コンピュータセキュリティシンポジウム2018
新企画セッション「サイバーセキュリティ研究のグレーゾーン」

サイバーセキュリティ研究におけるグレーゾーン

2018年10月24日(水)

西村あさひ法律事務所
弁護士 北條孝佳

サイバーセキュリティ研究の課題 2

- サイバー攻撃全般の研究
- 脆弱性検査(ペネトレ)の研究
- 匿名化通信を破る研究
- ハニーポットによる攻撃手法の把握
- ビッグデータの分析手法の研究
- 情報収集による分析
- 情報共有による連携

等

脆弱性発見・無断公開 3

- ホテルをハッキングし、管理者情報等を公開したエンジニアに対して、罰金刑@シンガポール
  - ✓中国のテンセント社のエンジニアは、2018年8月末にシンガポールで開催されたHack In The BoxのCTF競技に参加するため、ホテルに滞在
  - ✓ホテルのWi-Fiをチェックしたところ、telnetとFTP接続がオープンになっており、デフォルトのパスワードで利用可能であることを発見したが、**ホテルに脆弱性を報告せずに自身が運営するブログで公開**
  - ✓2018/09/24、このエンジニアに対して、**5,000SGD(約3,600USD)の罰金刑**

元記事：https://www.bleepingcomputer.com/news/security/security-engineer-hacks-hotel-wifi-fined-for-exposing-admin-password/

サイバーセキュリティ研究における注意点 4

- 犯罪や違法行為として…
  - ✓**不正アクセス禁止法違反**
    脆弱性を攻撃する等
  - ✓**不正指令電磁的記録作成等罪**
    適切な管理をせずマルウェアを収集、提供、作成、保管する→目的犯＋供用する
  - ✓**著作権法違反、特許権侵害等**
    HDDのイメージ丸ごとコピー等

サイバーセキュリティ研究における注意点 5

- 犯罪や違法行為として…
  - ✓ 名誉毀損等
    ●●社製ソフトの重大な不具合を公表し、意見、論評による酷評
    →適用除外もあり
  - ✓ 児童ポルノ規制法違反
    画像内容を判断せず自動で画像を収集する→除外規定あり
    等々

学問の自由の限界 6

- 学問研究の方法・手段において、他人の生命・身体等の法益を侵害してはならない

- 「研究の自由と対立する人権もしくは重要な法的利益(プライバシーの権利や生命・健康に対する権利など)を保護するのに不可欠な、必要最小限度の規律を法律によって課すことも、許されるのではないか」
  (憲法第6版/芦部信喜・高橋和之)

研究と倫理 7

- サイバーセキュリティ研究を検討するに当たり、既存の法制度を理解する必要
- 既存の法制度の枠組みでは捉えきれない、あるいは、不明確な部分の研究に関しては**その都度、適用可能性や影響を模索・検討**し、法や倫理に反しないように注意すべき

ハニーポットの研究 8

- 注意すべき法律・犯罪
  - ☑ 不正指令電磁的記録作成等罪
    不正プログラムの保管、共犯
    ビーコン等のファイルの作成・設置
  - ☑ フィッシング罪、詐欺罪の共犯
    アカウント情報の取得、カード情報の取得
  - ☑ 個人情報保護法
    個人情報に該当する通信・データを取得
    →除外規定76条1項(報道、著述、研究)等

C&Cサーバ等への攻撃 9

- 注意すべき法律・犯罪
  - ☑ 不正アクセス禁止法
    - ✓C2サーバに対し脆弱性を突いて攻撃
    - ✓接続されている感染端末の乗っ取り
  - ☑ 偽計・威力業務妨害罪
  - ☑ 電子計算機損壊等業務妨害罪
    - ✓DDoS攻撃
    - ✓虚偽情報の入力

まとめ 10

- サイバーセキュリティ研究は**攻撃を知る必要**があるが、当該攻撃を研究する場合は**犯罪に該当するおそれ**
- 研究に対する**規制も一定程度は必要**
- 倫理規程だけではなく、まずは**既存の法制度**を研究者は知る必要がある