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: DNS backscatter

どんな研究？

脆弱性のあるホストを探すネットワークスキャンを効率良く検出する，DNSを用いたネットワークスキャン検出センサ(DNS backscatter)を作っています。

何がわかる？

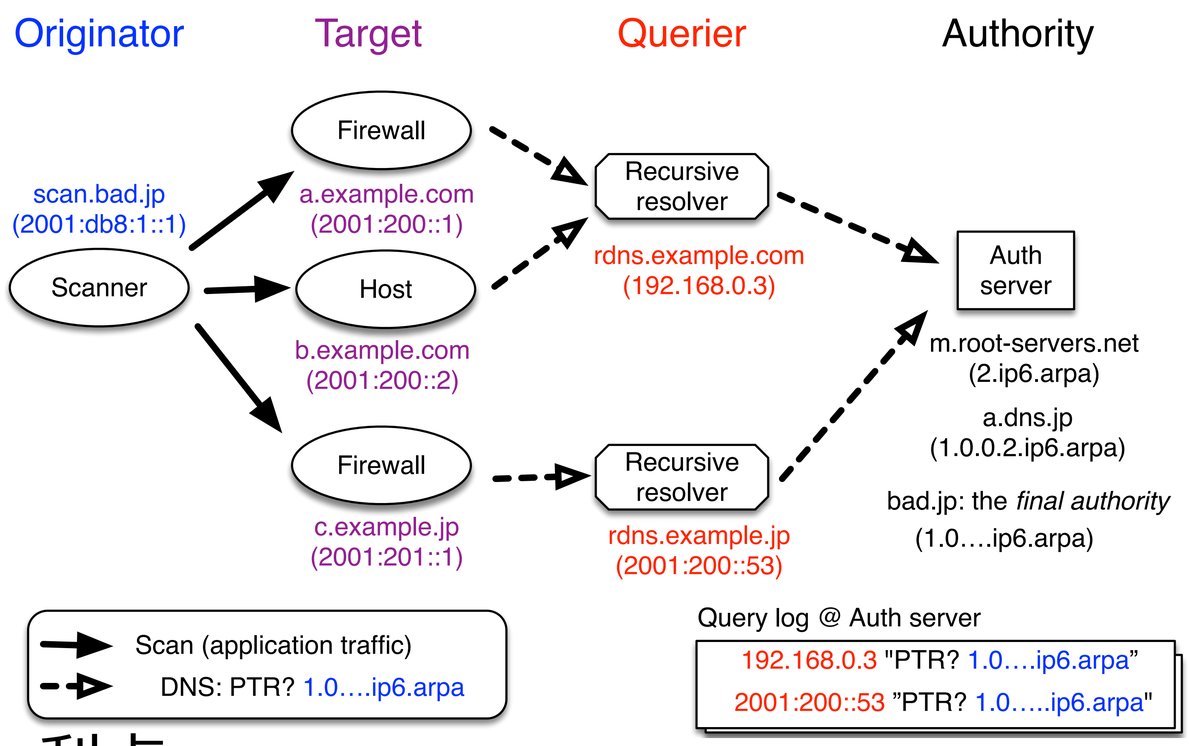
世界中で起きている大規模IPv6ネットワークスキャンの送信元を集中的に効率良く推定することができます。

状況設定

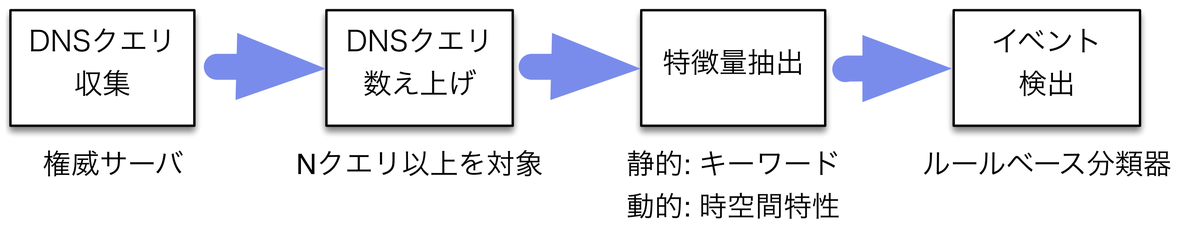
- 新たな脆弱性が発見されると，脆弱性を持つホストの探索(スキャン)が始まる
  - 乗っ取られたホストはさらなる被害を引き起こす
- ゴール: スキャンを行っている送信元を同定したい
- 従来手法:
  - ファイアーウォール(FW)のログを集める (規模拡張性に欠ける)
  - 囮のネットワークに到着するパケットを集める (パケットが来ない)

研究内容

- DNS backscatterの原理
  - FWではスキャナのIPアドレスを(自動的に)調査
  - DNS逆引きクエリが発生
  - DNS権威サーバでクエリを収集



- 検出の流れ



- 評価 (@B-Root DNSサーバ)

Category	Count (mean/week)	% total	
Services:			
Content Provider	**4722**	**70.24**	多くは正常なサービス(コンテンツプロバイダ)
Facebook	3653	54.34	
Google	727	10.82	
Microsoft	329	4.89	
Yahoo	13	0.19	
CDN	**286**	**4.25**	
Well-known service	**815**	**12.12**	(ネットワークサービス)
DNS	337	5.01	
NTP	414	6.16	
mail (SMTP)	42	0.62	
web (HTTP)	22	0.33	
Minor service	**268**	**3.99**	
other services	83	1.23	
qhost	185	2.75	
Routers:			
Router	**288**	**4.28**	Tracerouteの影響
iface	256	3.81	
near-iface	32	0.48	
Tunnel	**216**	**3.21**	
Teredo/6to4	207	3.08	
tor	9	0.12	
Potential Abuse:			
Abuse	**128**	**1.90**	異常(スキャン，スパム)
spam	17	0.25	
scan	16	0.24	
unknown (potential abuse)	95	1.41	
Total	**6723**	**100.00**	

- 利点
  - 中央集権で新たなセンサなし
  - プライバシに優しい
  - スキャナが隠れることは困難

“Who Knocks at the IPv6 Door? Detecting IPv6 Scanning” K.Fukuda, J.Heidemann, ACM IMC’18

NII
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