報道関係者各位

DarkGate による攻撃、ベトナムのサイバー犯罪グループが関与
ウィズセキュアがリサーチを発表

～ Ducktail や Duckport などの攻撃と同じ犯罪グループによるものと結論 ～

2023 年 10 月 24 日
ウィズセキュア株式会社

多様なユーザーベースと機能を備えているリモートアクセスのトロイの木馬 (RAT) である DarkGate は少なくとも 2018 年にはサイバー攻撃に使用され始めており、現在は MaaS (Malware-as-a-Service = サービスとしてのマルウェア) として複数のサイバー犯罪グループに供給され、情報窃取、クリプトジャッキング、ランサムウェアの攻撃キャンペーンで観測されています。

先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) のリサーチチームは、これらの攻撃をトラッキングし、ベトナムを拠点に活動するサイバー攻撃グループが DarkGate に関与しているとしたリサーチ結果を発表しました。

ウィズセキュアのリサーチチームはイギリス、アメリカ、インドの企業／団体への DarkGate を使用した複数の攻撃の試みを観測し、DarkGate の調査を開始しました。ルアーファイル、テーマ、ターゲット、配信方法などの非技術的な指標に基づき、同リサーチチームが過去約 1 年半にわたって追跡してきた Ducktail インフォスティーラーツールを使用する同じ攻撃グループによるものと特定することができました。同攻撃グループはまた、Ducktail、Duckport、Lobshot、Redline Stealer といったマルウェアを使用した攻撃にも関与していると考えられます。

ウィズセキュアでシニアスレットインテリジェンスアナリストを務める Stephen Robinson (スティーヴン・ロビンソン) は今回のリサーチについて次のように語っています。
「当社が観測した DarkGate の攻撃は、非常に強力な識別子を持っています。この識別子によって、これらの攻撃と、Ducktail を含む他のインフォスティーラーやマルウェアを使用したさまざまな攻撃との関連を特定することができました。私たちが観測した内容から、Meta Business のアカウントを標的としたいくつかのキャンペーンの背後には、単一の攻撃グループがいる可能性が非常に高いです。」

(Stephen Robinson)

同グループによるさまざまな攻撃キャンペーンで使用されているルアーや悪意のあるファイルには、以下のようなメタデータが含まれています:

- LNK ドライブ ID
- Canva PDF デザインサービス アカウント詳細
- MSI ファイルのメタデータ

Robinson はまた、サイバー犯罪グループが購入可能な攻撃サービスの増加により、防御側としては、攻撃で使用されるツールの種類だけでは誰が攻撃者なのかを特定できない状況が生まれていると話しています。
「DarkGate は長期にわたり存在しており、ベトナムの攻撃グループやクラスターだけでなく、さまざまな目的のために多くのグループによって使用されています。その反面、攻撃者は 1 つのキャンペーンのために複数のツールを使用することがあるため、マルウェアベースの分析からのみでは、活動の真の範囲が特定できない可能性があります。防御側は常にそれを考慮して対策を講じる必要があるのです。」

リサーチの全文 (英語) は以下の WithSecure Labs ブログページにてご覧いただけます:
https://labs.withsecure.com/publications/darkgate-malware-campaign

ウィズセキュア Web サイト:
https://www.withsecure.com/jp-ja/
ウィズセキュアプレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

ウィズセキュアは、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を検出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。
詳細は www.withsecure.com をご覧ください。また、X (旧 Twitter) アカウント @WithSecure_JP でも情報の発信をおこなっています。