令和4年 10 月 14 日
金　　融　　庁
警　　察　　庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年 10 月7日に公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年4月 18 日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にあります。

このサイバー攻撃グループは、

- 標的企業の幹部を装ったフィッシング・メールを従業員に送る
- 虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近する

などにより、マルウェアをダウンロードさせ、そのマルウェアを足がかりにして被害者のネットワークへアクセスする、いわゆるソーシャルエンジニアリングを手口として使うことが確認されています。その他様々な手段を利用して標的に関連するコンピュータネットワークを侵害し、暗号資産の不正な窃取に関与してきているとされ、今後もこのような暗号資産の窃取を目的としたサイバー攻撃を継続するものと考えられます。

また、最近では分散型取引所による取引など暗号資産の取引も多様化しており、秘密鍵をネットワークから切り離して管理するなど、事業者だけでなく個人のセキュリティ対策の強化も重要となっています。

暗号資産取引に関わる個人・事業者におかれましては、暗号資産を標的とした組織的なサイバー攻撃が実施されていることに関して認識を高く持っていただくとともに、以下に示すリスク低減のための対処例を参考に適切にセキュリティ対策を講じていただくようお願いいたします。あわせて、不審な動き等を検知した際には、速やかに所管省庁、警察、セキュリティ関係機関等に情報提供いただきますよう重ねてお願いいたします。

【リスク低減のための対処例】

前述のサイバー攻撃グループは、多様な手法、手口を駆使しているとされるところ、次のような対策の実施を推奨します。

（1）この種のサイバー攻撃に対する優先度の高い対策

○ ソーシャルエンジニアリングに関する意識の向上、ユーザ教育の実施

ソーシャルエンジニアリングの手法・技術について理解し、常に注意を払う。例えば、電子メールを介したマルウェア感染のリスクを低減するため、電子メールの添付ファイル又はハイパーリンクを不用意に開封又はクリックしない。企業・組織等においては、職員のトレーニングの実施を検討する。

例：SNS のプロフィールに違和感や偽りがないか。

○ ファイルをダウンロードする際の配信元の確認

外部からファイルをダウンロードする際には、配信元が信頼できるソースであることを常に確認する。特に暗号資産関連のアプリケーションは真正性が確認できる配信元以外からダウンロードしない。

例：配信元の Web サイトは別サイトを模したものや、登録後間もないドメインではないか。
社内資料のやり取りに社外の URL を使用していないか。

○ 秘密鍵のオフライン環境での保管

暗号資産への不正アクセスを防止するため、秘密鍵をインターネットから切り離されたハードウェアウォレット等のデバイス上などで保管する。

（2）この種のサイバー攻撃に対して効果的な対策

○ 電子メールに関する対策の実装

システム管理者等においては、電子メールの添付ファイルやハイパーリンクのスキャンを行う。

○ ドメインとの通信に関する対策の実装

レピュテーションの低いドメインや登録後間もないドメインとの通信について確認や制限を行う。

○ アプリケーションセキュリティの強化

マルウェア感染のリスクを低減するため、システム管理者等は、アプリケーション許可リストを用いて、許可されていないプログラムの実行を禁止する。また、Office ファイルのマクロ機能については、必要がなければ無効にする。

（3）多様な手法、手口に備えたその他の一般的な対策

○ セキュリティパッチ管理の適切な実施

ソフトウェアや機器の脆弱性に対して、迅速にセキュリティパッチを適用する。パッチ適用を可能な限り迅速化し、適用漏れをなくすため、脆弱性管理やパッチ管理を行うプログラムの導入を検討する。

○ 端末の保護（いわゆるエンドポイント・プロテクション等）

端末（PC、タブレット端末、スマートフォン等）のセキュリティ機能の活用や、セキュリティ対策ソフトの導入を行う。

○ ソフトウェア等の適切な管理・運用、ネットワーク・セグメンテーション

ソフトウェア及び機器のリストを管理し、不要と判断するものは排除する。また役割等に基づいてネットワークを分割する。

○ 本人認証の強化、多要素認証の実装

パスワードスプレー攻撃やブルートフォース攻撃によって認証が破られるリスクを低減するために、パスワードは十分に長く複雑なものを設定する。また、複数の機器やサービスで使い回さない。

システム管理者等においては、多要素認証を導入し本人認証をより強化する。また、不正アクセスを早期に検知できるようにするために、ログイン試行を監視する。

○ アカウント等の権限の適切な管理・運用

アカウントやサービスの権限はそのアカウント等を必要とする業務担当者にのみ付与する。特権アカウント等の管理・運用には特に留意する。

○ 侵害の継続的な監視

ネットワーク内で不審な活動が行われていないか継続的に監視を行う。たとえば、業務担当者以外がシステムやネットワークの構成に関する資料へアクセスするといった通常の行動から外れた活動や、外部の様々な脅威情報と一致するような不審な活動の監視を行う。

○ インシデント対応計画、システム復旧計画の作成等

インシデント発生時に迅速な対応をとれるように、インシデント対応の手順や関係各所との連絡方法等を記した対応計画を予め作成し、随時見直しや演習を行う。また包括的な事業継続計画の一部としてシステム復旧計画の作成等を行う。

○ フィッシングサイトへの注意

暗号資産取引所等を装ったフィッシングサイトに注意を払う。企業・組織等において自社を装ったフィッシングサイトを把握した場合は、利用者等への注意喚起を行う。

【参考資料】

○「安保理決議に基づく対北朝鮮措置に関する中間報告書（2022）」（令和４年 10 月７日公表 国連安保理北朝鮮制裁委員会専門家パネル）
https://undocs.org/S/2022/668

○「TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies」（令和４年４月 18 日）
https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

○「AppleJeus: Analysis of North Korea’s Cryptocurrency Malware」（令和３年２月 17 日）
https://www.cisa.gov/uscert/ncas/alerts/aa21-048a

○「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」（令和４年３月 24 日　経済産業省、総務省、警察庁、NISC）
https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf

○「サイバーセキュリティ対策の強化について（注意喚起）」（令和４年３月１日　経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、NISC）
https://www.nisc.go.jp/pdf/press/20220301NISC_press.pdf

○「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」（令和４年２月 23 日　経済産業省）
https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

（以上）