There is a lot of writing about North Korean hackers, and every six months or a year the author makes a kind of summary, pointing out how the stories about the Pyongyang trail have become a self-replicating myth, and the expression “Hackers believed to be linked to North Korea” - a proof. Moreover, spring-summer 2021 turned out to be rich in high-profile events in this area.

But let us go in order. On October 27, 2020, the US issued a warning against “the well-known North Korean hacker group Kimsuky, which was accused of hacking into Sony Pictures in 2014.” As it turns out, this is no less serious team than the notorious Lazarus. The problem is that to the Russian ear a group of hackers called “Kimsuky” sounds like an English translation of “Kim’s bitches”, which rather gives rise to suspicions of a completely non-Pyongyang trace.

However, on the one hand, the author still treats North Korean hackers with a fair amount of skepticism, yet on the other hand, one should not go too far in the opposite direction. It should be understood that a sufficient number of the North Korean elite are actively using the Internet. As Priscilla Moriuchi, a professor at the Harvard School of Government and senior fellow at the American cybersecurity company Recorded Future, noted in an interview with Der Spiegel on February 22, 2021, an analysis of North Korean Internet traffic in 2017 showed that over the past three years, the volume of its use has more than tripled.

In addition, the Kim Jong-un Military University has been established in North Korea, where military-technical specialists are trained, and the South Korean media were replete with suggestions that there was a hacker faculty there as well.

However, let us go back to the “kimsuky”. In April 2020, IBM identified hacker attempts to break into the websites of
major COVID-19 vaccine suppliers. In a statement released by the IBM website, it was said that back in September, a
group of hackers sent false emails on behalf of the Chinese supplier of vaccines to organizations associated with the
process of their distribution, including in Germany, Italy, South Korea, Czech Republic and Taiwan.

In November 2020, Kimsuky tried to hack into several international organizations, including companies that were
working on covid vaccines. The reason to suspect Pyongyang was that “the malware and infrastructure have similar
functions and were associated with the same IP address as other malware used by Kimsuky in the past”, although
the hackers weren’t limited to South Korea but also targeted the US, Europe, Russia and Japan.

On November 13, 2020, Microsoft discovered attacks against companies and research institutes that were
developing a vaccine against coronavirus Tom Burt, vice president of customer safety and trust, said the victims
were “leading pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea and the
United States.” One attack was allegedly from Russia and two from the DPRK. According to Reuters and CNN, North
Koreans posed as recruiters and offered jobs to employees of companies, including AstraZeneca.

On December 3, 2020, The Chosun Ilbo reported that in September 2020, North Korean hackers impersonated
recruiters on LinkedIn and WhatsApp, and created fake websites that resemble login portals used by drug
developers to force people to enter their registrations, numbers and also passwords by mistake.

As Vice reported citing Google, Pyongyang hackers developed a new social engineering technique and used it
against cybersecurity researchers by forcing them to visit the infected Exploit Investigator Blog website. This blog
allegedly discussed and analyzed already known vulnerabilities, as well as disseminated information about new, not
yet explored cybersecurity vulnerabilities. The attackers used fake Twitter and LinkedIn accounts to contact the
victims and offer them access to the resource.

In February 2021, the Korea Times reported that in 2019-2020, the DPRK stole cryptocurrencies worth
approximately $ 316.4 million. One is only left to wonder how all this can be cashed and put into motion inside North
Korea.

On February 16, Ha Tae-keung, a member of the parliamentary intelligence committee of the Republic of Korea, said
that since the beginning of the year, 1 million 580 thousand cyber attacks have been committed against the Republic
of Korea (an increase of 32% compared to last year), most of which were from the North. This was mentioned in the
report of the National Intelligence Service, but then there was a curious embarrassment. Ha stated that Pfizer was
also attacked by North Korean hackers, citing intelligence documents and other sources, which he refused to clarify,
but the intelligence services “did not confirm” this fact.

