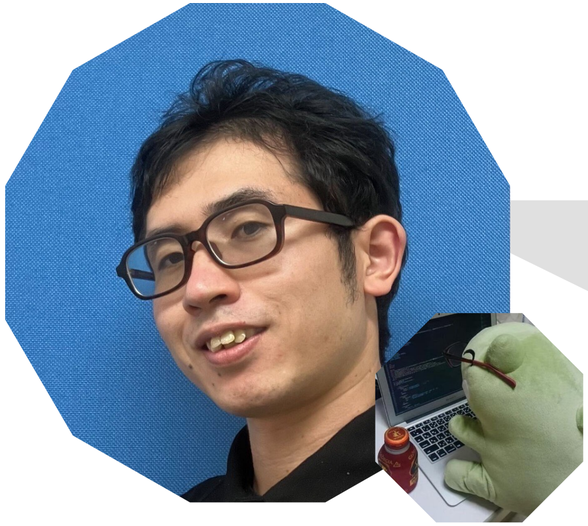
Operation So-seki: You Are a Threat Actor. As Yet You Have No Name.

Jan. 25th , 2024

Ryo Minakawa, Kaichi Sameshima, Atsushi Kanda

NTT Communications / N.F.Laboratories

$whoami



Ryo Minakawa
@N.F.Laboratories

NA4Sec
Network Analytics for Security

Kaichi Sameshima
@NTT Communications

Atsushi Kanda
@NTT Communications

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

ハクティビストは自分たちに関連する
情報発信を監視しています

安易にオープンな場（SNSなど）で
ハクティビストの話題を取り上げないで
ください

本講演とアクターの実名を紐付けた
情報の拡散は厳に慎んでください

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

Overview: Operation So-seki

- **[redacted]と呼ばれるサイバー脅威アクターの活動報告**
  - Telegramを中心に活動する親ロシア派DDoS攻撃煽動者の追跡
  - [redacted]など多角的観点からの分析を実施

- **Key Takeaways:**
  - DDoSインフラの追跡および分析手法
  - 長期的な複数視点でのDDoSアクター考察
  - フロー情報を活用したC2探索の現状
  - ハクティビスト対応についての学び

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

会場限定公開

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

会場限定公開

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

会場限定公開

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

ISPにおけるフロー情報の利用を巡る動向

- 2021年
  『電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第6版）』
  - 平時におけるフロー情報を利用したC2特定が電気通信事業者の正当業務行為として整理された
  - 「C2サーバの特定」までがスコープ

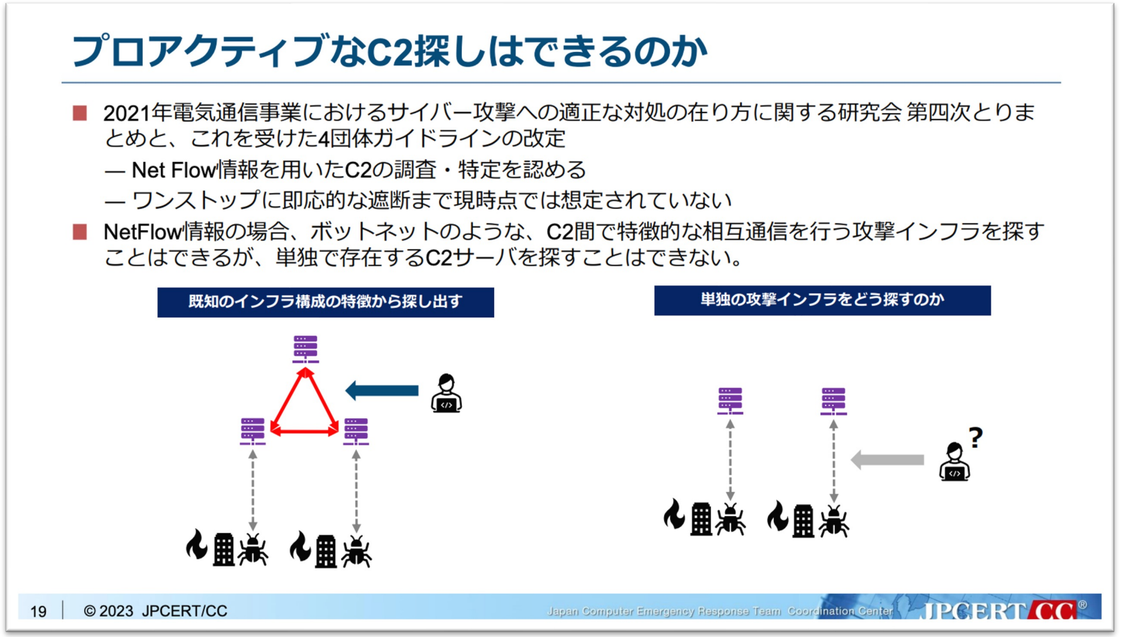
- 2022年 『国家安全保障戦略』
  - いわゆる“アクティブ・サイバー・ディフェンス”の導入に向けた検討事項として、
    通信事業者によるフロー情報の活用を意図した取組が記載された

