Press Release
報道関係各位

SecurityScorecard株式会社
2025年3月27日

SecurityScorecard
北朝鮮による世界規模のデータ窃取攻撃に関する最新調査レポート
「Operation Phantom Circuit」を発表

SecurityScorecard株式会社（本社：米国、ニューヨーク州、CEO：アレクサンドル・ヤンポルスキー、以下SecurityScorecard、日本法人代表取締役社長　藤本 大）は、同社の脅威分析チーム「STRIKE」が実施した最新の調査レポート、「**Operation Phantom Circuit：北朝鮮による世界規模のデータ窃取攻撃**」を発表しました。本レポートでは、北朝鮮のハッカー集団「Lazarus」による世界規模のデータ窃取攻撃の手口を詳細に分析し、サプライチェーン攻撃を通じて正規ソフトウェアを改ざんしてバックドアを仕込み、企業や開発者の機密データを巧妙に奪取する手法が明らかになりました。

背景
2024年9月以降に確認された複数のコマンド＆コントロール（C2）サーバーを経由した、北朝鮮からの支援を受けるハッカー集団「Lazarus」によるサプライチェーン攻撃であることが明らかになりました。攻撃で悪用されたC2サーバーは共通の構造を持ち、ペイロードの配信や感染端末との通信に利用されていました。さらに、Reactアプリケーションと Node.js APIで構築されたWebベースの管理プラットフォームが存在し、高度な機能を備えたこのサーバーによって窃取したデータの管理、感染端末の監視、攻撃全体の統制を行っていたことが確認されています。

サプライチェーン攻撃の手口
難読化されたバックドアを埋め込むことで、正規のソフトウェアパッケージを改ざんし、ソフトウェア開発者を騙すことで、これらの危険なパッケージを実行させることが確認されています。一般人の目にはわからないため、感染者に気づかれず、巧妙に実行されます。こうしたパッケージには、暗号通貨アプリから認証ソリューションまで、あらゆる種類のソフトウェアが含まれている可能性があります。

全世界への拡大
全世界の暗号通貨業界とソフトウェア開発者を標的に、世界規模の攻撃を組織的に行っていたことが明らかになりました。この攻撃によって、何百人もの感染者がペイロードをダウンロードして実行し、その間に窃取されたデータは密かに北朝鮮・平壌へ送信されていました。

主な調査結果
- **攻撃インフラの特定に成功**

Lazarusが使用していた標的型攻撃の作戦インフラを特定し、Astrill VPNからのトラフィックをプロキシを通じて、目的地のC2サーバーへ巧妙にルーティングしていた事実を明らかに

- **北朝鮮からの通信を追跡**
  VPN経由で平壌にある6つの異なるIPアドレスへ接続が行われていたことが判明し、攻撃の背後に北朝鮮が存在する明確な証拠を入手
- **ソフトウェアサプライチェーン攻撃の実施**
  正規ソフトウェアに悪質なコードを埋め込むサプライチェーン攻撃が行われ、2024年9月～2025年1月の間に世界中で233件の被害を確認
- **高度なC2管理アプリケーションの存在**
  窃取データや攻撃の制御には、ReactアプリケーションとAPIで構築された専用の管理アプリケーションが使用されており、全てのC2サーバーに展開され、ポート1245を通じて管理されていたことが判明

今回の攻撃は、ユーザーが信頼を寄せる開発ツールにペイロードを埋め込むことで、ソフトウェアサプライチェーン全体に影響を与えた点が特に深刻であり、企業や開発者が使用する正規ソフトウェアでさえ安全ではないことを示唆しました。また、攻撃者はVPNやプロキシを悪用して発信元を隠蔽し、検出を最小限に抑え、防護策を回避しながら、長期間にわたり攻撃インフラを維持していたため、**サプライチェーン全体の監視・防御の重要性が改めて浮き彫りになりました。**

SecurityScorecardは、以下の対策を推奨しています。

推奨されるセキュリティ対策

- ソフトウェアのコード検証プロセスを厳格化
- ネットワークトラフィックの常時監視
- サプライチェーンのセキュリティ体制強化
- セキュリティ担当者同士のグローバル規模での情報共有の強化
- Lazarusのような高度な攻撃手法に備える体制整備
- 難読化・ゼロデイに対応する高度な分析・検知機能の導入
- 堅牢な監視ツールを導入し、リアルタイムで脅威を検知・対応
- パッチ管理の徹底
- 予防的防御の導入

調査方法

この調査では、北朝鮮からの支援を受けるハッカー集団「Lazarus」によるサイバー攻撃の全容を明らかにするため、複数の技術的手法と情報源を組み合わせた多層的なアプローチが取られました。詳細はこちらのレポートを御覧ください。

その他のリソース

- 調査レポート「Operation Phantom Circuit：北朝鮮による世界規模のデータ窃取攻撃」はこちらを御覧ください。
- SecurityScorecardの脅威インテリジェンスについて詳しくは、弊社ウェブサイト（ https://securityscorecard.com/platform/ ）をご覧ください。

SecurityScorecard のThreat Research, Intelligence, Knowledge, and Engagement (STRIKE) チームについて
独自の脅威インテリジェンス、インシデント対応の経験、サプライチェーンのサイバーリスクに関する専門知識を兼ね備えています。SecurityScorecardのテクノロジーに支えられたSTRIKEチームは、世界中のCISOの戦略的アドバイザーとなり、STRIKE チームによる脅威調査を基に、組織にサプライ チェーンのサイバー リスクと攻撃者の特性に関してアドバイスを行っています。

SecurityScorecardについて
Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、Riverwood Capitalなど、世界トップクラスの投資家から出資を受けたSecurityScorecardは、サイバーセキュリティ レーティングにおけるグローバルリーダーであり、Supply Chain Detection and Response（SCDR・サプライチェーンにおける検知・対応）ソリューションのパイオニアです。
セキュリティとリスクの専門家であるアレクサンドル・ヤンポルスキー博士とサム・カッスーメによって2013年に設立されたSecurityScorecardの特許取得済みセキュリティレーティングテクノロジーは、企業のリスク管理、サードパーティリスク管理、取締役会報告、デューデリジェンス、サイバー保険の引き受け、規制当局の監視のために25,000以上の組織で使用されています。
SecurityScorecardは、企業におけるサイバーセキュリティ・リスクの理解、改善を促進し、取締役会、従業員、ベンダーに伝える方法を変革することで、世界をより安全にすることを目指します。https://jp.securityscorecard.com/

日本法人社名 ： SecurityScorecard株式会社（セキュリティスコアカード）
本社所在地 ： 東京都千代田区丸の内一丁目 1 番 3 号
代表取締役社長 ： 藤本 大

【本件に関する連絡先】
SecurityScorecard
広報代理店 株式会社プラップジャパン
担当　菊池(070-2161-7123)、牟田(090-4845-9689)、冨安(070-2161-6963)
Email: securityscorecard@prap.co.jp