The New American

Author: Luis Miguel

Date: December 22, 2023

Stockbyte/iStock/Getty Images Plus

White House Says Crackdown on Hackers Key to Combating North Korea

The federal government is going after North Korea’s cryptocurrency amid fears of the threat Pyongyang’s nuclear weapons program poses to the United States.

The White House asserts that the regime of Kim Jong Un is stealing cryptocurrency through cyberattacks and using this money to fund its nuclear arsenal development. As a result, the Biden administration is taking measures to stop North Korea’s digital money-laundering operations, per *Politico*.

Over the last year, the government has cracked down on North Korean hacking organizations, IT workers, and front companies with strict sanctions, and blacklisted the crypto services Pyongyang reportedly uses to launder the money it allegedly steals.

Just this month, national security adviser Jake Sullivan unveiled a new partnership with Japan and South Korea intended to strike at North Korea's cryptocurrency stash.

Anne Neuberger, the top cybersecurity official with the National Security Council, told *Politico* that "In countering North Korean cyber operations, our first priority has been focusing on their crypto heists." She also said the new focus on North Korea's cyber capabilities is the product of concern that the Kim regime is using these efforts to keep its nuclear program running.

According to Neuberger, hacking has made it possible for North Korea to "either evade sanctions or evade the steps the international community has taken to target their weapons proliferation … their missile regime, and the growth in the number of launches we've seen."

North Korea's hackers are reportedly more adept than laymen would think possible for a country known as the "Hermit Kingdom." The country's hackers, which often target startups (which tend to be more vulnerable than larger corporations), catch their victims off guard, pulling off major cryptocurrency heists.

These attacks rarely get much attention because they seem to not affect anyone in the public, only the specific firms targeted. However, the implications of these attacks are far-reaching, as government sources claim Pyongyang is using the funds obtained from the hacking to pay for weapons programs.

And experts say North Korea's hackers could use the techniques they've utilized in hacking crypto firms to cause widespread disruption. As *Politico* notes:

> In April, researchers at cybersecurity firm Mandiant uncovered that North Korean hackers had pulled off the first publicly known instance of a "double" software supply-chain hack — jumping from one software maker into a second and from there to the company's customers.
>
> Mandiant assessed the hackers were after cryptocurrency. Had they wanted to, however, the North Koreans could have used tactics like that to inflict "a massive level of damage," said SentinelOne's [Tom] Hegel.
>
> What North Korea "is able to do on a global scale, no one has replicated," added Mick Baccio, global security adviser at security firm Splunk.

The proficiency of North Korean hackers was made apparent in 2014, when operatives of the Kim regime hacked into Sony's film division and threatened the studio against releasing the film *The Interview*, which lampoons Kim and portrays his fictional assassination. Then, in 2017, Pyongyang was blamed for releasing a self-spreading computer virus that reportedly was responsible for billions of dollars in property damage in a mere matter of hours.

U.S. officials say the rapidly increasing rate of North Korean hacking attacks is motive for worry. Per Washington, Pyongyang is targeting think tanks and academics in an attempt to obtain intelligence, as well as launching ransomware attacks in which they scramble the data of victims unless they agree to pay an extortion sum. American healthcare companies have been subject to these kinds of attacks.

Organizations such as the FBI, Justice Department, and Treasury Department say North Korea has deployed thousands of tech workers to China and Russia, where they use false identities to obtain remote IT jobs and then send their earnings back home — thereby funding the Kim regime.

"It shows that they're always thinking outside the box, evolving and keeping up with the news in the same way we do, which is a little bit scary," said Erin Plante, who serves as vice president of investigations at the New

York-based blockchain analysis firm Chainalysis.

North Korea has made further waves in recent days with reports that its second nuclear reactor appears to be operational. And Kim this week said a new intercontinental ballistic missile (ICBM) test shows his country has the capability to launch a nuclear attack if his enemies provoke him.

While the United States and its allies blasted North Korea for this test, Russia spoke out in favor of Pyongyang. As The Associated Press reports:

> Russia’s deputy U.N. ambassador Anna Evstigneeva called attempts to condemn Pyongyang “a one-sided approach.”
>
> She warned that the situation is escalating “to a dangerous brink,” pointing to both Pyongyang and Seoul justifying their hostile moves as self-defense. And she accused the United States of deploying its massive military machine in the region, saying this looks “more and more like preparations for an offensive operation,” even though the U.S. says it has no hostile intentions.

Between North Korea’s nuclear capabilities and the support it has from Moscow and Beijing, the United States’ ability to cajole Pyongyang is minimal, calling for an approach that is less saber-rattling and more cerebral when it comes to dealing with the “Hermit Kingdom.”