On February 17, the US Department of Justice indicted three North Korean programmers for cyberattacks, who stole
$ 1.3 billion, including in cryptocurrency. According to the ministry, 36-year-old Park Jin Hyok, 31-year-old Jong
Chan Hyuk and 27-year-old Kim Il belonged to the DPRK military intelligence.

If you collect all the charges, then Park Jin Hyok is an analogue of the ubiquitous Russian spies Petrov and Boshirov.
He hacked Sony Pictures, created WannaCry and stole 81 million from the Central Bank of Bangladesh, while still
under 30 years of age. He allegedly robbed digital currency exchanges in Slovenia and Indonesia and extorted $ 11.8
million from the New York exchange. In 2018, he stole $ 6.1 million from the ATMs of Pakistani Islami Bank after
gaining access to its computer network. He also reportedly took an active part in hacking foreign financial
institutions, including Vietnamese, and cashing in virtual currency.

Still, it is not very clear how much of this money eventually reached the North, since the final charge was brought
against 37-year-old Canadian resident Caleb Alumari, who, according to the investigation, laundered money for the
North Koreans. So it cannot be ruled out that the detainee, who laundered money for other hackers who were
engaged in phishing, bank thefts, etc., simply shifted the responsibility to the representatives of North Korea.

In April 2021, NK News reported that North Korean experts are competing in various online programming
competitions to hone their cyber skills. However, cybersecurity experts said that this is not worrying because the
participation of North Korean programmers in coding competitions, on the contrary, can reveal their habits, which
can be used to link future attacks with the DPRK.

Another NK News story from the same month reported North Koreans posing as a cybersecurity firm, and the Google
Threat Analysis Group (TAG) discovered links between North Korean hackers and a website allegedly owned by a
Turkish cybersecurity company called SecuriElite.
Syngia researchers suspected a collaboration between the North Korean group Lazarus and the criminals behind the TFlower extortion campaign. According to them, a new variant of the MATA malware that was previously associated with Lazarus was used to install the ransomware TFlower.

And as reported by the company Group-IB, Lazarus representatives used a new type of malicious JavaScript to steal digital money from online retailers. The hackers injected this code into the websites of online stores, some of which were already infected with the so-called skimming malware that steals credit card information from customers.

On April 7, it even became known that supposedly North Korean hackers posed as journalists of NK News. The South Korean firm ESTsecurity told them that a “group suspected of operating on behalf of the DPRK” created a Facebook profile claiming it was owned by a “NK News journalist” named Vincent Jean. An NK News investigation found two twitter accounts with the same name and photo.

On April 8, 2021 British portal Raiders of Crypto put a virtual laurel wreath on North Korean hackers. It turns out that five of the 10 largest cybercrimes in the financial sector over the past decade were carried out by “hackers associated with the DPRK,” and of 102 cyber attacks, 30 are related to Pyongyang, although the real numbers are even higher, since the perpetrators of 64 attacks could not be identified. According to the portal, hackers associated with the DPRK stole more than $534 million from the Japanese cryptocurrency exchange Coincheck in 2018. In the same year, a cyberattack was carried out on the Central Bank of Malaysia. North Korean hackers were involved in the theft of $170 million from Union Bank of India in 2016, in the hacking of the system of the Export-Import Bank of Mexico in 2018 and the Bank of Nigeria in 2016.

Researchers from NKNews speculate that Kimsuky’s phishing attempts have followed a predictable pattern against certain US organizations for weeks after new sanctions or existing ones were introduced, the RAND Corporation said in a report earlier this month. The researchers said they analyzed phishing attacks against RAND attributed to Kimsuky over two years and found a high correlation between sanctioning activity and attempts to trick RAND employees into clicking malicious links.

On April 19, 2021, a researcher at the South Korean Institute for National Security Strategy Oh Il-Seok said that amid economic problems (trade with China has decreased due to the COVID-19 pandemic, and US and UN sanctions are tightened), cyber attacks on financial institutions and think tanks in South Korea, the United States and other countries of the North will continue. The expert also warned that the North could launch cyberattacks on the South Korean government and American think tanks related to nuclear negotiations, as well as other experts on North Korea.

