報道関係者各位

ウィズセキュア、ベトナムを拠点とする
新たなサイバー脅威に関する調査レポートを公開

～ Meta Business や Facebook アカウントの広告エコシステムをターゲットとした攻撃が増加 ～

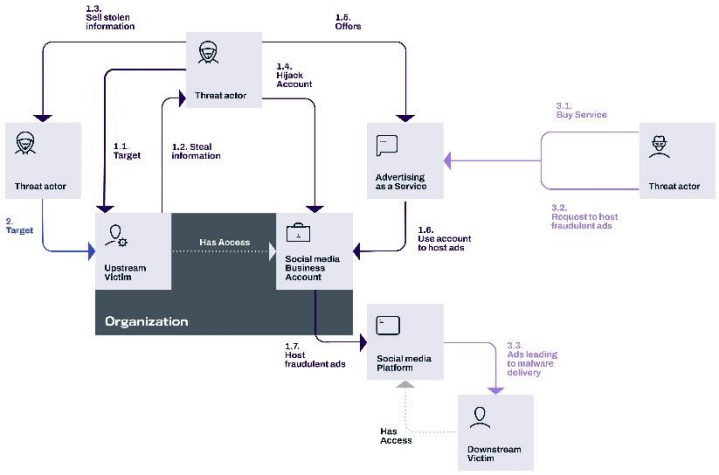
2023 年 9 月 6 日
ウィズセキュア株式会社

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 (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) は、『DUCKPORT』と名付けられた、ベトナムを拠点とする新たなサイバー脅威に関する調査レポートを公開し、Meta Business や Facebook アカウントなどの広告エコシステムをターゲットとした攻撃が増加していると注意を喚起しています。

ウィズセキュアのリサーチ部門である WithSecure Intelligence (略称: WithIntel) によるレポートによると、これらのプラットフォームを標的とする複数のグループを観測し、現在追跡しています。これの攻撃は、ターゲットとするアカウントにアクセスできるユーザーを操作して、インフォスティーラー (情報を搾取するマルウェア) に感染させるものです。

攻撃者は、電子メールやソーシャルメディアなどを通じて共有されるルアーを使用し、ターゲットがマルウェアをダウンロードするように仕向けます。WithIntel のリサーチャーがこれらの攻撃において観測したルアーに共通するテーマは、トレンドトピック (ChatGPT など)、ユーザー数の多いソフトウェア (Notepad++など)、採用関連 (求人広告など)、広告プラットフォームに関する情報 (Ads Manager ツールなど) などでした。

感染後、マルウェアは Facebook のセッション Cookie やログイン認証情報など様々な情報を盗み出し、攻撃者によるターゲットアカウントへのアクセスを可能にします。また、マルウェアの中にはアカウントを乗っ取り、ターゲットのマシンを経由して自動的に不正な広告を実行するものもあります。攻撃者はこれらのアカウントにアクセスすることで、恐喝、中傷、そしてターゲット企業の資金や信用を利用した詐欺広告の掲載など、金銭目的の機会を広く創出しようとしています。



(図 1: 広告プラットフォームへの攻撃のフロー)

