#ForensicPerspectives

Heightened cybersecurity risks posed by North Korean IT workers impersonating non-DPRK Nationals

Based on our experience in recent client matters, we have seen an escalating threat posed by the Democratic People's Republic of Korea (DPRK) information technology (IT) workers engaging in sophisticated schemes to evade US and UN sanctions, steal intellectual property from US companies, and/or inject ransomware into company IT environments, in support of enhancing North Korea's illicit weapons program.

What information should you know?

In general, the scheme involves the use of deceptive tactics, including stolen identities and remote access technology tools, to secure IT employee or contractor positions within US-based employers. The allure of high pay for these roles, coupled with a comparatively low risk of detection, makes this scheme particularly enticing for DPRK operatives.

The US Department of Justice announced in a recent court-approved seizure action:[1]

> *As alleged in court documents, the Government of the Democratic People's Republic of Korea (DPRK) dispatched thousands of skilled IT workers to live abroad, primarily in China and Russia, with the aim of deceiving U.S. and other businesses worldwide into hiring them as freelance IT workers, in order to generate revenue for its weapons of mass destruction (WMD) programs. Through this scheme, which involves the use of pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers located in the United States and elsewhere, and witting and unwitting third parties, the IT workers generated millions of dollars a year on behalf of designated entities, such as the North Korean Ministry of Defense and others, directly involved in the DPRK's UN-prohibited WMD programs.*

What can you do with this information?

We recommend that companies mitigate this risk by using a risk-based approach to:

- conduct enhanced due diligence on employee/contractor candidates.
- strengthen ongoing monitoring capabilities of employees/contractors.
- bolster defenses against the inappropriate exfiltration of valuable information.
- reduce the risk of remote access tools being launched in ways that could circumvent the typical requirement for admin privileges.
- prepare to better respond to ransomware and other cyber incident response situations.

We invite you to reach out to continue the conversation on how to most effectively detect, prevent, and correct this or other types of fraud, cybercrime, misconduct, and non-compliance.

[1] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation

Patricia Peláez, CPA/CFF, CFE, CPC, CAMS, CMS
Principal, Forensic Services
+1-312-577-4180 | ppelaez@crai.com