報道資料

令和８年４月２３日
国家サイバー統括室

侵害されたデバイスで構成される中国関連の匿名ネットワークに対する防御に関するアドバイザリーへの共同署名について

令和８年４月２３日、国家サイバー統括室は、英国が作成した国際アドバイザリー“Defending against China-linked covert networks of compromised devices”（以下「本件アドバイザリー」という。）の共同署名に加わり、本件アドバイザリーを公表しました。仮訳は追って公表予定です。

本件アドバイザリーに共同署名し協力機関として組織名を列記した国は、英国の他、豪州、カナダ、ドイツ、オランダ、ニュージーランド、スペイン、スウェーデン、米国及び日本の10か国です。

本件アドバイザリーは、匿名ネットワークを使用したサイバー攻撃を技術的に説明した上で、攻撃の検知手法や緩和策を示すものであり、我が国のサイバー安全保障強化に資する文書であることから共同署名に加わることとしました。

今後も、サイバー安全保障分野での国際連携の強化に努めてまいります。

１．本件アドバイザリーの概要

(1) 概要・背景
- 過去数年間で中国関連のサイバーアクターは、戦術、技術、手順（TTPs）を変更している。それまで個別に調達していたインフラの利用から、外部から提供される大規模な侵害デバイスのネットワーク（ボットネット）へ転換した。Volt Typhoon、Flax Typhoonがこうしたネットワークを利用。
- ネットワークは主に侵害されたSOHOルーター、IoTデバイス（ウェブカメラ、ビデオレコーダー、NAS等）、スマートデバイスで構成されている。中国関連の大半のアクターが匿名ネットワークを戦略的に大規模に利用。複数グループが単一のネットワークを利用している可能性がある。
- 匿名ネットワークは継続的に開発されている。また、防御側の対抗措置やアップデート等により、常に変化している。

(2) 匿名ネットワークの特徴
- 低コスト・低リスクで匿名性が高い通信経路を提供。
- マルウェア配信からデータ流出まで、サイバー攻撃のあらゆる段階で利用。
- 正当なユーザーも使用し、帰属特定が困難。
- 中国の情報セキュリティ企業が創設・管理。多層ボットネット「Raptor Train」は世界中の 20 万台以上の感染デバイスで構成され、Integrity Technology Groupにより運用されている。

(3) 防御策
- すべての組織向け

- エッジデバイスの把握
- リモート接続への二要素認証導入　　等

・ 大規模／高リスク組織向け
- IP 許可リスト、ゼロトラストポリシーの適用
- 地理的・OS・タイムゾーンによる接続制御
- 機械学習による異常検知　　等

・ 最高リスク組織向け
- アクティブハンティングで侵害デバイス IP を検出・監視
- バナー等を活用した報告済みの匿名ネットワークの追跡・マッピング
- 動的ブロックリストや脅威検知・警告ルールの作成
- ネットフロー解析による動的ネットワークマッピング　　等

２．関連リンク

【原文リンク】