4,410

# Senda-Nexus統合観測レポート

- 目的：Senda-Nexus環境におけるSYNトラフィック、高速スキャナ型トラフィック、Mirai関連トラフィック、およびBlackIPトラフィックを収集・分析し、展示会用の統合レポートを作成する。
- データソース：Senda-Nexus MCP
- 注：本最終レポートは、各ステージのレポートを統合し、ステージ間の総合分析を追加したものである。

## 1. 概要

Senda-Nexus環境におけるSYNトラフィック、高速スキャナ型トラフィック、Mirai関連トラフィック、およびBlackIPトラフィックの分析結果は、著しい変動性と潜在的なセキュリティリスクを示している。主な調査結果として、SYNトラフィックの急増、高速スキャナおよびMiraiボットネットにおける中国と米国からの顕著な活動、そして4月12日に検出された悪意のあるIPアドレスの著しい増加が挙げられる。これらの結果は、進行中または新たに開始された脅威キャンペーンがSenda-Nexusのインフラストラクチャを標的としている可能性を示唆している。直ちにネットワークセキュリティ対策を強化し、異常なアクティビティを綿密に監視する必要があります。

## 2. ステージハイライト

### 2.1 SYN

SYNトラフィック量は過去1か月間で著しい変動を示し、3月25日には約1億4100万パケットでピークに達しました。この期間、米国はSYNトラフィックの主要な発信源の一つであり、4月11日には1257万パケット以上が報告されています。

### 2.2 高速スキャナー型観測（SEQ）

Senda-Nexus環境における高速スキャナー型観測では、特に中国と米国からの活発な活動が確認されています。データは変動パターンを示しており、3月25日と3月27日にピーク値を示しています。

### 2.3 Mirai関連の観測

Miraiボットネットは、特に中国と米国からの活発な活動を継続しています。 Microsoft、GTT Communications Inc.、Comcastといった大手インターネットサービスプロバイダに関連付けられたIPアドレスを標的とした注目すべき攻撃が確認されています。最新のデータによると、Mirai関連の活動は多発しており、4月11日には中国から13,000件以上、米国から9,000件近くの観測がピークに達しました。

### 2.4 BlackIPによる観測

BlackIPによる観測では、悪意のあるIPアドレスとして識別されたIPアドレスの数が大幅に増加しており、4月12日に顕著な急増が見られました。4月11日から12日の間に、検出された悪意のあるIPアドレスの数は190件から424件に増加し、123.7%の増加となりました。

## 3. 段階間の相関関係

### 重複と強化シグナル

すべての段階において、活動が活発な地域には明確な重複が見られます。中国と米国は、SYNトラフィック、高速スキャナー型活動、そしてMirai関連攻撃の主要な発生源として際立っています。これは、これらの地域が厳重に監視すべき重要なエリアであることを改めて示しています。

### 対照と監視の優先順位

重複はあるものの、注目すべき対照も存在します。

- SYNトラフィックの大量発生は、高速スキャナー活動や特定のMirai関連活動とは相関していません。
- 米国はSYNトラフィックの重要な発生源ではありますが、他の段階における役割はそれほど顕著ではありません。一方、中国は高速スキャナーとMirai関連攻撃の両方において、より一貫した存在感を示しています。

### 監視の優先事項

- **米国など特定の国からのSYNトラフィックを監視する。**
- **Mirai攻撃に関連するネットワークアクティビティの異常なパターンを綿密に監視する。**
- **主要なインターネットサービスプロバイダに関連付けられたIPアドレスの監視を強化する。**

## 4. 統合された推奨アクション

1. **潜在的なDDoSリスクを軽減するために、**レート制限と異常検知メカニズムを実装する。**
2. **GOOGLE-CLOUD-PLATFORMやM247 Europe SRLなど、トラフィック量の多いASNに関連付けられたASNについて、より詳細な分析を実施する。**
3. **悪意のあるIPアドレスとしてフラグ付けされたIPアドレスを特に対象として、ネットワーク監視とアラートのしきい値を引き上げる。**

## 5. 最終結論

Senda-Nexus環境におけるSYN、高速スキャナ型、Mirai関連、およびBlackIPの観測結果を統合したレポートは、重大なセキュリティリスクを浮き彫りにしています。現在進行中または新たに開始された脅威キャンペーンが、特に中国と米国における活動の活発化を通じて、Senda-Nexusのインフラストラクチャを積極的に標的にしています。これらのリスクを軽減するために、ネットワークセキュリティ対策の強化と、異常な活動の綿密な監視に直ちに注力する必要があります。