Shadowserverの紹介

超セキュリティDAY @ Internet Week 2024

Korry Luke
WIDE Project
koluke@wide.ad.jp

自己紹介

コリー・ルーク (Korry Luke)

WIDEプロジェクトの運営協議委員

慶應義塾大学　政策・メディア博士課程　在学中

WIDEや研究室内の一部セキュリティ運用や監視を担当している

Shadowserverって何？

- 2004年に設立されたアメリカの非営利団体
- インターネット・セキュリティ全般のために幅広くセキュリティ
- 比較的にすぐに役にたつ形式でデータ提供活動を行っている
- 国際的に知られ、多数国のCERTや警察との連携がある
- shodan等のようなインターネット全般のスキャンを毎日で行っている
- ASN、ドメイン管理者向けの無料の情報提供サービスを行い、処理してレポートを毎日に各登録された組織に送る
- 簡易なattack surface management（攻撃対象領域管理）として使用が可能

どんなデータ？

- IPv4全般のスキャン
- ハニポーポット（Shadowserver及び協力先）
- シンクホール（過去にマルウェア等で使用されたドメイン）
- 臨時で外部機関から共有あったもの（セキュリティ研究機関、CERT系、政府機関等からのデータ共有）

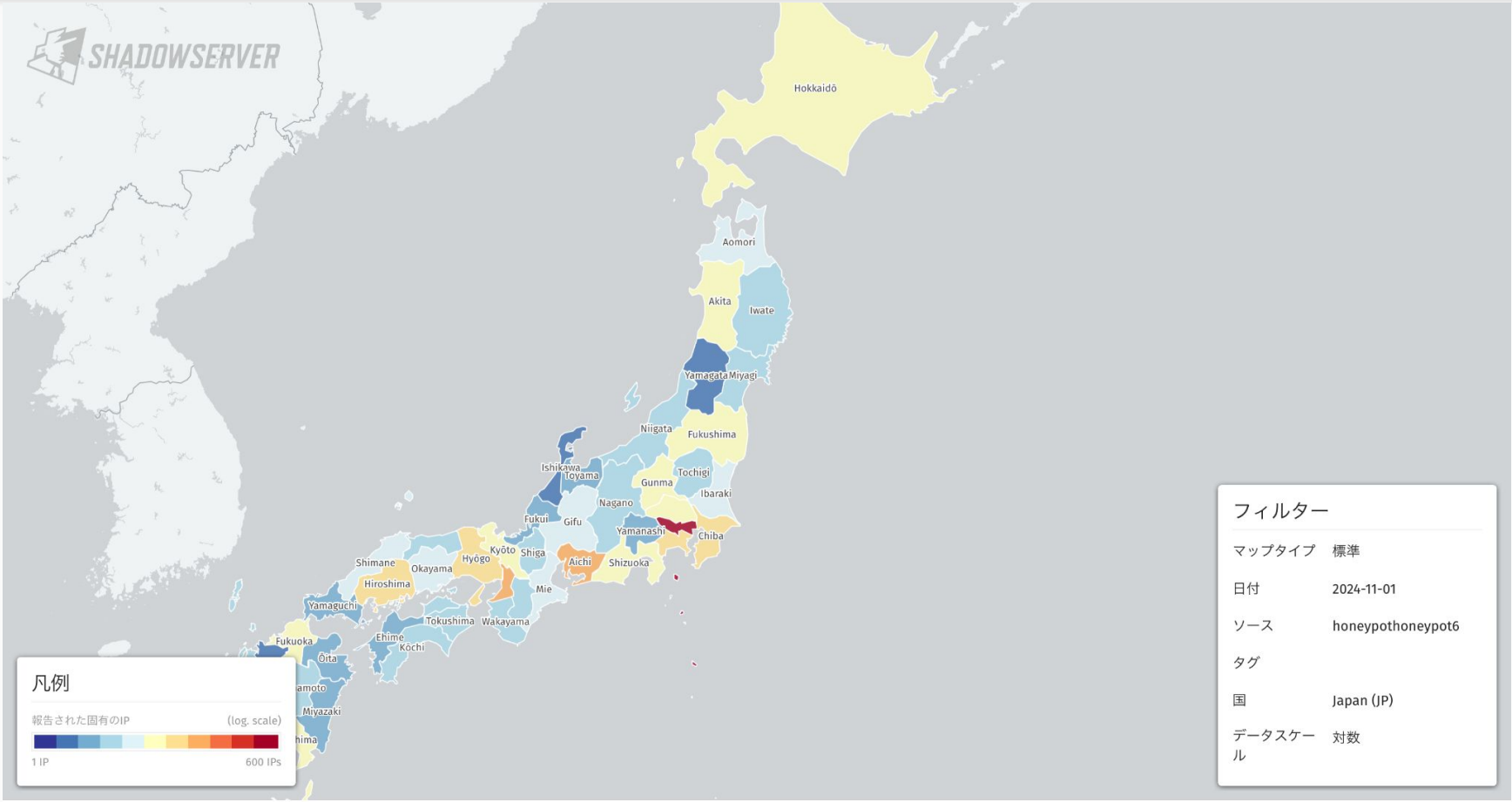
比較的にすぐ役に立つケースも

- 組織内のIPアドレスから、SSHやSMTPブルートフォースの送信を先方のハニーポットに検知された
- 組織内のIPアドレスから、マルウェアで使われたC2ドメイン宛に通信があった
- 先日に公開されたばかりの任意コード実行のCVEに該当する可能性が高そうなホストが組織内にある
- などなど（現時点で131種類のレポートある）
  https://www.shadowserver.org/what-we-do/network-reporting/

