+44 345 094 0945
www.waterstons.com

Article

Sep 2024

Security Firms Hires North Korean Hacker

The security engineer a security firm recently hired within its internal AI team turned out to be a North Korean threat actor, who immediately began loading malware to his company-issued workstation.

The security engineer a security firm recently hired within its internal AI team turned out to be a North Korean threat actor, who immediately began loading malware to his company-issued workstation.

What Happened?

KnowBe4 recently encountered a sophisticated social engineering attack, despite thorough pre-hiring background checks and multiple interviews. The company discovered that the hired candidate, referred to as 'XXXX', was actually using a stolen identity enhanced with AI. Upon receiving his workstation, XXXX immediately loaded malware onto it.

Suspicious activities were detected by KnowBe4's Security Operations Centre (SOC) shortly after the workstation was activated. XXXX initially claimed these activities were related to troubleshooting his router, however, he was actually manipulating session history files, transferring harmful files, and executing unauthorised software via a Raspberry Pi. When contacted by SOC for further investigation, XXXX became unresponsive, prompting the SOC to quarantine his device. KnowBe4 collaborated with the FBI, uncovering that XXXX was a North Korean operative. No data breach occurred as security measures blocked the malware. The incident served as a significant learning moment for KnowBe4, which emphasised that new hires only have limited access during onboarding, preventing XXXX from accessing sensitive data or systems.

Wider Implications

This incident is part of a broader, and increasingly sophisticated, cyber-espionage campaign driven by state-sponsored actors, particularly from North Korea. This specific attack fits within a larger context of global cyber threats where adversarial nations exploit vulnerabilities in remote work practices to infiltrate organisations

The rise of remote working has created new attack surfaces for cyber threats with remote positions, especially those that allow employees to work from different geographic locations, present a unique challenge for verifying identities and ensuring security.

Organisations Should:

- Whenever possible, require at least one interview to be conducted in person. This helps ensure the candidate's identity and prevents the use of AI-generated imagery or deepfakes.

- Place new employees in restricted environments initially, with limited access to critical systems and data. Gradually increase access as they prove their legitimacy and reliability.

- Train HR and hiring managers to recognise red flags, such as inconsistencies in resumes, discrepancies in interview answers, or unusual requests related to work logistics (e.g., unusual shipping addresses for equipment).

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