Elite N.Korean hacker group tied to bank attacks: researchers

October 3 2018

Security researchers say an elite group of North Korean hackers has stolen hundreds of millions of dollars from banks worldwide

An elite group of North Korean hackers has been identified as the source of a wave of cyberattacks on global banks that has netted "hundreds of

millions" of dollars, security researchers said Wednesday.

A report by the cybersecurity firm FireEye said the newly identified group dubbed APT38 is distinct from but linked to other North Korean hacking operations, and has the mission of raising funds for the isolated Pyongyang regime.

FireEye researchers said APT38 is one of several hacking cells within an umbrella group known as "Lazarus," but with unique skills and tools that have helped it carry out some of the world's largest cyber heists.

"They are a cybercriminal group with the skills of a cyberespionage campaign," said Sandra Joyce, FireEye's vice president of intelligence, in a briefing with journalists in Washington.

Joyce said one of the characteristics of APT38 is that it takes several months, sometimes nearly two years, to penetrate and learn the workings of its targets before its attacks, which have sought to illegally transfer more than $1 billion from victimized banks.

"They take their time to learn the intricacies of the organization," Joyce said.

Once they succeed, she added, "they deploy destructive malware on their way out" to hide their traces and make it more difficult for victims to find out what happened.

Sense of urgency

Joyce said FireEye decided to go public about the threat out of a "sense of urgency" because the group appears to still be operating and is "undeterred by any diplomatic efforts."

The group has compromised more than 16 organizations in at least 11 different countries since at least 2014, according to the FireEye report.

Some of the known attacks have targeted the Vietnam TP Bank in 2015, Bangladesh Bank in 2016, Far Eastern International Bank of Taiwan in 2017 and Bancomext of Mexico and Banco de Chile in 2018.

Joyce said the group appears to have "the scope and resources of a nation-state" but offered no specific figures on how many people it uses.

Researchers said that North Korean national Park Jin Hyok, who was named in a US criminal complaint last month unveiled by Justice Department officials at a news conference pictured here, was peripherally involved in an elite bank

Nalani Fraser, a member of the FireEye research team, said APT38 attacks sought at least $1.1 billion since 2014 and have managed to steal "hundreds of millions of dollars based on data that we can confirm."

FireEye said there appears to be some sharing of resources between hacker groups in North Korea, including those involved in espionage and those in other kinds of attacks.

Focused mission

Some of the information about APT38 was revealed in a US criminal complaint unsealed last month against Park Jin Hyok, charged in connection with WannaCry ransomware outbreak and the attack on Sony Pictures.

But Park likely played only a peripheral role in APT38,which "has a focused mission to steal money to fund the North Korean regime," according to Joyce.

FireEye's new report was based in part on forensic analysis it conducted for the FBI in the investigation into Park, but also from other data the security firm has gathered from its global client base.

The researchers said APT38 used techniques including "phishing" emails to gain access to credentials and using "watering holes"—hijacked websites that appear normal but which contain malware that enable hackers to gather more data and access.

As part of the scheme, the hackers created fake identities within known

nongovernmental organizations or foundations to help move the stolen money, in some cases manipulating the global interbank transfer system known as SWIFT.

The report is the latest highlighting a vast and increasingly sophisticated cyber campaign by North Korea for both political and financial ends.

In September, a 176-page criminal complaint against Park outlined what officials called "a vast and audacious scheme by the North Korean government to utilize computer intrusions as a means to support the varied goals of their regime."

On Tuesday, the US Department of Homeland Security warned that North Korea is likely behind malware used to hack into and steal money from bank teller machines.

The bulletin said officials believe the "Hidden Cobra" malware enabled North Korea to illegally get cash from bank machines in at least 30 countries, mainly in Asia and Africa, since 2016.