Article

Oct 2024

North Korea aggressively targeting crypto industry with well-disguised social engineering attacks

North Korea is currently conducting an aggressive campaign against the crypto industry using well-disguised social engineering attacks.



Damon Brooker
Information Security Consultant

Email damon.brooker@waterstons.com

It is using extensive pre-operational research to identify potential targets and attempt to contact dozens of employees, with the primary goal to gain unauthorised access to a company's network.

The threat actors create individualised fake scenarios such as offers of new employment or corporate investment, in combination with personal details such as the victim's background, skills, employment or business interests to make the interaction seem more legitimate. By initiating prolonged conversations with victims to build rapport, they are able to deliver malware in situations that may appear natural and non-alerting.

The malicious cyber actors routinely impersonate a range of individuals, including general recruiters, or prominent people associated with decentralised finance. To make impersonations more convincing they have been utilising realistic imagery, and fake images of time sensitive events, to induce immediate actions from intended victims. Additionally, the Department of Justice has identified and seized multiple fake North Korean websites that impersonated recruiting firms or technology companies backed by professional websites designed to make the fake entities appear legitimate.

Wider context

Within the wider context, state-sponsored threat actors are on the rise and engaging in more sophisticated and advanced forms of social engineering attacks on businesses. These state actors are becoming a more common threat and have great capability than seen before with usual threat actors.

It is becoming increasingly difficult to verify and authenticate individuals or businesses that employees are engaging with, to ensure that they are legitimate and aren't hiding malicious intent.

Recommendations

Organisations should not store business critical information on internet connected devices, such as credentials.

Make sure that multiple factors of authentication and approvals from several different unconnected networks are required before prior to any movement of company financial assets.

Train employees and HR to recognise potential red flags when interacting or communicating online, such as avoidance of in person meetings, and demanding that a pre-employment test that executes code on devices must take place.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430