報道資料

令和７年８月 27 日
国家サイバー統括室
警察庁

「ソルトタイフーン（Salt Typhoon)」に関する国際アドバイザリーへの共同署名について

令和７年８月 27 日、国家サイバー統括室及び警察庁は、米国が作成した国際アドバイザリー“Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System”（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、米国の他、豪州、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、スペイン及び日本の 13 か国です。

本件アドバイザリーは、一般的に「ソルトタイフーン（Salt Typhoon)」と呼称されるサイバー攻撃グループの攻撃手法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

・ 中国政府が支援する「APT 攻撃者」（※）は、少なくとも電気通信、政府、交通、宿泊、軍事インフラを含む、世界中のネットワークを標的としている。このサイバー脅威活動の一群は、米国、豪州、カナダ、ニュージーランド、英国等で観測されている。

（※）本件アドバイザリーでは、サイバーセキュリティ業界において、Salt Typhoon、OPERATOR PANDA、RedMike 等と呼ばれる攻撃者との重複を指摘しつつ、より一般的に「APT 攻撃者」と呼称。

・ これらの「APT 攻撃者」による悪意ある活動は、中国の具体的な複数企業と関連付けられる。これら企業は、中国人民解放軍（PLA）及び中国国家安全部（MSS）にサイバー関連の製品・サービスを提供している。活動を通じて取得されたデータは、最終的に、中国の諜報機関が、対象者の通信や移動を世界中で追跡するために分析することを可能としている。
・ 本件アドバイザリーの共同署名機関は、ネットワークの守り手に対し、悪意のあるサイバー活動の脅威をハンティングし、本件アドバイザリー中の緩和策を適用することを強く求める。

(2) 技術詳細

・ 初期アクセス（Initial Access）：「APT 攻撃者」は、特別のツールやマルウェア、ゼロデイ脆弱性を使用する必要が殆どなく、公開された脆弱性等（本件アドバイザリーでは悪用された脆弱性を例示）を利用して大

きな成功を収めている。「APT 攻撃者」は、仮想専用サーバ（VPS）や中間ルーターといったインフラを利用している。
- 永続化（Persistence）：「APT 攻撃者」は、対象ネットワークへの永続的なアクセスを維持するため、システムログ内の攻撃者の送信元 IP アドレスを隠蔽する手法を使用。（例：アクセス制御リスト（ACL）の変更による IP アドレスの追加、リモートアクセスの経路を提供する標準ポート／非標準ポートの開放等）
- 横展開・収集（Lateral Movement & Collection）：「APT 攻撃者」は、初期アクセス後、ネットワークデバイス間の横移動を容易にするため、認証に関するプロトコルやインフラを標的にして、パケットキャプチャを収集。特に、侵害されたルーター上で内部資格情報のトラフィックを収集（個別製品における侵害を例示）。
- データ窃取（Exfiltration）：ピアリング接続を悪用することでデータ窃取を行っていることが主な懸念。データ窃取を隠蔽するため、複数別々のコマンドアンドコントロール（C2）チャネルを利用。

(3) ケーススタディ
- 「APT 攻撃者」が初期アクセスで使用した手法と、分析によって得られた、その活動を検出するための指標を詳述。

(4) 脅威ハンティングガイダンス
- 重要インフラ組織（特に電気通信）は脅威ハンティングの実施が推奨される。悪意ある活動が疑われる場合は当局への報告が求められる。
- 脅威ハンティングのために実行が強く推奨される事項を列挙。（例：稼働中のネットワーク機器の設定や全てのルーティングテーブルの確認、ファームウェアのハッシュ検証、ディスク上とメモリ上の両方のイメージのハッシュ値比較等）

(5) 侵害指標（IoC）
- 2021 年８月から 2025 年６月までの間の「APT 攻撃者」の活動と関連付けられる IP 指標等を列挙。

(6) 緩和策
- 「APT 攻撃者」は公開された CVE（Common Vulnerabilities and Exposures）を悪用するため、パッチ適用を優先することが強く推奨される。また、一般的な推奨事項に加え、製品固有の推奨事項が列挙。

２．関連リンク

【原文リンク】