報道関係者各位

ウィズセキュア、医療研究／エネルギー産業へのサイバー攻撃は北朝鮮の「Lazarus Group」によるものと特定

～ 過去の攻撃キャンペーンの攻撃手法／テクノロジー／戦術における酷似点を多数観測 ～

2023 年 2 月 1 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、同社のセキュリティリサーチチームが、最近観測されたヨーロッパ／北米／南アジアの医療研究／エネルギー産業へのサイバー攻撃キャンペーンが、北朝鮮の国家サイバー攻撃グループ「Lazarus Group」によるものであると特定したリサーチ結果を発表しました。

Lazarus Group は、北朝鮮の朝鮮人民軍偵察総局の一部であると目される APT (Advanced Persistent Threat = 高度かつ持続的な脅威) グループです。ウィズセキュアのリサーチチームは、WithSecure™ Elements セキュリティプラットフォームで保護されている企業でランサムウェアの疑いのある攻撃が検知されたことをきっかけに、Lazarus Group の最新攻撃キャンペーンを観測しました。調査の結果、このキャンペーンはランサムウェアではなく、より大規模な情報収集オペレーションの一部であることを示す証拠をさらに発見しました。収集した証拠に基づき、このキャンペーンは Lazarus Group が諜報活動のために官民の医療研究機関、エネルギー／リサーチ／防衛／医療の各分野で利用される技術の開発メーカー、主要大学のケミカルエンジニアリング関連研究室などをターゲットにしていたものであると結論付けました。

日本のエネルギー業界は今回当社が調査した Lazarus Group による攻撃キャンペーンのターゲットとはなっていないと思われるものの、2022 年前半には同グループによるカナダ／アメリカ／日本のエネルギー関連企業へのサイバー攻撃が観測されており、また、同グループはこれまで日本を含む多くの国の暗号資産業界に攻撃を仕掛けたと目されているため、日本企業も防御を緩めてはならない状況となっています。

ウィズセキュアでシニアスレットインテリジェンスリサーチャーを務める Sami Ruohonen (サミ・ルオホネン) は、今回の Lazarus Group の攻撃キャンペーンの観測について、以下のように述べています。
「私たちは当初、これらは BianLian ランサムウェア攻撃であるとの疑いを持っていましたが、収集した証拠はすぐに別の方向を示しました。さらなる証拠を集めるにつれ、この攻撃キャンペーンは北朝鮮政府に関連するサイバー攻撃グループによって実行されたと確信し、最終的にこれは Lazarus Group によるものであると確信するに至りました。」

「今回のように攻撃キャンペーンと実行グループを強く結びつけることができるのは極めて異例のことです」と、ウィズセキュアのシニアスレットインテリジェンスアナリストである Stephen Robinson (スティーヴン・ロビンソン) は語っています。

Lazarus Group がこれまでの攻撃キャンペーンで使用した攻撃手法／テクノロジー／戦術などから、ウィズセキュアではこの攻撃キャンペーンは Lazarus Group によるものであるという結論に達しました。

以下、今回の攻撃キャンペーンにおいて、過去の攻撃から進化したと考えられる点の一部となります:

● これまでの攻撃とは異なり、ドメイン名を使用せず IP アドレスのみに依存するなど、新しいインフラが使用されている
● Lazarus Group や Kimsuky (北朝鮮が関与する別の攻撃グループ) が過去の攻撃で使用したインフォスティーラー型マルウェア「Dtrack」の改良版が使用されている
● 攻撃者がファイアウォールをバイパスしてリモートデスクトッププロトコル権限を持つ新しい管理者アカウントを作成できるマルウェア「GREASE」の新バージョンが使用されている

リサーチチームが発見した注目すべき証拠の 1 つは、北朝鮮に属する 1,000 未満の IP アドレスのうちの 1 つを攻撃者が短期間使用していたことです。この IP アドレスは、攻撃者が管理する Web シェルに短時間接続されたことが確認されており、リサーチチームでは、Lazarus Group のメンバーが手動で行ったミスであると推測しています。

しかし、攻撃側がこのようなミスを犯したからといって、防御側が安心して警戒を解いてはならないと、ウィズセキュアのスレットインテリジェンス部門の責任者である Tim West (ティム・ウエスト) は注意を喚起しています。
「Lazarus Group はオペレーションにおいてミスを犯したにもかかわらず、その優れた技術を発揮し、慎重に選択されたエンドポイントに対応した行動を取ることができました。高度なエンドポイントの検知テクノロジーを備えていても、防御側である企業／団体は継続した警戒体制を敷く必要があります。特に、優秀で巧妙な攻撃者に対してより深い防御を行うためには、スレットインテリジェンスとスレットハンティングの併用が必要であると考えます。」

今回の Lazarus Group による攻撃キャンペーンのリサーチに関する詳細および英語版レポートは、以下のページでご覧いただけます。
https://www.withsecure.com/jp-ja/expertise/resources/no-pineapple

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。