Nordkoreanische Hacker haben erneut zugeschlagen – diesmal mit einem Diebstahl, der selbst in der Welt der Cyberkriminalität beispiellos ist. Die US-Bundespolizei FBI bestätigte, dass die Gruppe Lazarus hinter dem Diebstahl von 1,5 Milliarden Dollar an virtuellen Vermögenswerten von der Kryptowährungsbörse Bybit steckt. Dieser Angriff könnte als der größte Kryptodiebstahl der Geschichte in die Bücher eingehen.

Hochentwickelte Cyberangriffe aus Nordkorea

Die Attacke auf Bybit fand am 21. Februar statt. Das FBI erklärte, dass Lazarus sogenannte „TraderTraitor"-Taktiken nutzte – eine Kombination aus Spearphishing und mit Malware infizierten Krypto-Anwendungen. Das Ziel: Zugriff auf Wallets und private Schlüssel der Opfer.

Und die Täter sind schnell: „Die Hacker haben bereits begonnen, einige der gestohlenen Vermögenswerte in Bitcoin und andere Kryptowährungen umzuwandeln und über Tausende von Adressen auf mehreren Blockchains zu verteilen", so das FBI in einer offiziellen Mitteilung. Es sei davon auszugehen, dass die Vermögenswerte weiter gewaschen und schließlich in Fiatgeld umgewandelt werden.

Bybit-Chef erklärt „Krieg" gegen Lazarus

Bybit, mit Sitz in Dubai, ist nach Handelsvolumen die weltweit zweitgrößte Krypto-Börse und hat mehr als 60 Millionen Nutzer. Der CEO von Bybit, Ben Zhou, reagierte mit einer Kampfansage: „Wir erklären Lazarus den Krieg!" Er kündigte eine neue Website an, die sich der Jagd auf die gestohlenen Gelder widmet.

Dort können Nutzer die Wallet-Adressen der Hacker verfolgen – und es gibt eine Belohnung: Wer Informationen liefert, die zur Sperrung der Gelder führen, erhält 5 % der wiederhergestellten Summe. Zhou machte klar, dass dies erst der Anfang sei: „Wir werden nicht aufhören, bis Lazarus und andere schlechte Akteure aus der Branche verschwunden sind."

Krypto-Diebstahl zur Finanzierung nordkoreanischer

Waffenprogramme

Warum hackt Nordkorea überhaupt Krypto-Börsen? Ganz einfach: Das Regime von Kim Jong-un finanziert damit sein militärisches Arsenal.

Ein Bericht des inzwischen aufgelösten UN-Sicherheitsrats-Panels schätzte, dass Nordkorea rund 40 % seiner Waffenprogramme durch Cyberkriminalität finanziert. Zwischen 2017 und 2023 sollen 58 Hackerangriffe auf Krypto-Unternehmen etwa 3 Milliarden Dollar in die Kassen von Pjöngjang gespült haben.

Die Cyberkriminalität Nordkoreas hat sich 2024 weiter verschärft: Allein in diesem Jahr haben nordkoreanische Hacker bereits 1,34 Milliarden Dollar gestohlen – verteilt auf 47 Angriffe, so eine Analyse von Chainalysis. Das entspricht unglaublichen 61 % aller weltweit gestohlenen Krypto-Gelder des Jahres.

Lazarus – Nordkoreas berüchtigtste Hackergruppe

Lazarus ist längst kein unbekannter Name mehr. Die Gruppe hat sich in den letzten Jahren durch immer ausgefeiltere Angriffe einen Namen gemacht. Sie nutzt hochentwickelte Malware, Social-Engineering-Taktiken und innovative Kryptodiebstahl-Techniken, um Sanktionen zu umgehen und an frische Devisen zu gelangen.

Ein weiteres besorgniserregendes Detail: Nordkorea verstärkt nicht nur seine Cyberangriffe, sondern auch seine militärische Zusammenarbeit mit Russland. Die USA und Südkorea werfen Pjöngjang vor, Munition und sogar Truppen nach Russland geschickt zu haben, um Moskaus Krieg in der Ukraine zu unterstützen.

Nach Angaben des südkoreanischen Geheimdienstes hat Nordkorea kürzlich weitere Soldaten nach Russland entsandt – einige davon sollen sich bereits an der Front im Gebiet Kursk befinden. Dort hätten sie schwere Verluste erlitten.

Fazit: Ein gefährlicher Trend setzt sich fort

Nordkoreas Cyberkriminalität ist längst keine Randnotiz mehr. Mit jedem erfolgreichen Angriff wächst nicht nur die Kriegskasse des Regimes, sondern auch die Gefahr für den globalen

Kryptomarkt.

Bybit schlägt mit seiner „Jagd auf Lazarus“ eine neue Richtung ein. Ob das genug ist, um Nordkoreas Cyber-Offensive zu stoppen? Die kommenden Monate werden es zeigen.

Von C. Hatty