WHOIS の正確性と公安

発表の目的

- 公安のためのWHOISの利用
- 現在のWHOIS正確性における課題
- 不正確なWHOISに関する事例
- グローバルに調整する(globally coordinated)WHOIS正確性に関するポリシー提案に向けた原則

WHOISの利用

RIRコミュニティに限らず, WHOISは公共に利用されている:

- 世界的なIPアドレスの分配先が適切に登録されることで、個人、消費者および市民が、公安を脅かす悪質な行為に対応できる能力
- ネットワークのセキュリティおよび安定性の確保
- 企業、消費者団体、医療組および他の団体による不正行為への対応の支援
- 一般市民に対する安全に責任を持つ組織への支援

公安におけるWHOISの利用

- WHOIS検索は、以下に加え、調査に利用する **数多くあるツールのひとつ**：
  - 経路テーブル・経路情報に関するサービス
  - 市販の商用ツール
  - 内部で開発したツールおよびサービス

- しかし、WHOISは多くの調査において**まずはじめに利用するもの(starting point)**

目下の課題

- **配下のIPアドレス分配における正確性の課題**
  - ISPへの二次割り振り(Sub-allocation)情報が多くの場合、当初の分配先から変わり、不正確で古いデータ
  - RIRごとに二次割り振りに関する二次割り振りのポリシーおよび要件が異なる傾向
- **問題の拡大**
  - IPv6 – ISPがさらなるアドレス空間のため追加割り振り申請を行わず、二次割り振り情報を登録しない可能性
  - IETF MODERN Protocol – VoIPへのシフト
  - IOT
- **業界としての対策を模索**
  - ARIN (および他のRIRコミュニティ)と最適な対策をつくりたい

課題

公安の観点から、WHOIS情報の正確性を保つことに失敗すると以下の課題に直面する:

- 公的安全機関が不正活動の元を迅速に特定できない
- 誤った法的要請は公的安全機関およびネットワークオペレータ双方の時間を無駄にする
- IPアドレスのハイジャックは、それらのアドレスを利用した複数の犯罪行為につながる可能性をもっている

事例紹介

事例紹介

- 2013年7月、セキュリティ組織が企業AがIPアドレスを盗み、数百万のスパムメールを配信していることを法執行機関に報告
- 企業Aは、数百～数千万のIPアドレスをハイジャックし、史上最大のスパマーとした容疑
- 企業Aはスパムのキャンペーンを行うためにWHOISの不正確で古い情報を見つけ出し、登録者になりすました登録情報変更を立て続けに実施

From: CA Business Ops Manger Sent: Monday, February 11, 2013 10:25 AM ***To: CA Manager*** ***CC: CA Tech. Ops Mgr***	"Just got the logins to the domain. Working on setting everything up now. Will have an email/LOA to you soon from @surfa.net"

DEA の事例

時間がいつもお金に引き換えられるものではない、命が引き換えになることもある

すべての捜査はインターネットに携わる。前述の通り、WHOIS検索は捜査の第一歩に使われる。以下は麻薬の過剰摂取に関する過去数ヶ月の統計。

- 2016年7月27日: 1ヶ月で200を超える過剰摂取 Akron, Ohio地域.
- 2016 年8月15日: 4時間で27を超える過剰摂取 Huntingdon, WV 地域.
- 2016 年8月29日: 6日間で174を超える過剰摂取 Cincinnati, Ohio 地域.
- 2016 年10月20日: 過剰摂取による死亡が今月Delray Beach, Florida.

これらの状況下で、公的安全組織は、生活パターンを確立し、麻薬乱用者の供給元の特定に迅速に対応しなければいけない

カナダにおける状況紹介

- R v. Spencer decision
- NCECC – 現在まで今年19,000件 の苦情
  - ほとんどのものは児童ポルノに関わるIPアドレス
  - WHOISは、要請を行う法執行機関を特定する第一歩
- WHOISは被害者捜索にも利用 – 最近33,000個のカナダのIPアドレスが押し売りウィルス(ransomware)に冒されていた
- 2016年3月、若い女性をヌードと性的な動画のためにゆすり取っている男性の捜査
  - 容疑者の情報を得るうえで四つの法廷からの命令(production orders), と3ヶ月を要した
  - 下流ISPに関するWHOIS情報が最新であればこのうち、うち三つの法的からの命令は防げた
  - 2016年6月逮捕、しかし逮捕の遅れは、この期間、容疑者が女性および他の被害者を脅し続けられたことを意味する

ポリシー提案

ポリシー提案　2017

- **ポリシーの幻想**
  - すべての二次割り振りが正確にWHOISに反映されるため下流ISPへのすべての二次割り振りの登録を必須とする
  - エンドユーザに関する情報開示は求めず、代わりに接続を提供している下流ISPの情報に焦点を絞る
  - コミュニティ全体への利点
    - 市民および業界コミュニティ双方にとって、効果的なインシデント対応につながる
  - ポリシー要件に従うようことを促す方法は？
    - 動機付け?

今後の対応

- **RIRと法執行機関によるグローバルに連携した対応**
  - LACNIC: Costa Rican Police and DEA – done Sept. 2016
  - APNIC: Sri Lanka Police – done Oct. 2016
  - ARIN: DEA, RCMP and FBI – done Oct 2016
  - RIPE NCC: Europol and Spanish Guardia Civil – done Oct 2016
  - AfriNIC: Mauritius Police and African Union – to be done Dec. 2016

- **2017年春に統一したポリシー提案を予定**
  - 全五つのRIRコミュニティの協力を得ながら策定
  - 各RIRミーティングで2017年春に提出予定

- **業界からの支援**
  - 業界主導の対策のためにARIN/RIRコミュニティと連携

目標(GOALS)

- 現在から2017年春までに、コミュニティが支持するWHOIS正確性に向けたポリシーを全RIRと一緒に取り組む
- グローバルに連携したポリシー提案(globally coordinated)を各RIR地域で2017年春に紹介
- 2017年秋に施行

THANK YOU