Binance: fake job interview led to $6.34 billion crypto theft



Binance's incident report says North Korean attackers used a fake recruiter and a malicious coding task to reach its wallet infrastructure and steal about $6.34 billion. The case shows how hiring-themed social engineering can reach critical systems.

- The attack began in September, when a software engineer was approached through a legitimate job platform by someone posing as a project director.
- A coding assignment from an online repository installed previously unseen malware that endpoint tools did not detect.
- By October 20 the attackers had used the engineer's device and an internal AI tool to compromise two more employees and obtain credentials and a container deployment token.
- On October 29 they accessed the wallet signing service; abuse of Ethereum's EIP-7702 let theft

> continue after withdrawals were suspended.
>
> - About $2.85 billion was frozen or intercepted, and 98% of impacted token assets had been replenished by October 31.

Binance has published an incident report explaining how the theft of about $6.34 billion in digital assets on October 29 began with a fake job interview. The FBI has attributed the attack to the North Korean group known as TraderTraitor, also tracked as Lazarus Group, Jade Sleet and APT38.

How the attack unfolded

In September, a software engineer was contacted on a legitimate job-hunting platform by someone posing as a project director at a fictitious company. His profile mentioned Binance. He then went through two interviews: a video call with a supposed HR representative, and a chat-based interview with a supposed CEO, who told him to download a coding assignment from an online repository.

The code installed custom malware that, according to Binance, endpoint security tools did not detect. On macOS it replaced a legitimate development tool component with a malicious one that took commands from an attacker-controlled server, and the attackers worked to hide their traces.

By October 20 they had used the engineer's computer and an internal AI tool to compromise two employees working on wallet infrastructure, obtaining credentials and a container deployment token. On October 29 these were used to deploy a malicious script and reach the wallet signing service.

Response and context

Binance says it has rebuilt affected systems, replaced compromised devices and revoked stolen credentials. Independent security firms are reviewing its findings. The tactic resembles previously documented North Korean campaigns such as Contagious Interview and Operation Dream Job, although Binance has not linked this case to either.

What to do now

1. Brief developers, engineers and staff in privileged roles on fake-recruiter approaches, and require that coding tests from outside parties run only in isolated sandboxes, never on corporate devices.
2. Restrict personal chat apps and code repository downloads on devices with access to production or signing systems.
3. Review endpoint detection coverage on macOS and developer machines, including alerts on replaced or altered tool binaries.
4. Limit and monitor access to container deployment tokens and signing services, and rotate credentials quickly when a device is suspected.

5. Assess what internal AI tools can reach, and segregate duties and approvals around high-value transaction systems.
6. Add a fake-recruitment compromise scenario to incident response exercises.