令和6年 12 月 24 日
警　　察　　庁

北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について

警察庁は、同庁関東管区警察局サイバー特別捜査部及び警視庁による捜査・分析の結果を総合的に評価し、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）とともに、令和6年5月に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、我が国の暗号資産関連事業者「株式会社 DMM Bitcoin」（以下「DMM」という。）から約 482 億円相当の暗号資産を窃取したことを特定しました。

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）の一部とされており、手法の特徴として、同時に同じ会社の複数の従業員に対して実施される、標的型ソーシャルエンジニアリングが挙げられます。

- 令和6年3月下旬、TraderTraitor は、LinkedIn 上で、リクルーターになりすまし、日本に所在する企業向け暗号資産ウォレットソフトウェア会社「株式会社 Ginco」（以下「Ginco」という。）の従業員に接触しました。同サイバー攻撃グループは、Ginco のウォレット管理システムへのアクセス権を保有する従業員に、GitHub 上に保管された採用前試験を装った悪意ある Python スクリプトへの URL を送付しました。被害者は、この Python コードを自身の GitHub ページにコピーし、その後、侵害されました。

- 令和6年5月中旬以降、TraderTraitor は、侵害を受けた従業員になりすますためにセッションクッキーの情報を悪用し、Ginco の暗号化されていない通信システムへのアクセスに成功しました。同月下旬、同サイバー攻撃グループは、同アクセスを利用して、DMM 従業員による正規取引のリクエストを改ざんしたものと認められます。その結果、4,502.9BTC（攻撃当時約 482 億円相当）が喪失しました。最終的に、窃取された資産は TraderTraitor が管理するウォレットに移動されました。

警察庁は、FBI、その他の米国政府機関及び国際パートナーと連携し、引き続き、北朝鮮に利益をもたらすサイバー犯罪及び暗号資産窃取を含む違法な活動を明らかにし、厳正に対処してまいります。

なお、警察庁、内閣サイバーセキュリティセンター及び金融庁は、この攻撃グループの手口例及び緩和策に関する文書を発出しております。暗号資産関連事業者におかれましては、当該文書を併せて御確認ください。

【参考資料】

○ 「FBI, DC3 and NPA Identification of North Korean Cyber Actors, tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.Com」（2024 年 12 月 24 日公表 FBI、DC3、警察庁）
https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom

○ （仮訳）「FBI、DC3 及び警察庁は、Bitcoin.DMM.Com から 3 億 800 万ドルを窃取したとして、北朝鮮のサイバーアクターTraderTraitor を特定」（令和６年 12 月 24 日公表 FBI、DC3、警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20241224_jp.pdf

○ 「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）」（令和６年 12 月 24 日公表 警察庁、NISC、金融庁）
https://www.npa.go.jp/bureau/cyber/pdf/20241224_caution.pdf

（以上）