誰向け？

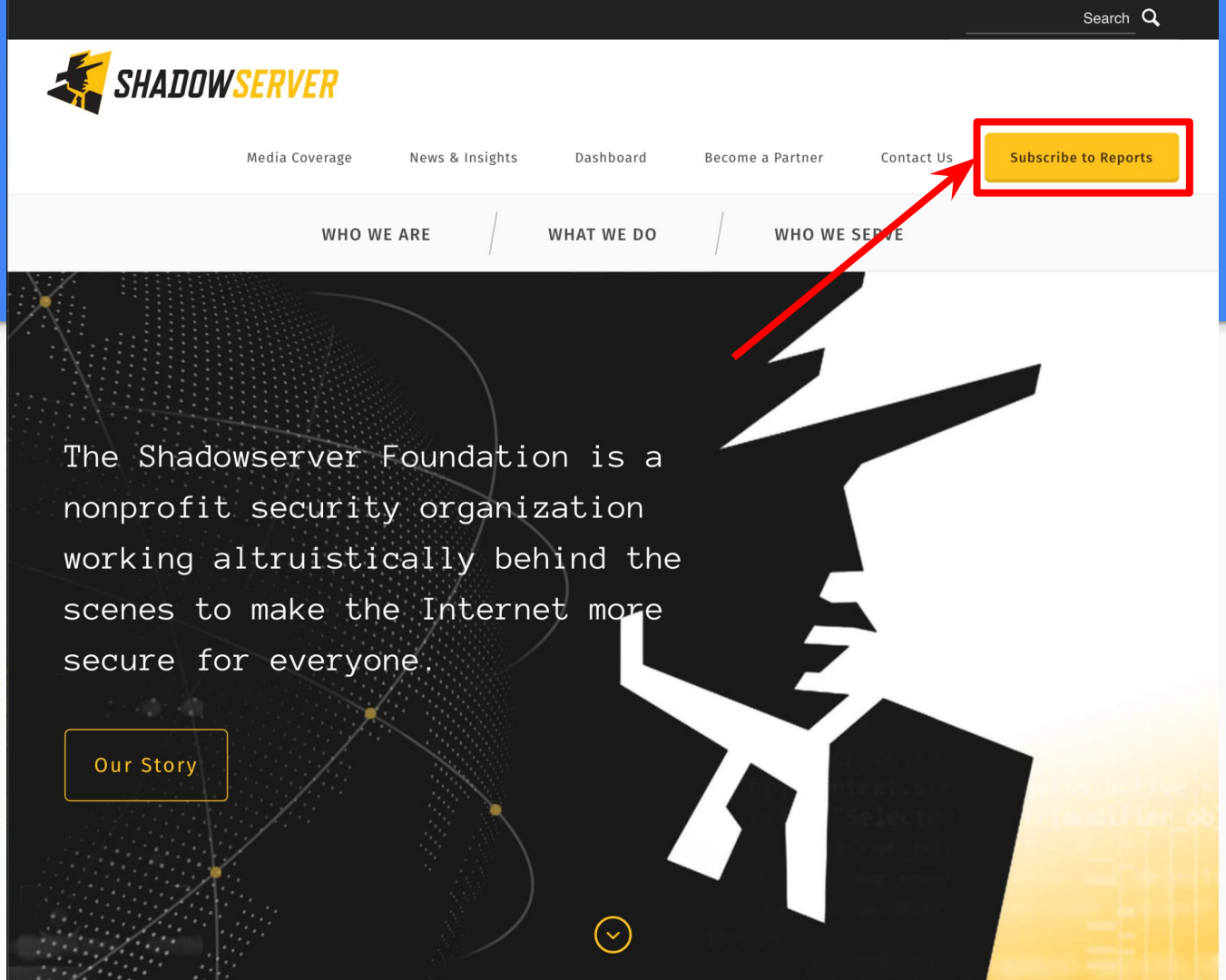
- ASNやドメインの正規管理者
- メール、APIで受け取れる
- 外から自分の組織がどう見えるか？と迷ったことある方
- Splunk, Elasticsearchのインテグレーションある
- ダッシュボードでインタラクティブで地域ごとの統計が見える

例：日本と思われるIPから、ハニーポットへの接続



どうやって使えるようにする？

- セキュリティ関連の情報のため、組織レベルで登録が必要
- 費用はかからない
  - 寄付、スポンサーなどでファンドされている
- まず登録してみましょう


Search
SHADOWSERVER
Media Coverage
News & Insights
Dashboard
Become a Partner
Contact Us
Subscribe to Reports
WHO WE ARE
WHAT WE DO
WHO WE SERVE
The Shadowserver Foundation is a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyone.
Our Story

申請に必要な情報

- 申請する方の氏名、メールアドレス、職位、電話番号
- 組織の名前
- PGP鍵（任意）
- 対象のネットワークリソース（AS番号、ドメイン、CIDR等）
- レポートの送付先（メールアドレス）
  - 専用のメーリングリストやaliasの作成がおすすめ
  - メールでレポートを受け取る場合、レポート別で1日1回にくるため、複数レポートが対象となる場合、その分のレポートが送信される
- レファレンスできる連絡先
  - Whoisに登録されている情報が一致していることが推奨
  - 連絡が行く場合があり、企業内の調整等が大変かもしれない

URL編

公式ホームページ
https://www.shadowserver.org

ダッシュボード
https://dashboard.shadowserver.org/ja/

Github (API使用時のスクリプト、スキーマなど)
https://github.com/The-Shadowserver-Foundation

APNICブログ(英語) https://blog.apnic.net/2021/06/10/securing-your-network-using-shadowserver-reports/