NACHRICHTEN
Österreich

18. Juni 2025

Pro-Israel Hacker stehlen 90 Millionen Dollar von Irans größter Krypto-Börse

Pro-israelische Hacker, bekannt als „Predatory Sparrow“, beanspruchen den Diebstahl von 90 Millionen US-Dollar von Irans größtem Krypto-Austausch, um den Druck auf das Regime zu erhöhen. Cyberangriffe eskalieren im Konflikt.

Am Mittwoch erbeuteten Hacker das Gegenstück von etwa 90 Millionen US-Dollar von Irans größter Kryptowährungsbörse, wie mehrere unabhängige Krypto-Tracking-Firmen berichteten.

Cyberangriff auf Nobitex

Eine geschickte pro-israelische Hackergruppe, bekannt als „Predatory Sparrow“, übernahm die Verantwortung für den Cyberangriff, der offenbar darauf abzielte, Iran weiter zu destabilisieren, während **militärische Angriffe Israels** auf

Teheran stattfinden.

In einem Beitrag auf X in Farsi gaben die Hacker an, dass sie die iranische Krypto-Börse Nobitex angegriffen hätten und behaupteten, Iran benutze die Börse, um internationalen Sanktionen zu umgehen. In einem außergewöhnlichen Schritt haben die Hacker möglicherweise die gestohlene Kryptowährung ins Leere transferiert, indem sie sie auf digitale „Wallets“ überwiesen, über die sie keine Kontrolle haben, so mehrere Cybersicherheitsexperten.

Anerkennung des Vorfalls durch Nobitex

Nobitex bestätigte den Vorfall in einer Erklärung auf ihrer Website am Mittwoch und gab bekannt, dass der Zugang zur Krypto-Börse aus Vorsichtsgründen „ausgesetzt“ wurde, bis weitere Mitteilungen erfolgen. Die Krypto-Tracking-Firmen **Elliptic** und **TRM Labs** bestätigten, dass die Kryptowährung gestohlen und an „Wallets“ oder Krypto-Konten überwiesen wurde, mit einem Schimpfwort, das auf das iranische Islamische Revolutionsgardekorps (IRGC) anspielte.

Zusätzlicher Cyberangriff auf die Bank Sepah

In einem separaten Hack am Dienstag erklärte Predatory Sparrow, sie hätten Daten der staatlichen Bank Sepah in Iran zerstört, mit der Behauptung, dass Mitglieder des IRGC die Bankdienste als Rechtfertigung für die Aktion genutzt hätten. Die staatlich affiliierte Nachrichtenagentur Fars warnte vor möglichen Störungen der Bankdienstleistungen an Tankstellen.

Eine Quelle in Teheran berichtete CNN, dass sie in den letzten zwei Tagen etwa 10 Geldautomaten aufgesucht hätten und alle entweder nicht funktionierten oder leer waren.

Steigende Cyberkriegsführung zwischen

Israel und Iran

Diese beiden beeindruckenden Cyberangriffe markieren eine Eskalation im jahrelangen Schattenkrieg zwischen Israel und Iran im Cyberspace, wo die Erzfeinde – oder ihre Unterstützer – digitale Spionage und datenzerstörende Angriffe zu taktischen Vorteilen nutzen.

Predatory Sparrow hat sich in den letzten fünf Jahren als Gruppe hervorgetan, die spektakuläre Cyberangriffe durchführt und zuvor eine iranische Stahlfabrik sowie Zahlungsabwicklungen an iranischen Tankstellen gestört hat. Die Hacker präsentieren sich als anti-regierungsnahe iranische Hacktivisten, werden jedoch von Cybersicherheitsexperten weitgehend als mit Israel verbunden vermutet.

Auswirkungen auf die Bevölkerung

Hamid Kashfi, ein persischsprachiger Cybersicherheitsexperte, erklärte gegenüber CNN, dass der Hack auf Nobitex auch gewöhnliche Iraner betreffen könnte, trotz der Behauptungen der Hacker, nur die Vermögenswerte des IRGC ins Visier zu nehmen. In dem aktuellen Krieg mit Israel und dem schwindenden Zugang zu finanziellen Ressourcen setzen „viele Iraner auf Krypto“, sagte Kashfi.

Ein Großteil der jüngsten Cyberaktivitäten, während Israel und Iran Raketenangriffe austauschen, scheint darauf abzuzielen, Panik in beiden Ländern zu säen. Israelis erhielten beispielsweise massenhaft Textnachrichten, die sich als Behörden ausgaben und behaupteten, dass die Bunkerschutzanlagen unsicher seien.

Sicherheitsbedenken der iranischen Regierung

Die iranische Regierung warnte derweil die Bürger davor, den

Messaging-Dienst WhatsApp zu nutzen, aus Angst, dass Israel Informationen aus diesen Chats sammeln könnte. Ein Sprecher von Meta, dem Unternehmen, das WhatsApp besitzt, wies diese Behauptungen zurück und betonte, dass die Nachrichten von WhatsApp Ende-zu-Ende-verschlüsselt seien.

Die Berichterstattung von CNN wurde von Muhammad Darwish unterstützt.

Details