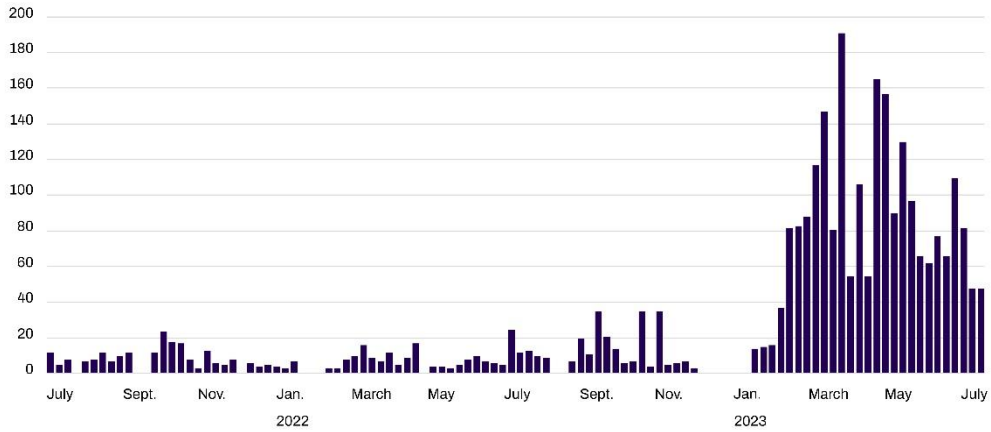
レポートを執筆した WithIntel のリサーチャーである Mohammad Kazem Hassan Nejad (モハマッド・カゼム・ハッサン・ネジャッド) は、こうした攻撃について次のように語っています。
「これらの攻撃グループは、しばしば他のサイバー犯罪者に広告を販売し手数料を取ったり、攻撃を分担させたりしています。そのため、他のサイバー犯罪者にとっての一種のイネイブラー (enabler) になり、最終的には企業やそのプラットフォーム、そしてユーザーに被害をもたらすこととなります。さらに、彼らは盗み出すことに成功した情報の多くを外部に販売することでより多くの収入を得て、そしてその結果、被害者にとってさらに多くの問題を引き起こすことになるのです。」

レポートでは、攻撃の概要を説明するとともに、攻撃に関与していると考えられる 2 つのサイバー脅威についての分析を提供しています。

1. DUCKTAIL
WithIntel が過去約 1 年半にわたって追跡してきた脅威です。リサーチャーたちは、過去 6 ヶ月間に DUCKTAIL の活動が大幅に急増したこと、またその活動において、X (旧 Twitter) の広告アカウントをターゲットにしたもの、検知を回避するための回避／反解析テクニックの利用の拡大など、複数の重要な進化が観察されました。

参考ページ:
ウィズセキュア、Facebook ビジネスアカウントから情報を盗むインフォスティーラー型マルウェア『DUCKTAIL』を発見 (2022 年 7 月 26 日)
https://www.withsecure.com/jp-ja/whats-new/pressroom/20220726-ducktail
インフォスティーラー『DUCKTAIL』による被害が拡大、1 件あたり数十万米ドルの被害に (2022 年 11 月 24 日)
https://www.withsecure.com/jp-ja/whats-new/pressroom/20221124-ducktail

2. DUCKPORT
WithIntel が本年 3 月に発見した脅威です。DUCKTAIL と DUCKPORT の間にはかなりの共通点が見受けられますが、別個のサイバー犯罪グループであると判断するに値する大きな相違点もまた存在します。DUCKPORT 特有の機能の代表的なものとしては、スクリーンショットを撮影する機能や、C&C (コマンドアンドコントロール) チェーンの一部としてオンラインノート共有サービスを悪用する機能などが挙げられます。



(図 2: DUCKTAIL による攻撃数の推移)

リサーチに参加したウィズセキュアの Neeraj Singh (ニーラジ・シン) は、類似する複数の攻撃グループが関与していることは、この分野で活動する攻撃グループ間での一定レベルの関与があることを示していると話しています。
「これらの様々な攻撃グループは、共通の人材プールから専門的なナレッジを集めていたり、より効果的な攻撃戦略のためのツールやインサイトの共有のために、情報共有のグループを組んで活動している可能性があります。さら

に、RaaS (Ransomware-as-a-Service = サービスとしてのランサムウェア) のような専門サービスを提供する仲介業者が関与する可能性も無視できません。しかし、この種の攻撃が増加していることは明らかであり、また、これらの攻撃グループが一定の成功を収めていることも否めません。」

レポートの全文は以下のページでご覧いただけます:
(英語) https://labs.withsecure.com/publications/meet-the-ducks
(日本語) https://www.withsecure.com/content/dam/with-secure/ja/news-library/202308_WithSecure_Meet-the-ducks_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、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、Twitter @WithSecure_JP でも情報の発信をおこなっています。