突然の問い合わせにどう対応するか？

高倉弘喜
国立情報学研究所

高倉弘喜

- H2年 九州大学卒
- H4年 九州大学大学院修士課程修了
- H7年 京都大学大学院博士後期課程修了 博士(工学)

  京都大学研究員、米国イリノイ州立大学訪問研究員、
  奈良先端科学技術大学院大学助手、
  京都大学講師・助教授(准教授)
  名古屋大学教授…どんどん東へ
- H27年 国立情報学研究所教授
  - SINET SOCの構築準備
- サイバーセキュリティに関する各委員
  - NISC、総務、経産、IPA、京都府警、愛知県警…
- サイバーセキュリティ対策(攻撃識別＆被害軽減)研究に従事

関係機関からの打診

- 都道府県警
  - 他県からの問い合わせも珍しくない
    - ほぼ同時に複数から…
- JPCERT/CC
  - 後追いで警察から連絡がある場合も
  - 第三者からの苦情を仲介
    - 第三者が海外の場合もある
- 監督官庁
  - 官公庁系、地方公共団体、独法
    - NISC(GSOC)からの伝言
- 弁護士
  - 時々自称弁護士からも連絡がある

正規の問い合わせでは…

- 最初は詳しいことを教えてくれない
  - このIPアドレスのマシン
    - 不正アクセスを受けている疑い
    - 利用者は特定できますか？
    - ログを頂けませんか？
      - ✓ どのログ？→出していただけるものでしたら何でも
  - 第三者への被害の有無は教えてくれない
- 一番困るのは…担当者や担当部署への直電
  - 技術的にも法的にも意味を理解できない
  - そもそも当事者なのでは…
    - 「問い合わせを受けたらCSIRTへ第一報を！」の啓発

捜査関係事項照会書に書いて欲しいこと

- 範囲：どんな情報が希望なのか？
  - マシンの所在確認は必要か？
  - 使用者の特定は必要か？
  - ログの指定
    - マシンのログ、proxy等のログ、セキュリティ監視系ログ…
  - 外部からの接続の有無も調べたほうがいいのか？
    - あれば、その情報も出しましょうか？
  - ネットワーク構成
- 理由：なぜその情報が必要なのか？
  - 大抵、無回答
  - 念押しして「捜査上必要なため」

水面下で何を持っている
情報のやり取りが必要に

内部での調査

- 学術機関の場合
  - マシンの管理者はそれぞれの教職員
    - 大学本部で管理しているのはごく一部(これらは滅多に事故らない)
  - 学生というお客様
    - 雇用関係はない者による私物PCの持ち込み
      - ✓ 大学側にも調査権限がない…BYODの普及で企業でも
  - 学会や公開講座等の参加者
    - そもそもどこのどなたやら…
      - ✓ 一応、ネットワークを使わせた担当者や学会に責任があるが…
      - ✓ 海外だと学会損害賠償保険を義務付けてることも
- 捜査関係事項照会書の内容を伝えていいのか？
  - 不正利用されただけという確信が持てるか？
  - 下手すれば、証拠隠滅や逃亡…

被疑マシン上のログ

- 不正利用されている…多分root権限も取られている
  - ログが信用できない
    - 法的な証拠としても使えない
  - IoT機器の不正利用だとログなんかない
    - 複合機、Webカメラ、NAS、テレビ会議システム、多機能電球
    - PLC(制御系)
- 対外接続点での監視ログが必須
  - IDS/IPS、FW、proxy…
    - セッションログが嬉しい…転送バイト数から色々と推察
  - ログを解析すると、お問い合わせの理由が見えてくることも
    - 単純な被害者 or 被害者＆加害者
    - 加害者としての責任範囲
      - ✓ 私物の任意提供を勧めるか否かの判断材料

SYNパケットで
10バイトずつ
持ち出し

弁護士

- 法人なら顧問弁護士にまず相談
  - たまに、「わし、ハイテク苦手やねん」で逃げられるけど…
  - 素人判断は極めて危険
    - サイバー犯罪に詳しい理系教授とか…
      - ✓ 法令を仕様書の感覚で解釈する癖が出ることが
      - ✓ 法律の文言
        - 時代変化に応じて柔軟に解釈できるよう曖昧に書かれている
        - 判例の積み重ねで解釈が固まっていく
          - ときどき、最高裁がちゃぶ台返しを…
  - ただ、国際犯罪だとさすがに厳しい
    - 損害賠償だって半端じゃない額がありえる

肥大化するログサイズ

- 1日当たりのログサイズがテラバイトを超えることも
  - 例：http://www.hogehoge.com/ へのアクセス履歴半年分
    - クラウド上のサーバ
      - ✓ 数日単位でIPアドレスが点々と…
    - 水飲み場型攻撃のサーバ
      - ✓ 有名サイトへ or その広告サイトへのアクセスログ
  - DNS queryのログ × セッションログ(IPアドレスのみ)
    - 数テラバイト × 数テラバイトの突き合わせ × 調査対象日数
  - http proxyのログ
    - 数テラバイトのfull textスキャン × 調査対象日数

→抽出するだけで1週間なんてのはざらに

  - お問い合わせに備えた、軽量なログの保存も必要
    - とりあえず何でも取っておけは難しくなっている

マスコミ対応

- 出せる情報はさっさと出しておく
  - 警察発表後の記者会見は最悪のパターン
  - 問い合わせ
    - 「Webで発表している通りです」で返す
- 出してはいけないマシン管理者
  - 「自分も被害者なのに…」な感情が滲み出ることが
    - 同情してくれるのは被害経験者のみ
    - 編集…切って貼っての罠
  - 謝罪会見慣れしていない役職者も要注意
- (粗方の)原因究明後の(中間)最終報告公開
  - 情報が短時間で二転三転するのはよろしくない