Internet Crime Complaint Center (IC3)

Published: 2024-09-03 · Archived: 2026-04-06 03:18:04 UTC

The Democratic People's Republic of Korea ("DPRK" aka North Korea) is conducting highly tailored, difficult-to-detect social engineering campaigns against employees of decentralized finance ("DeFi"), cryptocurrency, and similar businesses to deploy malware and steal company cryptocurrency.

North Korean social engineering schemes are complex and elaborate, often compromising victims with sophisticated technical acumen. Given the scale and persistence of this malicious activity, even those well versed in cybersecurity practices can be vulnerable to North Korea's determination to compromise networks connected to cryptocurrency assets.

North Korean malicious cyber actors conducted research on a variety of targets connected to cryptocurrency exchange-traded funds (ETFs) over the last several months. This research included pre-operational preparations suggesting North Korean actors may attempt malicious cyber activities against companies associated with cryptocurrency ETFs or other cryptocurrency-related financial products.

For companies active in or associated with the cryptocurrency sector, the FBI emphasizes North Korea employs sophisticated tactics to steal cryptocurrency funds and is a persistent threat to organizations with access to large quantities of cryptocurrency-related assets or products.

This announcement includes an overview of the social engineering tactics North Korean state-sponsored actors use against victims working in DeFi, cryptocurrency, and related industries; potential indicators of North Korean social engineering activity; mitigation measures for those most at risk; and steps to take if you or your company may have been victimized.

North Korean Social Engineering Tactics

Extensive Pre-Operational Research

Teams of North Korean malicious cyber actors identify specific DeFi or cryptocurrency-related businesses to target and attempt to socially engineer dozens of these companies' employees to gain unauthorized access to the company's network. Before initiating contact, the actors scout prospective victims by reviewing social media activity, particularly on professional networking or employment-related platforms.

Individualized Fake Scenarios

North Korean malicious cyber actors incorporate personal details regarding an intended victim’s background, skills, employment, or business interests to craft customized fictional scenarios designed to be uniquely appealing to the targeted person.

North Korean fake scenarios often include offers of new employment or corporate investment. The actors may reference personal information, interests, affiliations, events, personal relationships, professional connections, or

details a victim may believe are known to few others.

The actors usually attempt to initiate prolonged conversations with prospective victims to build rapport and deliver malware in situations that may appear natural and non-alerting. If successful in establishing bidirectional contact, the initial actor, or another member of the actor's team, may spend considerable time engaging with the victim to increase the sense of legitimacy and engender familiarity and trust.

The actors usually communicate with victims in fluent or nearly fluent English and are well versed in the technical aspects of the cryptocurrency field.

Impersonations

North Korean malicious cyber actors routinely impersonate a range of individuals, including contacts a victim may know personally or indirectly. Impersonations can involve general recruiters on professional networking websites, or prominent people associated with certain technologies.

To increase the credibility of their impersonations, the actors leverage realistic imagery, including pictures stolen from open social media profiles of the impersonated individual. These actors may also use fake images of time sensitive events to induce immediate action from intended victims.

The actors may also impersonate recruiting firms or technology companies backed by professional websites designed to make the fake entities appear legitimate. Examples of fake North Korean websites can be found in affidavits to seize 17 North Korean domains, as announced by the Department of Justice in October 2023.

Indicators

The FBI has observed the following list of potential indicators of North Korean social engineering activity:

- Requests to execute code or download applications on company-owned devices or other devices with access to a company's internal network.
- Requests to conduct a "pre-employment test" or debugging exercise that involves executing non-standard or unknown Node.js packages, PyPI packages, scripts, or GitHub repositories.
- Offers of employment from prominent cryptocurrency or technology firms that are unexpected or involve unrealistically high compensation without negotiation.
- Offers of investment from prominent companies or individuals that are unsolicited or have not been proposed or discussed previously.
- Insistence on using non-standard or custom software to complete simple tasks easily achievable through the use of common applications (i.e. video conferencing or connecting to a server).
- Requests to run a script to enable call or video teleconference functionalities supposedly blocked due to a victim's location.
- Requests to move professional conversations to other messaging platforms or applications.
- Unsolicited contacts that contain unexpected links or attachments.

Mitigations

To lower the risk from North Korea’s advanced and dynamic social engineering capabilities, the FBI recommends the following best practices for you or your company:

- Develop your own unique methods to verify a contact's identity using separate unconnected communication platforms. For example, if an initial contact is via a professional networking or employment website, confirm the contact's request via a live video call on a different messaging application
- Do not store information about cryptocurrency wallets — logins, passwords, wallet IDs, seed phrases, private keys, etc. — on Internet-connected devices.
- Avoid taking pre-employment tests or executing code on company owned laptops or devices. If a pre-employment test requires code execution, insist on using a virtual machine on a non-company connected device, or on a device provided by the tester.
- Require multiple factors of authentication and approvals from several different unconnected networks prior to any movement of your company's financial assets. Regularly rotate and perform security checks on devices and networks involved in this authentication and approval process.
- Limit access to sensitive network documentation, business or product development pipelines, and company code repositories.
- Funnel business communications to closed platforms and require authentication — ideally in person — before adding anyone to the internal platform. Regularly reauthenticate employees not seen in person.
- For companies with access to large quantities of cryptocurrency, the FBI recommends blocking devices connected to the company’s network from downloading or executing files except specific whitelisted programs and disabling email attachments by default.

Response

If you suspect you or your company have been impacted by a social engineering campaign similar to those discussed in this announcement, or by any potential North Korea-related incident, the FBI recommends the following actions:

- Disconnect the impacted device or devices from the Internet immediately. Leave impacted devices powered on to avoid the possibility of losing access to recoverable malware artifacts.
- File a detailed complaint through the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov.
- Provide law enforcement as many details as you can regarding the incident, including screenshots of communications with the malicious cyber actors. If possible, take screenshots of (or otherwise save) identifiers, usernames, online accounts, and any other details about the actors involved.
- Discuss options for incident response and forensic examination of impacted devices with law enforcement. In some situations, law enforcement may recommend taking advantage of private incident response companies.
- Share your experience with colleagues, if appropriate, to raise awareness and broaden the public's understanding of the significant malicious cyber threat emanating from North Korea.

For related information and additional details on North Korea's malicious cyber activity, see FBI press releases from September 2023, August 2023, and January 2023, as well as Joint Cybersecurity Advisories released in June 2023 and April 2022.

Source: https://www.ic3.gov/PSA/2024/PSA240903