（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

米国連邦捜査局（FBI）、米国国防省サイバー犯罪センター（DC3）及び警察庁は、2024 年 5 月、北朝鮮のサイバーアクターが日本に所在する暗号資産事業者 DMM から 3 億 800 万ドル相当の暗号資産を窃取したことについて、注意喚起を実施する。この窃取は、TraderTraitor による脅威活動と関連しており、同アクターは Jade Sleet、UNC4899、Slow Pisces としても追跡されている。TraderTraitor の活動の特徴として、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る。

- 2024 年 3 月下旬、北朝鮮のサイバーアクターは、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 Ginco の従業員に接触した。同脅威アクターは、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、侵害された。

- 2024 年 5 月中旬以降、TraderTraitor アクターは、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た。2024 年 5 月下旬、同アクターは、この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る。その結果、4,502.9BTC（攻撃当時 3 億 800 万ドル相当）が喪失した。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した。

FBI、警察庁、その他の米国政府機関及び国際的パートナーは、これからも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、戦いを続けていく。