

令和8年10月9日

国家サイバー統括室

警察庁

中国政府関連のサイバー攻撃グループを支援する企業に関する 国際アドバイザリーへの共同署名について

令和8年10月9日（日本時間）、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“Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools to Steal Sensitive Data”（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。

本件アドバイザリーに共同署名した協力機関として組織名を列記した国は、米国のほか、英国、豪州、カナダ、スペイン、NZ 及び日本の7か国です。

本件アドバイザリーは、中国政府と関連があり中国を拠点とする企業である「永信至誠科技集団（Integrity Technology Group: ITG）」が、他の中国関連サイバー攻撃グループが様々なツールや手法を用いて米国や海外の複数セクターの組織のネットワークを侵害することを可能にしていると指摘し、ITG 及び ITG が提供するツールを利用するサイバー攻撃グループの戦術、技術及び手順（TTPs）並びに侵害の指標（IOCs）について分析結果を提供するとともに、ネットワーク防御者に対し、サイバー攻撃グループが重要なデータを侵害するリスクを低減するための探知・緩和のガイダンスを提供するものです。

今後も、我が国のサイバー安全保障や同盟国・同志国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）背景・サイバー攻撃グループの活動概要

ITG は、中国政府と関連があり同国を拠点として活動する企業であり、悪意あるサイバー活動を支援する個人を雇用し、また、同社が提供するサービスは、世界規模での機密データ窃取を目的とした、より大きな中国のサイバーエコシステムに貢献している。

サイバー攻撃グループは、大規模ボットネット、VPN インフラ、LOTL（Living-Off-The-Land）技術及びコンピューターネットワーク侵害（CNE）ツールのリポジトリという特徴的（unique）な組合せを利用している。

サイバー攻撃グループは、政府関連サービス・施設、重要製造業（Critical Manufacturing）、医療、公衆衛生及び情報通信を含めた複数の米国の重要インフラ分野の被害組織を標的にしたほか、米国の法執行機関、教育機関、宗教団体、そして東南アジア、アフリカ及び北米の組織も標的とした。

(2) 技術詳細

本アドバイザーでは、サイバー攻撃グループが組み合わせて使用するツールとして、オープンソースの各種ポートスキャンツール、各種エクスプロイトコードをベースに作成されたコマンドラインユーティリティ、アプリ「MicroScan」、ツール「Eburst」、VPN ソフトウェアクライアント「SoftEther」、PHP スクリプト「Curlc4.txt」、実行ファイル「DC.exe」、Linux ベースバイナリ「office-cli」等を列挙して解説している。

(本アドバイザーに記載の情報は、ITGに関連する複数件のFBIによる犯罪捜査を通じて収集・観測された技術的証拠に基づく。)

※詳細は、本アドバイザーの5ページ以降参照。

(3) 緩和策

以下を始めとする22項目を列挙し、サイバー攻撃グループの活動に基づき、組織のサイバーセキュリティ態勢の改善を推奨している。

○不使用のサービス（自動設定、リモートアクセス、ファイル共有プロトコル等）やポートを無効化

○XSS (Cross-Site Scripting) ペイロードインジェクションを防ぐため、Web アプリケーションのユーザ入力をサニタイズ

○ICAM ポリシー (Identity, Credential and Access Management Policy) を導入してできる限り全てのサービスに多要素認証を適用

※詳細は、本アドバイザーの14ページ以降参照。

(4) 侵害指標 (IOC)

ITG 及び ITG が提供するツールを利用するサイバー攻撃グループによる活動と関連付けられる2016年1月以降に検知されたドメイン名等を列挙している。

※詳細は、本アドバイザーの19ページ以降参照。

2. 関連リンク

["Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools to Steal Sensitive Data"](#)

(了)