これらを背景にOperation So-sekiにおいてもC2追跡にフロー情報を活用

会場限定公開

フロー情報の限界

- 網羅性：観測できるのは、**あくまでインターネットトラフィック全体のサブセット**
  - 収集ポイントの制約：
    フロー収集ポイントを通らない通信は全く見えない
  - サンプリングの制約：
    確率的に見えない通信がある
    （通信量の少ない通信は見逃されやすい）
- 情報量：フローの基本単位は5タプル※
  - フロー情報のみでC2通信と**断定することはかなり難しい**



『「アクティブ・サイバー・ディフェンス」事始め
～攻撃者プロファイリングの意義について～』（JSAC2023）より

フローからしか得られない有益な情報はあるが、決して銀の弾丸ではない

様々なコンテキスト情報との複合で蓋然性を高めることが肝要

※ 5タプル＝送信元IP、送信元ポート、宛先IP、宛先ポート、プロトコル

目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

脅威情報の発信・拡散行為が生む負の効果

攻撃技術情報の公表 ▶ TTPs変更

被害情報の拡散 ▶ 攻撃者自身の成功体験強化

さらなるプロパガンダへの利用

会場限定公開

ハクティビスト特有の事情

- 最終目標
  ＝「**自分たちの主張を広く知らしめて世論に影響を与える**」
  - DDoSは関心を集めるための手段
  - 自分たちのメッセージがどれだけ世の中に伝わるかに関心
    - 自分たちの存在/攻撃が認識されているか
    - DDoS被害の話題性

ハクティビストは自分たちの存在・活動をもっと知ってもらいたい

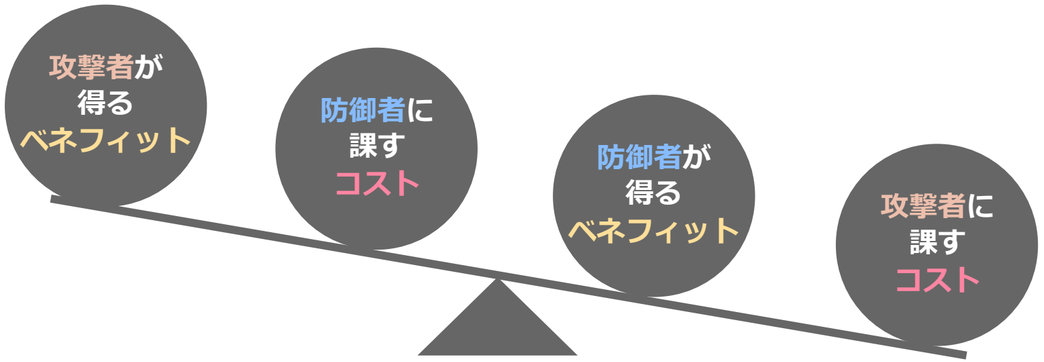
▼

脅威情報を公にする行為と特に相性が悪い

会場限定公開

ハクティビスト対応についての学び

- **脅威アクターの性質に合わせた情報共有**
  - **攻撃者/防御者双方のコストとベネフィット**
    - 公の場での情報共有はハクティビストと特に相性が悪い
  - 脅威インテリジェンスの4Aに立ち返る
    - Accurate（正確であること）
    - Audience Focused（消費者視点であること）
    - Actionable（意思決定・アクションにつながること）
    - Adequate Timing（適切なタイミングであること）
  - 情報の二次的共有にも注意を払う
    - 安易な情報拡散は攻撃者を利する行為



目次

- Operation So-seki
- 脅威アクターのプロファイル
- DDoS基盤と攻撃能力の変遷・分析
- DDoS活動の変遷・分析
- フロー情報を活用した攻撃基盤探索
- ハクティビストと脅威情報共有
- まとめ

まとめ

- 親ロシア派ハクティビスト[redacted]の長期追跡
- **Key Takeaways:**
  - DDoSインフラの追跡および分析手法
    - [redacted]
  - 長期的な複数視点でのDDoSアクター考察
    - [redacted]
  - フロー情報を活用したC2探索の現状
    - フロー情報の価値と限界
  - ハクティビスト対応についての学び
    - 脅威アクターの性質に合わせた情報共有

NA4Sec
Network Analytics for Security

Thank you !

docomo business | NTT Communications NFLabs.

Your comments & feedbacks are always welcome