡先：福田 健介　国立情報学研究所　アーキテクチャ科学研究系
Email：kensuke@nii.ac.jp