FBI schließt Webseiten, die Nordkoreaner zur Firmenimitierung nutzten

Das FBI hat mehrere Websites beschlagnahmt, die von nordkoreanischen Operativen genutzt wurden, um amerikanische Unternehmen zu imitieren. Diese Maßnahmen sollen Gelder für das nordkoreanische Regime sicherstellen.

Das FBI hat mehrere Websites beschlagnahmt, die von **nordkoreanischen** Operativen genutzt wurden, um sich als legitime US- und indische Unternehmen auszugeben. Dieser Schritt geschah offenbar, um Geld für das mit Nuklearwaffen ausgestattete nordkoreanische Regime zu beschaffen, so Aussagen auf den Websites sowie Sicherheitsforscher, die die Aktivitäten untersucht haben.

Die Beschlagnahmung der Websites

Alle vier von der Cybersecurity-Firma SentinelOne als nordkoreanische Tarnunternehmen identifizierten Websites hatten eine Erklärung in Englisch und Koreanisch, die besagte, dass sie im Rahmen eines Haftbefehls des US-Bezirksgerichts von Massachusetts beschlagnahmt wurden. Dies sei Teil einer „koordinierten Durchsetzungsmaßnahme“ gegen die nordkoreanische Regierung. Die Forscher von SentinelOne konnten die Tarnunternehmen einer größeren Gruppe von Organisationen mit Sitz in China zuordnen.

Die Herausforderung für die nationale Sicherheit

Das Aufspüren und Eliminieren dieser gefälschten Unternehmen stellt eine große Herausforderung für die nationale Sicherheit dar, die die Biden-Administration anzugehen versucht und die die Trump-Administration erben wird. Schätzungen zufolge wird etwa die Hälfte von **Nordkoreas** Raketenprogramm durch Cyberangriffe und Kryptowährungsdiebstahl finanziert, wie ein Beamter des Weißen Hauses im letzten Jahr berichtete.

Vorsätzliche Täuschung durch gefälschte Websites

Die Tarnunternehmen ahmten die Websites mehrerer US-Software- und Beratungsfirmen genau nach und forderten potenzielle Kunden auf, Kontakt aufzunehmen, wie die Analyse von SentinelOne zeigt. Das FBI wollte sich nicht zu dem Fall äußern.

Hinweis auf frühere Warnungen

Die Erklärung des FBI und anderer US-Strafverfolgungsbehörden auf den beschlagnahmten Websites verweist die Besucher auf eine Warnung aus dem Jahr 2022, in der US-Beamte betonten, dass Nordkorea Tausende von IT-Arbeitern im Ausland einsetzt, um heimlich Geld für das Regime zu sammeln.

Untersuchungen und Infiltrationsversuche

Eine Untersuchung von CNN aus jenem Jahr ergab, dass nordkoreanische Operative aggressiv versuchten, in US-Kryptowährungs- und andere Technologiefirmen einzudringen, indem sie sich als Personen anderer Nationalitäten ausgaben. Ein amerikanischer Unternehmer berichtete CNN, dass sein Unternehmen unwissentlich Zehntausende von Dollar an die nordkoreanische Regierung überwiesen hatte.

Internationale Zusammenarbeit in

Betrugsfällen

In einigen Fällen könnte es sein, dass die Nordkoreaner Unterstützung von Amerikanern erhalten. US-Bundesstaatsanwälte haben im Mai eine Frau aus Arizona beschuldigt, an einem ausgeklügelten Betrugsschema beteiligt gewesen zu sein, das ausländischen IT-Arbeitern ermöglichte, sich als Amerikaner auszugeben und bei großen US-Unternehmen angestellt zu werden. Dies führte zu Einnahmen von 6,8 Millionen US-Dollar, die Pyongyang zugutekommen könnten.

Einblick in eine tiefere Operation

„Diese Tarnunternehmen und Websites sind nur die Spitze des Eisbergs“, erklärte Tom Hegel, leitender Bedrohungsforscher bei SentinelOne, gegenüber CNN. „Was wir aufgedeckt haben, stellt nur einen Bruchteil einer viel umfassenderen und tief verwurzelten Operation dar, die darauf abzielt, im Verborgenen zu agieren.“

Rückverfolgung der Aktivitäten bis nach China

Hegel und sein Kollege Dakota Cary konnten einige Aktivitäten der Tarnunternehmen auf eine Adresse in Liaoning zurückverfolgen, der chinesischen Provinz, die an Nordkorea grenzt. Dies ist nicht das erste Mal, dass Forscher nordkoreanische IT-Arbeiter-Operationen nach Nordostchina zurückverfolgen. CNN berichtete im April über einen nordkoreanischen Computer-Server, der Illustrationen enthielt, die offenbar für US-Animationsstudios produziert worden waren. Protokolle des Servers zeigten zahlreiche Zugriffe von Internetverbindungen in Nordostchina.

Besuchen Sie uns auf: die-nachrichten.at