**North Korean Hackers have stolen over $3,000,000,000 to fund their military (nuclear) programs.**

It is hard to believe that hackers from North Korea have been successful in pilfering more than several billion dollars to fund North Korean priority projects, including their nuclear programs.

One of their most successful hacks involved Sky Mavis, an engineer blockchain gaming company Sky Mavis thought he was on the cusp of a new job that would pay more money.

A recruiter had reached out to him via LinkedIn, and after the two spoke over the phone, the recruiter gave the engineer a document to review as part of the interview process. But the recruiter was part of a vast North Korean operation aimed at bringing in funds to the cash-poor dictatorship. And the document was a Trojan horse, malicious computer code that gave the North Koreans access to the engineer’s computer and allowed hackers to break into Sky Mavis. Ultimately they stole more than $600 million— mostly from players of Sky Mavis’s digital pets game, Axie Infinity.

**==============================================**

**SOURCE:**

***The Wall Street Journal* | Page A006, Monday, 12 June 2023**

**Digital Heists Fund North Korea Missiles**

**Cybercriminals have netted more than $3 billion in crypto for nuclear program**

BY **ROBERT** MCMILLAN AND DUSTIN VOLZ

**Last year an engineer working for the** **blockchain gaming company Sky Mavis thought he was on the cusp of a new job that would pay more money.**

**A recruiter had reached out to him via LinkedIn, and after the two spoke over the phone, the recruiter gave the engineer a document to review as part of the interview process. But the recruiter was part of a vast North Korean operation aimed at bringing in funds to the cash-poor dictatorship. And the document was a Trojan horse, malicious computer code that gave the North Koreans access to the engineer’s computer and allowed hackers to break into Sky Mavis. Ultimately they stole more than $600 million— mostly from players of Sky Mavis’s digital pets game, Axie Infinity.**

**It was the country’s biggest haul in five years of digital heists that have netted more than $3 billion for the North Koreans, according to block-chain analytics firm Chainalysis. That money is being used to fund about 50% of North Korea’s ballistic missile program, U.S. officials say, which has been developed in tandem with its nuclear weapons. Defense accounts for an enormous portion of North Korea’s overall spending; the State Department estimated in 2019 Pyongyang spent about $4 billion on defense, accounting for 26% of its overall economy.**

**Although Sky Mavis has now repaid victims of the cyberattack, the incident threatened the very existence of the then-four-year-old company, said Aleksander Larsen, the firm’s chief operating officer.**

**“When you look at the amount of funds stolen, [it] would look like an existential threat to what you are building.”**

**The incident also caught the attention of the White House, where it and other North Korean crypto attacks throughout 2022 have raised grave concerns. “The real surge in the last year has been against central crypto infrastructure around the world that hold large sums, like Sky Mavis, leading to more large-scale heists,” said Anne Neuberger, President Biden’s deputy national security adviser for cyber and emerging technology. “That has driven us to intensely focus on countering this activity.”**

**North Korea’s digital thieves began hitting their first big crypto attacks around 2018. Since then, North Korea’s missile launch attempts and successes have mushroomed, with more than 42 successes observed in 2022, according to data tracked by the James Martin Center for Nonproliferation Studies.**

**U.S. officials cautioned that so much is unknown about the nation’s sources of funds amid Western sanctions that it isn’t possible to have a precise understanding of the role crypto theft is playing in the increased rate of missile tests. But the test buildup by Kim Jong Un’s reclusive regime has occurred at the same time as a concerning upswing in crypto heists.**

**Roughly 50% of North Korea’s foreign currency funding for purchasing foreign components for its ballistic missile program is now supplied by the regime’s cyber operations, Neuberger said. That is a sharp increase from earlier estimates, which had put the figure at a third of overall funding for the programs.**

**U.S. officials say North Korea has built what is essentially a shadow workforce of thousands of IT workers operating out of countries around the world, including Russia and China, who make money— sometimes more than $300,000 a year—doing mundane technology work. But this workforce is often linked up with the regime’s cybercrime operations, investigators say.**

**They have pretended to be Canadian IT workers, government officials and freelance Japanese blockchain developers. They will conduct video interviews to get a job, or, as with the Sky Mavis example, masquerade as potential employers.**

**To get hired by crypto companies, they will hire Western “front people”—essentially actors who sit through job interviews to obscure the fact that North Koreans are the ones actually being hired. Once hired, they will sometimes make small changes to products that allow them to be hacked, former victims and investigators say.**

**Starting two years ago, hackers linked to North Korea began infecting U.S. hospitals with ransomware—a kind of cyberattack where hackers lock up a victim company’s files and demand payment for their release—to raise money, U.S. officials say.**

**“It seems like a modern-day pirate state,” said Nick Carlsen, a former FBI analyst who works for blockchain tracing firm TRM Labs. “They’re just out there raiding.”**

**Carlsen and others in the cryptocurrency industry say that weeding out these fake IT workers is a constant problem.**

**International experts have long said that North Korea has been developing a digital bank-robbing army to evade harsh sanctions and support its ambitions to project geopolitical power through nuclear weapons and ballistic missiles. A 2020 United Nations report found that the regime’s revenue- generating hacking has proven to be “low-risk, high-reward and difficult to detect, and their increasing sophistication can frustrate attribution.”**

**For years the U.S. and other Western governments blamed North Korea for a string of brazen—and sometimes haphazardly executed—cyberattacks, ranging from the 2014 hack of Sony Pictures to a massive global ransomware attack in 2017. But the country has increasingly sought to focus its cyberattacks on generating cash, while dramatically improving its technical sophistication to pull off large-scale thefts, according to U.S. officials and security experts. “Most nation-state cyber programs are focused on espionage or attack capabilities for traditional geopolitical purposes,” the White House’s Neuberger said. “The North Koreans are focused on theft, on hard currency to get around the rigor of international sanctions.”**

**In 2016, hackers linked to North Korea stole $81 million from the central bank of Bangladesh, part of an attempted $1 billion cyberheist that was disrupted by the Federal Reserve Bank of New York.**

**The North Koreans also have stolen money from ATMs and even made more than $100,000 in cryptocurrency from a quickly spreading worm called WannaCry, but nothing has been as lucrative as their string of crypto heists, which began in earnest in 2018, according to Erin Plante, the vice president of investigations with Chainalysis. “They were really early into crypto, and they were some of the most advanced users of crypto ear**ly on.”