報道関係者各位

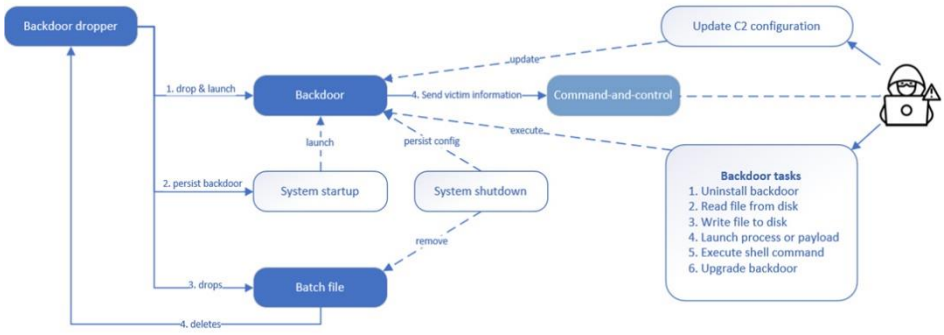
ウィズセキュア、ロシアの国家ハッカーグループ『Sandworm』と関連する新たなマルウェア『Kapeka』を発見

～ 観測時期や使用地域、Sandworm との関連から、ロシア・ウクライナ戦争に関連するものと推定 ～

2024 年 4 月 18 日
ウィズセキュア株式会社

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 (本社: フィンランド・ヘルシンキ、以下、ウィズセキュア) は、同社のリサーチチームが、主に東欧のターゲットに対して使用されたとみられる新しいバックドアマルウェアを発見し、『Kapeka』と名付けたことを発表しました。このマルウェアは少なくとも 2022 年半ばには既に使用されており、ロシア連邦軍総参謀本部 (GRU) が運営する、ウクライナへの破壊的な攻撃で知られる『Sandworm』と呼ばれるサイバー攻撃グループとの関連性があると考えられます。

Kapeka はこれを使用する攻撃者に初期段階のツールキットとして必要なすべてを備え、またターゲットの資産への長期にわたるアクセスを可能にする、柔軟性を持ったバックドアです。マルウェアによる被害状況、稀な目撃情報、そしてステルス性と巧妙さのレベルは、Kapeka が APT (Advanced Persistent Threat = 高度かつ持続的な脅威) レベルの活動であることを示しています。Kapeka の開発と展開は 2022 年のロシア・ウクライナ戦争の勃発を受けておこなわれており、ウクライナへの侵攻以来、中欧および東欧全域のターゲットに対する標的型攻撃に使用されている可能性が高いと言えます。



Kapeka の概要

ウィズセキュアのリサーチ部門である WithSecure Intelligence (WithIntel) で今回のリサーチのリーダーを務めた Mohammad Kazem Hassan Nejad (モハマッド・カゼム・ハッサン・ネジャッド) は Kapeka の観測について次のように述べています。
「Kapeka バックドアはロシアの APT 活動、特に Sandworm グループとの関連性によって、人々に大きな懸念をもたらしています。観測頻度の低さとターゲットを絞った標的型であるという特徴が主に東欧で観察されており、限定された範囲の攻撃に使用されるカスタムツールであることを示唆しています。さらなる分析により、Sandworm に関連するもう 1 つのツールキットである GreyEnergy との共通点が明らかになりました。これはヨーロッパにおいて標的とされる企業／団体にとっては大きな潜在的脅威となります。」

WithSecure が最後に Kapeka の活動を観測したのは 2023 年 5 月でした。攻撃グループ、特に国家ハッカーグループが活動を停止したり、ツールを完全に廃棄したりすることは非常に稀です。したがって、Kapeka の観測例が少ないことは、ロシア・ウクライナ戦争など、数年にわたる作戦において APT が Kapeka を綿密に利用していることの証拠と考えることができます。

Kapeka リサーチに関する完全なレポート (日本語) は以下にてご覧いただけます:
https://www.withsecure.com/content/dam/with-secure/ja/news-library/202404_WithSecure_Kapeka_Report_JP.pdf

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、多くのヨーロッパ企業に選ばれるサイバーセキュリティパートナーです。世界中の IT サービスプロバイダー、MSSP、ユーザー企業から、中堅・中小企業を保護するアウトカム(成果)ベースのサイバーセキュリティソリューションにおいて大きな信頼を勝ち取っています。ウィズセキュアはヨーロッパにおけるデータ保護の規制に準拠し、プライバシー、データ主権、コンプライアンスに注力しています。
当社は 35 年以上の経験を持ち、ユーザー企業の消極的／保守的なサイバーセキュリティ対策から積極的／先進的なアプローチへのパラダイムシフトのサポートのためのポートフォリオを持っています。ウィズセキュアはパートナーとの協力的な成長へのコミットメントに基づく柔軟な商業モデルを提供し、ダイナミックなサイバーセキュリティの世界において両者の成功を保証します。
ウィズセキュアの最先端のポートフォリオの中心となるのは、AI を搭載したテクノロジー、人の専門知識、コ・セキュリティ (共同セキュリティ) サービスをシームレスに統合する Elements Cloud です。さらに、エンドポイントおよびクラウドの保護、脅威の検出と対応、エクスポージャー管理にまたがるモジュール式の機能により、中堅・中小企業ユーザーのセキュリティ対策を強固なものとします。
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 https://twitter.com/WithSecure_JP でも情報の発信をおこなっています。