報道関係者各位

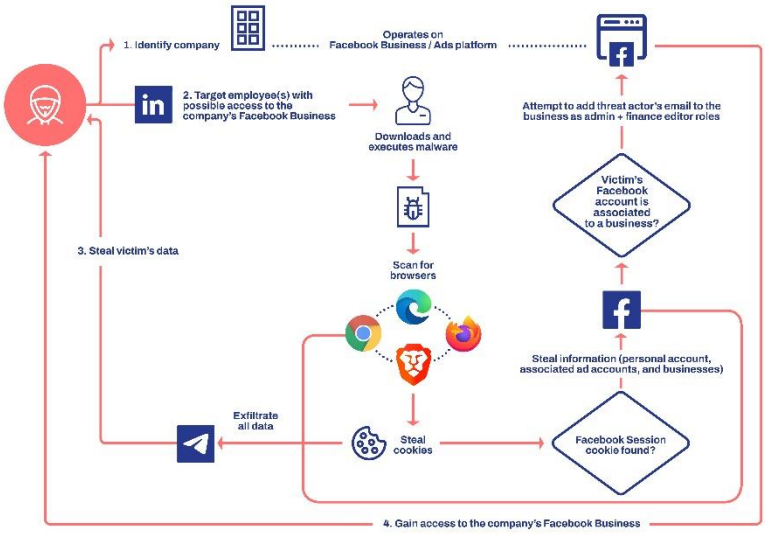
ウィズセキュア、Facebook ビジネスアカウントから情報を盗むインフォスティーラー型マルウェア『DUCKTAIL』を発見

～ マーケティング担当者や人事担当者をターゲットに、LinkedIn でのスピアフィッシング経由で Facebook のビジネスアカウントを乗っ取り ～

2022 年 7 月 26 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、Facebook の広告およびビジネスアカウントを利用する個人／企業を攻撃対象として進行中の、『DUCKTAIL』と命名されたサイバー攻撃オペレーションを発見したと発表しました。ウィズセキュアでは収集データと分析に基づき、このオペレーションがベトナムのサイバー攻撃者によって行われていると強く確信しています。また、一連の証拠から、攻撃者の動機は金銭的なものであることが濃厚です。

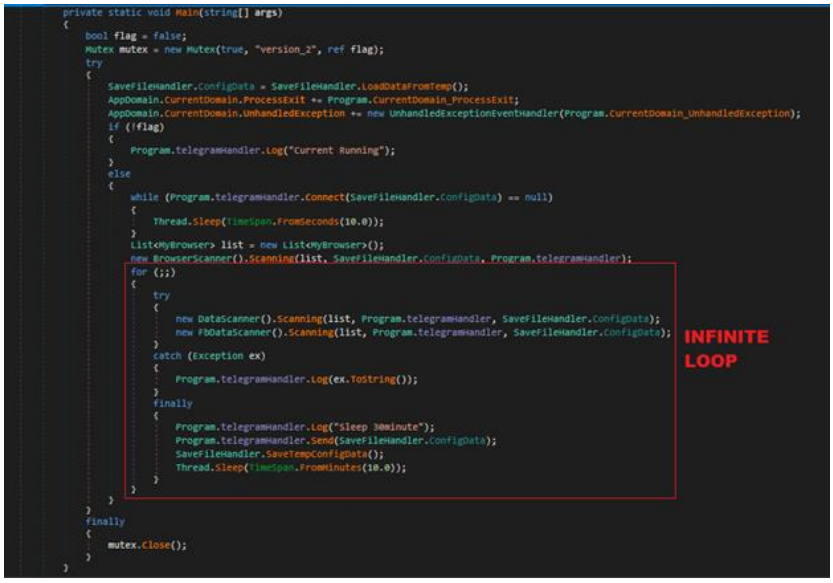
DUCKTAIL は、Facebook ビジネスアカウントを乗っ取るために特別に設計された機能を含むインフォスティーラー型マルウェアコンポーネントを利用しています。このような機能はウィズセキュアが知る限り初めてであり、DUCKTAIL はこれまでの Facebook を主なターゲットとしたマルウェアとは一線を画しています。このマルウェアはブラウザのクッキーを盗み、認証された Facebook のセッションを利用して、被害者の Facebook アカウントから情報を盗み、最終的には被害者がアクセスできるあらゆる Facebook ビジネスアカウントを乗っ取るよう設計されています。DUCKTAIL はまず LinkedIn 内において、Facebook ビジネスアカウントに高位のアクセス権 (特に管理者権限) を持つユーザーを探し、フィッシングを行います。



(DUCKTAIL の攻撃ルート／手法)

ウィズセキュアのリサーチ部門である WithSecure Intelligence (略称: 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、DUCKTAIL の手法に関して次のように語っています。
「DUCKTAIL を使用するサイバー攻撃者は、攻撃の成功率を高めるために少数のターゲットを慎重に選択し、気付かれにくくしようとしているようです。当社では、企業で管理職／デジタルマーケティング／デジタルメディア／人事などの役割を担う人々がターゲットになっていることを確認しています。」

発見当初、DUCKTAIL は未知のマルウェアとされましたが、ウィズセキュアが DUCKTAIL の動向の追跡と分析を行ったところ、攻撃者が 2021 年後半から DUCKTAIL と連携したマルウェアの開発／配布を行っていることが判明しました。DUCKTAIL のオペレーションは、その後もマルウェアの更新と配布を続け、実装された他の機能とともに、既存のまたは新しい Facebook のセキュリティ機能をバイパスする能力を向上させようとしています。



(DUCKTAIL の実行ロジック)

ウィズセキュアでは自社の EPP (エンドポイント保護プラットフォーム) や EDR (エンドポイントでの検知と対応) ソリューションにおいて、静的および振る舞い検知シグネチャ、攻撃ライフサイクルの複数のステージに対する検知機能を備えていますが、Mohammad Kazem Hassan Nejad はユーザーが被害者にならないためには強い警戒心を持つことが重要であると述べています。
「多くのスピアフィッシングキャンペーンは LinkedIn のユーザーをターゲットとしています。企業のソーシャルメディアアカウントに管理者としてアクセスできる立場にあるならば、ソーシャルメディアプラットフォームで他者と交流する際、特に見知らぬユーザーから添付ファイルやリンクが送られてきた場合には、細心の注意を払って対応することが重要です。」

ソーシャルネットワークやメディアプラットフォームの利用は、引き続き上昇傾向にあります。そうした人気に乗じて、サイバー犯罪者はマルウェアの配布／窃盗／情報操作／詐欺など、これらのプラットフォームを悪用して利益を得る方法を探しています。Facebook のような SNS を標的としたマルウェアは、SNS のプラットフォームが実装しているセキュリティメカニズムにより、これまではあまり見られないケースでした。しかし、Facebook は、その広範な活動範囲とユーザベースから、攻撃者にとっては格好の攻撃ベクトルとなっています。


(Mohammad Kazem Hassan Nejad)

ウィズセキュアは DUCKTAIL の調査レポートの公開前に、その内容を Facebook の運営会社である Meta 社と共有しています。DUCKTAIL に関するレポート (MITRE のフレームワークを用いた攻撃の概要を含む) は、以下のページよりご覧いただけます。
https://www.withsecure.com/content/dam/with-secure/ja/resources/20220726_WithSecure_Ducktail_Report_JP.pdf

WithSecure Web サイト:
https://www.withsecure.com/jp-ja/
WithSecure プレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

WithSecure™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探し出し、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 WithSecure 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 でも情報の配信をおこなっています。