報道関係者各位

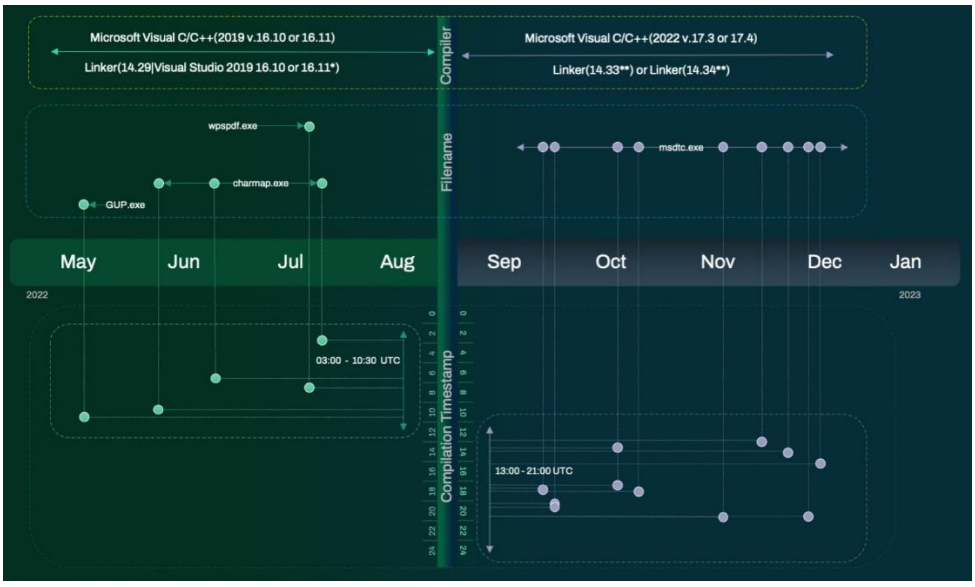
ロシアのランサムウェア犯罪グループ、中国製サイバー攻撃ツール『SILKLOADER』を入手／使用

～ ウィズセキュアのリサーチチーム、両国の脅威アクター間での『SILKLOADER』の共有を観測 ～

2023 年 3 月 16 日
ウィズセキュア株式会社

サイバー犯罪の世界においては、脅威アクター同士が持っている技術を互いに共有することがあり、それにより攻撃の件数が増加し、その精度が高くなってきています。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) は同社が観測した中国のサイバー犯罪者からロシアのランサムウェアギャングへのサイバー攻撃ツール『SILKLOADER』の提供に関するレポートを発行し、サイバー犯罪集団間でのツール共有のダイナミズムについて説明しています。

ウィズセキュアのリサーチ部門である WithSecure Intelligence (通称: WithIntel) のリサーチャーたちが SILKLOADER を初めて観測したのは、フランスの社会福祉団体への攻撃で同ツールが使用されたケースであり、少なくとも 2022 年初頭から攻撃で使用されていたものとみられます。2022 年夏以前は、中国のサイバー犯罪集団が東アジアのターゲット (主に香港と中国) への攻撃においてのみ SILKLOADER を使用していました。しかし、同年 7 月に一旦その活動を停止しました。その後 9 月に入ると、台湾、ブラジル、フランスなど様々な国の多くのターゲットに向けた攻撃で再び観測されるようになりました。



(Silkloader 使用のタイムライン)

こうした攻撃の傾向から、ウィズセキュアのリサーチャーたちは SILKLOADER がロシアのサイバー犯罪集団の手に渡ったと結論付けました。最も可能性の高い説明は、中国のサイバー犯罪者がロシアの同業者たちに SILKLOADER を販売したということです。

WithIntel でリサーチャーを務める Mohammad Kazem Hassan Nejad (モハマッド・カゼム・ハッサン・ネジャッド) は SILKLOADER の動きについて、以下のように述べています。
「私たちは、SILKLOADER が現在、Packer-as-a-Service プログラムを通じて直ちに使用可能な (off the shelf) ローダーとしてロシアのランサムウェアグループ内で共有されていると考えています。あるいは、Cobalt Strike/Infrastructure-as-a-Service を提供するグループ経由で、信頼のおけるサイバー攻撃者グループに配布されている可能性もあります。これまで、ランサムウェアのような攻撃の初期段階でのハンズオン侵入の際にこれらが観測されていました。それらのグループの多くは、ランサムウェア犯罪集団として名をはせ、活動を終了したと考えられている『Conti』グループと直接または間接的に密接な協力関係を持っていたものと考えられます。」

ローダー (Loader) と呼ばれるマルウェアの一種である SILKLOADER は、VLC Media Player を使用した DLL サイドローディングと呼ばれる手法を悪用し、デバイス上で Cobalt Strike のビーコンを起動させるものです。これらのビーコンは、攻撃者が感染したデバイスに継続的にアクセスし、さらに使用し続けることを可能にします。

Hassan Nejad によると、このローダーは Cobalt Strike ビーコンを見えなくして、被害者のマシンの防御対策を回避するよう設計されています。
「Cobalt Strike ビーコンは非常によく知られた存在であり、十分に保護されたマシンにおいてはビーコンの検出はほぼ保証されています。しかし、ファイルの内容にさらに複雑なレイヤーを追加し、サイドローディングによって VLC Media Player などの既知のアプリケーションを介して起動することで、攻撃者はこれらの防御対策を回避しようとしているのです。」

サイバー犯罪ネットワークへの対抗策

ウィズセキュアのバイスプレジデントで WithIntel の責任者を務める Paolo Palumbo (パオロ・パルンボ) によると、ローダーは既に多くの脅威アクターが購入できるサービスとなってしまっているため、ターゲットとなり得る企業／団体にとっては、ローダーに対抗する上で使用できる技術の開発が重要となっています。
「攻撃者はサイバー犯罪業界のリソースを上手く活用して新しい能力や技術を獲得し、ターゲットが持つ防御策に素早く適応して攻撃を仕掛けようとしています。そのため、防御側もリソースを特定の攻撃グループやその手法に絞り込んで対策を立てることが困難になってきています。その反面、攻撃側がリソースを共有することで、防御側である企業／団体は、複数の攻撃グループが共有／使用するリソースに対抗する戦略を立てることで、より効果的な防御が可能になるということも言えるのです。」

ウィズセキュアでは、WithSecure™ Elements と WithSecure™ Countercept Managed Detection and Response により、SILKLOADER を使用した攻撃／関連アクティビティを検知しています。これらのソリューションの詳細については、こちらのページをご覧ください。
https://www.withsecure.com/jp-ja/solutions

SILKLOADER に関するレポート (英語) は、以下のページでご覧いただけます。
https://www.withsecure.com/content/dam/with-secure/ja/news-library/20230316_WithSecure_Silkloader_Report_ENG.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 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 でも情報の発信をおこなっています。