令和６年７月９日
内閣サイバーセキュリティセンター
警察庁

豪州主導の APT40 グループに関する国際アドバイザリーへの共同署名について

１．概要

７月９日、内閣サイバーセキュリティセンター及び警察庁は、豪州通信電子局（ASD）豪州サイバーセキュリティセンター（ACSC）が作成した国際アドバイザリー“APT40 Advisory PRC MSS tradecraft in action”（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、豪州の他、米国、英国、カナダ、ニュージーランド、ドイツ、韓国、日本の８か国です。

これまで、我が国でも、APT40 といわれるサイバー攻撃グループからの攻撃について、我が国企業が対象になっていたこともあると確認しています。

本件アドバイザリーは、APT40 による過去の攻撃事例をケーススタディとして攻撃手法を詳述した上で、攻撃の検知や緩和策を示しており、我が国のサイバーセキュリティ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、サイバーセキュリティ分野での国際連携の強化に努めてまいります。

２．本件アドバイザリーの概要

（１）中国の国家的な支援を受けたサイバーグループと、同グループが与える豪州のネットワークに対する脅威について概説。サイバーアクターは、中国国家安全部（MSS）と関連付けられると理解されている。その活動や手法は、APT40 と呼ばれるグループと重複している。海南省海口市を拠点に活動し、国家安全部海南支部から業務を請け負っているとされている。

（２）APT40 は、豪州政府・民間部門を繰り返し標的にしており、豪州のネットワークに対する脅威は継続している。特筆すべきは、APT40 は、新たな脆弱性の概念実証エクスプロイトを迅速に変換・適応させ、標的ネットワークに対して即座に利用する能力を有している。

（３）APT40 は、インターネットに接続されている脆弱なインフラを悪用することを指向し、有効な認証情報を獲得することを優先する。APT40 は定期的にウェブシェルを利用しつつ、アクセス維持に注力するが、こうした永続化は侵入の初期段階で行われるため、あらゆる侵入で確認される。

（４）APT40 は、豪州に対する攻撃において、これまで侵害されたウェブサイトを C2 サーバとして使用してきたが、攻撃インフラや踏み台として小規模オフィス・家庭用機器（SOHO 機器）を含む侵害された機器を利用するとのグローバルな傾向を採用するようになっている。この手法は、世界中で、中国が国家的に支援する他のアクターも日常的に利用している。

（５）APT40 の攻撃による２件のインシデント（ケーススタディ）：

（ア）ケーススタディ１：攻撃者が 2022 年７月～９月に豪州のある組織のネットワークを侵害し、ウェブシェルを展開。その後、ネットワーク内で横展

開を行い、認証情報を含む機微データにアクセス。

（イ）ケーススタディ２：攻撃者が 2022 年４月から豪州のある組織のネットワークを侵害し、数百に及ぶユーザ名とパスワード、多要素認証コード、遠隔アクセスセッションの技術情報を窃取。

（６）豪州のセキュリティ措置を定めた「エッセンシャルエイト(Essential Eight)」を強く推奨し、検知と緩和のために特に下記の諸点が重要。

（ア）APT40 の攻撃によるインシデントで確認されたファイルは、Windows に登録された全てのユーザアカウントからアクセスでき、データ書き込みが容易になるような場所に蔵置されていることから、疑わしい場所からのプロセス実行を検知するルール設定により、悪意ある振る舞いを検知する。

（イ）緩和策

（i）ログ記録：ウェブサーバのリクエストログや Windows イベントログ、プロキシログの保存を適切に行う。

（ii）パッチ管理：ウェブサーバやリモートアクセスゲートウェイなどインターネットに接続している全ての機器には、セキュリティパッチや緩和策を 48 時間以内に適用し、可能であれば、ソフトウェアや OS は最新バージョンを使用する。

(iii)ネットワークの分離：ネットワークを分離することで、攻撃者の横展開を困難にできる。Active Directory や認証サーバなど重要なサーバは、限定されたサーバからのみアクセスを可能とし、これらのサーバを監視し、ユーザや機器からの接続を限定する。

(iv)その他

- 不要なネットワークサービス・ポート・プロトコルを無効にする。
- ウェブアプリケーションファイアーウォール(WAF)を利用する。
- 管理者権限を必要最小限にする。
- 多要素認証及びマネージドサービスアカウントの使用により、認証情報の解読と再利用を困難にする。
- サポート切れの機器を交換する。

（了）