On October 15, 2021, the Korean National Police Agency (KNPA) reported that four members of an unnamed money laundering organization, including its leader, were detained in a joint investigation that involved Ukrainian police, the United States Federal Bureau of Investigation, and Interpol.

Three Ukrainians and another foreigner are accused of distributing the Clop ransomware that paralyzed some 720 computer systems containing academic and business data and extorted a 65 bitcoin ransom of 4.5 billion won ($3.8 million). Two of them will soon be extradited to South Korea.

They were key members of an international criminal organization suspected of carrying out massive ransomware hacking attacks on South Korean companies and universities in February 2019.

The National Police Agency of South Korea’s cyberterrorism unit opened an investigation immediately after committing the crime. The police agency analyzed Clop, attack tools, and methods of intruding into a computer network. They shared tracking information with the intelligence services of 20 countries, and it turned out that virtual assets extorted by the suspects were converted into cash on foreign exchanges. After conducting a joint operation and identifying the criminals, the KNPA requested Interpol to apprehend the hackers and their accomplices, which was done.

These links are no longer available, but the author clearly remembers how this attack was actively put into the
framework of the intrigues of Pyongyang hackers two years ago. The same hackers were accused of racketeering to allegedly provide currency to the country’s nuclear program and buy luxury goods for the Kim family while the people starved.

Meanwhile, when the author first learned that the malware used to paralyze computer systems by changing the extensions of their files, and then to use it as blackmail to demand payment with cryptocurrency, was called Clop, he immediately noted that to the Russian ear, this sounds quite specifically, meaning the corresponding parasitic insect.

In general, the cybersecurity situation in South Korea is of interest to the authorities. For example, on December 16, 2020, the Blue House reviewed South Korea’s position on cybersecurity during a high-level interagency meeting. Blue House National Security Officer Director Suh Hoon noted that amid the proliferation of non-contact activities such as online classes and working from home, the importance of cybersecurity has increased, especially when it comes to the use of ransomware.

On June 5, 2021, the Yonhap News Agency reports that ransomware attacks increased in South Korea in 2020 as the coronavirus pandemic increased online activity.

The number of ransomware attack reports here stood at 127 last year, more than tripling from 39 in 2019, according to the Ministry of Science and ICT. Seventy-eight cases were reported in the first half of this year.

The ransomware attacks were directed at various businesses. For example, in May 2021, the operations of food delivery company Super Hero was paralyzed for hours after an attack that affected 15,000 delivery workers across the country. In November 2020, local fashion and retail giant E-Land Group was hacked, forcing 23 of the department store’s 50 branches to cease operations.

As Seungjoo Kim, Professor of School of Cybersecurity, states, a vicious circle is forming. During a pandemic, companies rely more and more on remote work, and ransomware attacks become a more significant threat because they can damage the entire work system. Accordingly, more companies pay the ransom, encouraging more ransomware attacks.

As a result, the ministry created a 24/7 monitoring team to support companies targeted by attacks and conducted a two-week cybersecurity exercise for 230 companies.

On August 4, the Ministry of Science and Information and Communications Technology raised its cyberthreat alert level by one notch by stepping up monitoring malware and other cyber threats and strengthening response measures. The ministry said the decision was taken as a preventive response to the ransomware threat after intelligence agencies uncovered hacking attacks upon major local hospitals prior to mass vaccination plans.

As part of strengthening cybersecurity cooperation, the US National Security Council said on its Twitter page, the meeting took place, and participants agreed to extend the power of the bilateral alliance to combat cybercrime. The working group was established in line with an agreement reached in May by Presidents Moon Jae-in and Joe Biden to strengthen the partnership in countering global cyber threats.

In addition, the Ministry of Science and ICT said it would strengthen support to small businesses that have weaker cybersecurity systems by offering them data back-up, encryption and restoration systems to protect their internal data in order to help restore their systems in ransomware attacks.

International cooperation is also developing. On August 5, South Korea and the USA agreed to strengthen cooperation in responding to global cyber threats. The parties agreed to work on joint measures to counter them and cooperate in developing various information-sharing systems. And on September 10, South Korea and the USA held their first meeting of the joint working group in combating ransomware. The detention of Ukrainian hackers on their own territory is one of the consequences of this project.

They did not attempt to associate North Korea with a series of high-profile scandals in South Korea in the spring and summer of 2021 with hackers from the North, and the author hopes that after such an incident, the “Pyongyang trail” will not be searched anywhere. Let’s also see if this hacker group turns out to be involved in other cybercrimes and if the author's hunch is confirmed that turning the tables on North Korea is a common trick among hackers when a completely different region is confirmed.

Konstantin Asmolov, PhD in History, leading research fellow at the Center for Korean Studies of the Institute of the Far East at the Russian Academy of Sciences, exclusively for the online magazine “New
Eastern Outlook."