令和６年 12 月 24 日

一般社団法人　日本暗号資産等取引業協会　会長　殿

金融庁総合政策局長
屋敷　利紀

暗号資産の流出リスクへの対応等に関する再度の自主点検要請について

本日、警察庁・内閣サイバーセキュリティセンター・金融庁の連名で、「北朝鮮を背景とするサイバー攻撃グループ TraderTratior によるサイバー攻撃について（注意喚起）」が出されたところですが、当該注意喚起は、本年５月に発生した暗号資産交換業者における暗号資産の不正流出事案に関する具体的なソーシャルエンジニアリングの手法が判明したことを踏まえ、参考となる手口例や緩和策を示しつつ、事業者に適切なセキュリティ対策を講じることを要請する内容となっています。

先般（9 月 26 日）、当庁から、貴協会を通じ、貴協会会員に対して、暗号資産の流出リスクへの対応及びシステムリスク管理態勢に関し、事務ガイドライン第三分冊（金融会社関係 16．暗号資産交換業者関係）等に記載している内容が適切に実施されているかに関して自主点検を行うことを要請したところですが、今回の注意喚起の内容を踏まえ、ウォレットに関する管理態勢を含めて、改めて速やかに自主点検を行うことを貴協会会員に対して求めるとともに、その結果を取りまとめてご連絡いただくようにお願いします。

（参考添付）「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について（注意喚起）」

以上

令和６年 12 月 24 日
警　　察　　庁
内閣サイバーセキュリティセンター
金　　融　　庁

北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について
（注意喚起）

本日（令和６年 12 月 24 日）、警察庁、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）は連名で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、暗号資産関連事業者「株式会社 DMM Bitcoin」から約 482 億円相当の暗号資産を窃取したことを特定したと公表しました。

TraderTraitor に関しては、米国では令和４年４月 18 日に、FBI、米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）及び米国財務省の連名で注意喚起が行われています。また、TraderTraitor は、北朝鮮当局の下部組織とされる「Lazarus Group」（ラザルスグループ）の一部とされていますところ、Lazarus Group については、我が国でも同年 10 月 14 日に、金融庁、警察庁及び内閣サイバーセキュリティセンターの連名で「「ラザルス」と呼称されるサイバー攻撃グループ」として既に一度注意喚起を行うなど、累次にわたり注意喚起が行われている状況にあります。

北朝鮮による暗号資産の窃取に関しては、本年９月３日に、FBI がソーシャルエンジニアリングの手法を用いた北朝鮮による暗号資産の手口や対応策に関する資料を公表しているところです。

今回、警察庁関東管区警察局サイバー特別捜査部及び警視庁の捜査・分析による結果、具体的なソーシャルエンジニアリングの手法が判明したことから、以下に示す手口例及び緩和策を参考に、標的となり得る組織や事業者に適切なセキュリティ対策を講じていただくことを目的として注意喚起を発出しました。北朝鮮は引き続き暗号資産の窃取を企図し続けるものとみられるところ、暗号資産取引に関わる個人・事業者におかれましては、サイバー空間の脅威を認識いただくとともに、ネットワークの不審な通信を検知した際には、速やかに金融庁等所管省庁、警察、内閣サイバーセキュリティセンター、セキュリティ関係機関等に情報提供いただきますようお願いします。

【手口例及び緩和策】

1　ソーシャルエンジニアリングによる接近手口例

- 攻撃者は、第三者の名前や顔写真を悪用し、企業幹部を装うなどして、SNS で標的対象者にメッセージを送信します。
- 標的となるのは、日本人だけではなく、国内外に居住する、外国人を含む暗号資産関連事業者の従業員です。また、ブロックチェーンや Web3 と呼ばれる技術の技術者も標的となり得ます。
- 攻撃者は、アプローチの際に、標的対象者のプロフィールに掲載されている経歴やスキルを元に、関心を引くような問いかけを行います。例えば、ソフトウェア技術者であれば、「あなたからプログラミングを学びたい」「私のプログラムの不具合を直してほしい」といったものです。
- 攻撃者は、異なる SNS や、メッセージングアプリでのやりとりを希望する場合があります。これは、攻撃者側が、送信したメッセージを受信者側の記録から消去できるサービスを利用したいことが理由として考えられます。