However, in the event of a massive cyberattack from the North, the United States can view them as “serious threats” and take more aggressive retaliatory measures, such as introducing economic sanctions and even delivering a physical strike using UAVs to targets from which cyberattacks originate. However, given most of the horror stories, does this mean that drones will attack China or the Russian Federation?

But the real scandal erupted in South Korea after the leadership of the Korea Atomic Energy Institute (KAERI) informed the Ministry of Science and Information and Communications Technology and the main cybersecurity center under the National Intelligence Service on June 1 that the internal computer network from 14 to 31 May has been repeatedly subjected to cyberattacks. The experts updated the security system and blocked 13 IP addresses of the attackers. At the same time, the institute refused to comment on reports that cyberattacks were carried out from the territory of North Korea, as well as to assess the damage. Apparently, because they remembered that it was possible to connect to a network completely isolated from the outside world not with the help of special hacker magic, but through an insider.

However, on June 18, 2021, Ha Tae-keung stated that the network was hacked as a result of a North Korean cyber attack. It turns out that “some IP addresses were traced back to the hacking of the servers of Kimsuky, a North Korean cyber espionage group.” What’s more, some of the IP addresses were recovered using the email of President Moon Jae-in’s former special adviser for foreign policy, Moon Jong-in, who was either a victim of phishing or pandering to hackers.

Of course, later on, Ha and other representatives of the conservative “Power of the People” launched a campaign of rumors that the damage was actually much greater, but the administration of Moon Jae-In simply did not dare to admit the fact of the cyberattack and the scale of its real success.

On June 25, 2021, cybersecurity firm ESTsecurity reported that “North Korean-related hackers” such as Thallium and
Kimsuky are suspected of conducting cyberattacks using South Korean government email addresses, including the Korea National Unification Institute.

And on June 30, a “flight scandal” was added to the “nuclear scandal” - it turned out that the KAERI hack followed similar cyberattacks on Korea Aerospace Industries (KAI) and Daewoo Shipbuilding and Marine Engineering (DSME). According to Ha Tae-keung, they were attacked with a VPN system vulnerability.

In the first case, the target was apparently confidential data on large projects, including drawings of the prototype of the KF-21 fighters; in the second - the development of the latest submarines, blueprints for nuclear reactors and accompanying SLBMs: just when the North Koreans themselves are about to launch a submarine capable of carrying ballistic missiles.

Of course, “some of the cyber attacks have been traced back to the Kimsuky.” The real effect of the attack is not known, but, according to conservative newspapers, it seems that they should have stolen everything they needed: after all, North Korean hackers leave no traces other than those that indicate their involvement in Pyongyang. According to Ha and another committee member, Kim Ben Gi, the damage done to the country by hacker groups rose 9 percent in the first half compared to the second half of last year.

Amid reports of cyberattacks on July 7, the Ministry of Unification disclosed attempts to hack its information infrastructure.

Since 2016, the department has noted an upward trend in the number of hacker attacks, as evidenced by the cited figures - 260 (2016), 336 (2017), 630 (2018), 767 (2019). Last year, 633 hacking attempts were recorded. Among them, 310 were for attempts to collect system information, 265 for attacks by hacking e-mail, 46 were attempts to hack through a website, 8 incidents with access to malicious IP addresses, and 4 detections of malicious code.

Conservatives in this context recall the recent attack on the US fuel infrastructure and argue that the country still does not have a national cyber warfare strategy or related legislation. The national cyber strategy developed by the government in 2019 is more about cybersecurity than defense. There is no secretary to the president in charge of cybersecurity, and the role and functions of the NSA have long been outdated.

In recap. Such stories, of course, are of interest to cybersecurity experts, but you can note that in almost all cases, concrete evidence of the North Korean trail leaves much to be desired. For details, the author refers to the methodological section of his research on North Korean hackers, the conclusions of which have not yet lost their relevance.

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”. 