報道関係者各位

エフセキュア、暗号通貨業界へのサイバー攻撃における Lazarus Group の関与についてのレポートを発表

～ 北朝鮮とのつながりを指摘されるサイバー犯罪集団が日本や米国など 14 ヶ国への攻撃を実行～

2020 年 8 月 26 日
エフセキュア株式会社

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 F-Secure (本社: フィンランド・ヘルシンキ、CEO: Samu Konttinen、日本法人: 東京都港区、以下、エフセキュア) は本日、暗号通貨業界の企業に対する攻撃に Lazarus Group が関与しているとのレポートを発表しました。APT38／Hidden Cobra／Zinc などの別名でも知られる Lazarus Group は北朝鮮とのつながりが深いとされる、高度な技術を持つ、主に金銭目当ての攻撃を仕掛けるサイバー犯罪者集団です。エフセキュアが検証をおこなった攻撃から得られた証拠と既存の研究を結び付けることにより、事件が米国、英国、オランダ、ドイツ、シンガポール、日本、およびその他の国の暗号通貨業界を対象としたサイバー攻撃キャンペーンの一部であったという結論に達しています 。

エフセキュアの戦術的インテリジェンスレポート (Tactical Intelligence Report) は、暗号通貨業界の企業からの依頼によるインシデントレスポンス調査中に発見されたサンプル、ログ、およびその他の技術的な痕跡の分析を掲載しています。レポートによると、攻撃に使用された悪意のあるインプラント (密かにインストールされたスパイウェア) は、以前にも Lazarus Group が使用したと報告されているツールとほぼ同じものでした。

レポートは、サービスを介したスピアフィッシング (今回に関しては、LinkedIn を使用してユーザのプロファイルに合致する偽の求人情報の送信) など、攻撃中に使用された TTP (戦術、手法、手順) について解説しています。エフセキュアの検知および対応 (Detection & Response) 担当ディレクターである、Mat Lawrence (マット・ローレンス) は、この調査は、実用的なセキュリティアドバイスのための強固な基盤を企業に提供するものだと語っています。
「私たちの調査には、インシデントレスポンス、マネージドの検知と対応、そしてエフセキュアの戦術防御ユニット (Tactical Defense Unit) からの洞察が盛り込まれています。今回の調査対象となった攻撃には、Lazarus Group による既知の活動と多くの共通点があることが判明しており、私たちは彼らが攻撃の背後にいることを確信しています。発見した証拠はまた、これが十数ヶ国の企業に対して進行中の攻撃キャンペーンの一部であることを示唆しており、証拠の出処は非常に重要なものとなります。企業はこのレポートを使用することで、今回のインシデントや TTP、そして Lazarus Group について理解し、将来の攻撃から身を守ることができるのです。」

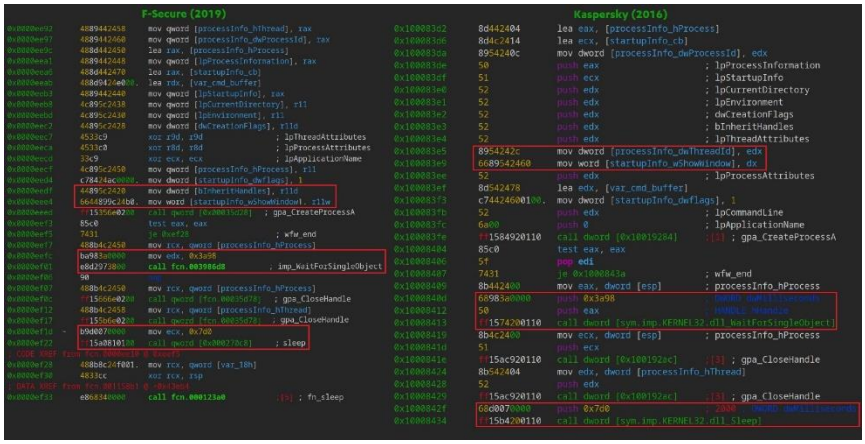

図: ネットワークバックドアの類似性

Lazarus Group の攻撃から回収されたフィッシングの痕跡に基づき、エフセキュアのリサーチャーたちは、今回の事件を少なくとも 2018 年 1 月からこれまでに進行中の広範な攻撃キャンペーンと関連付けることができました。レポートによると、同様の痕跡が少なくとも以下の 14 ヶ国に向けた攻撃キャンペーンにおいて発見されています。

米国、中国、イギリス、カナダ、ドイツ、ロシア、韓国、アルゼンチン、シンガポール、香港、オランダ、エストニア、日本、フィリピン。

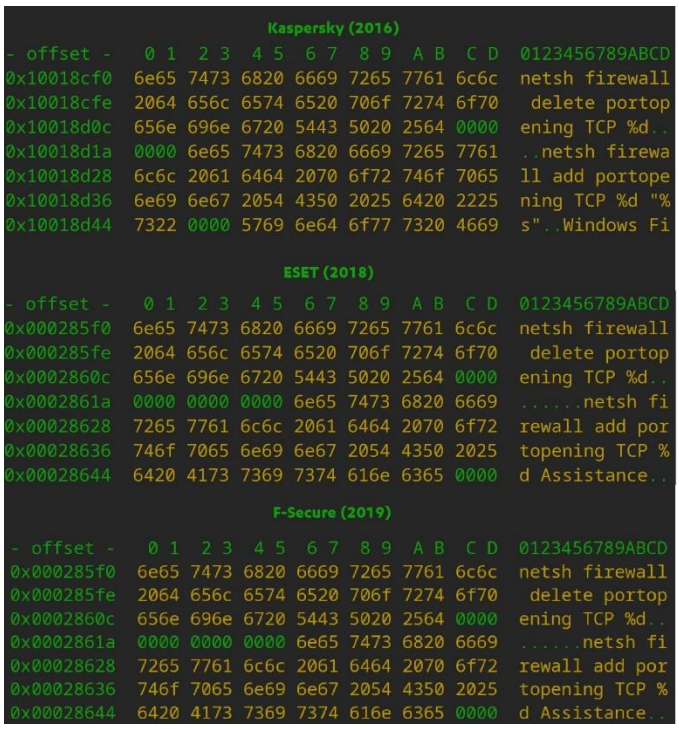

図: Netsh 文字列の共通性

Lazarus Group はその攻撃において、標的企業による防御を回避するために多大な労力を費やしました。例えば、侵害されたホストのウイルス対策ソフトウェアの無効化や、悪意のあるインプラントの証拠の削除などです。また、この報告では攻撃は非常に巧妙なものであると説明していますが、Lazarus Group がその存在を隠そうとする努力でさえ、彼らの活動の証拠を探ろうとするエフセキュアの調査を妨げるには不十分であったと指摘しています。

レポート『暗号通貨を狙う Lazarus Group の攻撃キャンペーン』には、侵害の指標、攻撃で使用された TTP のリスト、Lazarus Group の活動を検出するための追加のアドバイスなど、防御側にとって役立つ多くの詳細情報が含まれています。詳細なレポート (日本語版) は、以下のブログページよりご覧いただけます。
https://blog.f-secure.com/ja/threat-intelligence-report-lazarus-group-targeting-cryptocurrency/

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関する AI テクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。

エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフ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 https://www.f-secure.com/en/welcome (英語) および https://www.f-secure.com/ja_JP/ (日本語) をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

※以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
広報部　秦　和哉
TEL：03-4578-7745 (直通)　　japan-pr@f-secure.com