2　マルウェアを感染させる手口例

- 攻撃者は、標的対象者の PC をマルウェアに感染させようとします。
- 例えば、攻撃者が GitHub にコミットした、「不具合があってうまく動かない」と主張する、シンプルな API へアクセスするプログラムを、標的対象者に実行させて、不具合を特定させようとすることが考えられます。
- 攻撃者は、API の通信先に、正規のサーバーのほか、攻撃者が用意したサーバーを含めており、API からの応答を処理する関数に、コード実行可能な関数を紛れ込ませて、マルウェアに感染させようとする可能性があります。
- 他にも、様々な手口によって、標的対象者で不正なプログラムを実行させることでマルウェアに感染させようとします。

3　認証情報等の窃取～暗号資産窃取の手口例

- 攻撃者は、マルウェア感染させた PC に保存されている認証情報や、セッションクッキー等を窃取し、標的対象者になりすまして、暗号資産管理やブロックチェーン関連業務で利用するシステムにアクセスし、暗号資産等の窃取を行おうとする可能性があります。また、個人管理する暗号資産の窃取を狙うことも考えられます。
- 攻撃者は、システム構成を短期間で把握し、なりすました標的対象者が持つロールや権限に応じた、暗号資産の窃取が可能なポイント・手法を見つけ出そうとするおそれがあります。

4　対処例と緩和策

令和 4 年 10 月 14 日付の注意喚起に掲載した 【リスク低減のための対処例】 と重複する部分もありますが、以下の対処例と緩和策の実施を推奨します。

(1) システム管理者向け

- 通信先ドメインの登録日が数日～数週間前など、比較的新しくないか確認する。
- 多要素認証を導入する。
- 業務付与期間に限定した必要最小限のアクセス範囲と権限を付与する。(業務付与期間終了後、速やかに縮小・削除する。)
- 事前申請または通常の業務時間帯・曜日ではない期間に行われたアクセスに関する認証ログ、アクセスログがないか監視する。(例：時差の大きい地域に居住する従業員が、通常は日本時間の夜や早朝にアクセスしているにもかかわらず、ある時期から日本時間の日中もアクセスしている等。)
- EDR や PC 内のログと矛盾がないか監視する。(例：PC が電源 OFF している期間にアクセスしていないか。)
- 居住地以外の地域や VPN サービスからとみられるアクセスに関する認証ログ、アクセスログがないか監視する。
- 貸与している業務用 PC 以外からとみられるアクセスに関する認証ログ、アクセスログがないか監視する。(例：UserAgent が通常と異なる。)
- 退職した従業員のアカウントは速やかにロックするとともに、認証試行があった際は、速やかに検知・対処ができるようにしておく。
- 従業員の理解と協力を得て、ダミーの認証情報を Web ブラウザに記憶させる等しておき、認証試行があった際は、速やかに検知・対処ができるようにしておく。
- PC のログ保存期間や、マルウェアに感染した後にログが消去されるリスクを考慮し、ログを集中的に保存・検索できる仕組みを構築し、異常の把握と速やかな対処ができるようにしておく。

(2) 従業員向け

- 事前に許可されている場合を除き、私用 PC で機微な業務用システムにアクセスしない。
- SNS でアプローチを受けた際は、ビデオ通話を要求する。(複数回拒否する場合は不審と判断する。)
- アプローチ元のプロフィールや、SNS でのやりとりについて、スクリーンショットを保存する。
- ソースコードの確認や実行を急がせる兆候があれば、不審性を考慮する。
- 内容を確認せずにコードを実行せず、コードエディタで開いて、折り返し表示に

する。

- コードを実行する際は、業務用 PC を使用しない、または仮想マシンを使用する。

5　対応

被害拡大防止および適切な事後対策に必要となる原因究明のため、PC のマルウェア感染が疑われる場合は、原則として電源を入れたまま、速やかにインターネットや業務用ネットワークから隔離し、なるべく早く適切な保全措置を行ってください。（メモリダンプを含む揮発性情報の収集を優先的に行ってください。）

（以上）