Self-Exposure of the Myth of North Korean Hackers

More recently NEO wrote that the termination of the DPRK moratorium and a potentially new round of tension could have been caused by a series of hacker attacks on the North Korean Internet in the second half of January 2022, since fortunately back in 2018, the United States stated that the first shot of this war would be fired in cyberspace.

Yes, it was not possible to collapse the entire Internet for a long time. The maximum that a hacker or hackers managed was to temporarily “crash” most of the sites for about six hours, but for the North Koreans it was a series of attempts to disable the Internet of the whole country or at least key sites, of which there are not so many, that was important. At least one of the central routers providing access to the country’s networks turned out to be paralyzed at some point, which disrupted the North’s digital connections with the outside world.

After that, the North Koreans began to act accordingly, but it is worth talking more about how, in this delicate situation, the DPRK enemies are trying to turn it around and how in the meanwhile they inadvertently exposed the myth they invented about Pyongyang hackers.
Firstly, out of nowhere (NEO did not find any links about the activities of this person earlier and out of connection with this incident), a hacker nicknamed P4x appeared, while claiming in an interview with WIRED that it was he who collapsed the North Korean Internet allegedly as revenge for trying to hack it.

According to an anonymous but talkative hacker, a little over a year ago he was hacked by North Korean spies as one of the victims of a campaign that targeted Western security researchers with the obvious goal of stealing their hacking tools and detailed information about software vulnerabilities. However, when trying to clarify the details, it turned out that the hack looked like this. At the end of January 2021, he opened a file sent to him by a fellow hacker. 24 hours later, he discovered a blog post from Google’s Threat Analysis Group warning that North Korean hackers had targeted security researchers. Indeed, when P4x carefully examined the hacking tool he received from a stranger, he saw that it contained a backdoor designed to provide remote access to his computer. As can be noted, there is no evidence that he was hacked from the DPRK, even at the level of “the attack came from a North Korean address” or “it was a signature line of.” P4x read that malicious North Koreans are hacking hackers, and since he is a hacked hacker, the threat is surely from Pyongyang. Truly, a genius of logic!

Later, the FBI contacted the hacker, “but he was never offered any real help to assess the damage from hacking North Korea or to protect himself in the future.” After a year of waiting, he never saw “the government’s reaction to North Korea’s attacks on American citizens” and did not hear “about any consequences for the hackers who targeted him, about an open investigation of their activities, or even about an official recognition that North Korea is responsible.” It is interesting here that a professional hacker contacts the FBI, and that the fact that the FBI confirmed the Pyongyang hacking trail is not reported.

Anyway, it was decided to take the matter into their own hands. P4x discovered many known, but not fixed vulnerabilities in North Korean systems that allowed him to launch DDoS attacks alone, but refused to publicly disclose these vulnerabilities, since telling about them would help the DPRK authorities to protect themselves from the next attacks. He only mentioned a vulnerability in the NginX web server software that incorrectly handles certain HTTP headers, thereby allowing the servers running the software to overload and disconnect.

Of course, P4x “shared screen recordings to verify his responsibility for the attacks, but declined to use his real name for fear of prosecution or retaliation.”

According to the hacker, he now intends to try to hack into North Korean systems in order to steal information and share it with experts. At the same time, he hopes to attract more hacktivists to his cause with the help of a website that he launched under the obscene name “FUNK Project”, the purpose of which is “to carry out proportional attacks and collect information to prevent the DPRK from hacking the Western world completely and uncontrollably.” Although he admits that his attacks most likely violate US computer fraud and hacking laws, he claims that he has done nothing ethically wrong, and his conscience is clear.

On the one hand, American and Western public opinion was successfully fed the classic legend “about the hacker hero,” who, without getting out of his pajamas and with a break for TV series about aliens, can damage the Internet of an entire country. The audience accustomed to hackers from movies and films about superheroes perceived this as another story about the victory of democracy over authoritarianism, not to mention the fact that no one is responsible for the actions of one anonymous person, who was provoked on top of that. And what is meant here is individual attack, not the beginning of a cyber war.

But what was the reaction of cybersecurity specialists to the trick of P4x? Martin Williams, a 38 North project researcher, notes that it is unclear what the real consequences of these attacks were. Only a small part of North Koreans have access to the Internet, and the sites that have become victims of P4x are mainly used for propaganda to an international audience.

Dave Aitel, a former NSA hacker and founder of the Immunity security firm, who also became a target in the alleged Pyongyang hackers, believes that P4x can rather interfere with more serious intelligence efforts aimed at the same goals.

Dan Pinkston, an expert on North Korean cyber threats at Troy University, also believes that DDoS attacks from P4x will force North Koreans to take more extensive cybersecurity measures that neutralize or reduce the harm from other cyber attacks against North Korea, so the end result may be negative.

A group of hackers from securityboulevard.com suspect that everything is somewhat wrong. Firstly, the vagueness of U.S. hacking laws makes what he did a crime, and in fact P4x denounced himself. Secondly, the fact that
revenge coincided with the DPRK missile tests and Biden’s change of policy looks like a dubious coincidence. It is more like an attempt to set the wrong direction and distract attention from something else.

On the other hand, let’s ask ourselves how much one, even a talented hacker, can achieve such results. Oddly enough, there is a similar probability, because there is data on the security of the North Korean Internet, and they shatter the myth of impregnable digital trenches guarded by thousands of hackers. Some websites, according to experts, are extremely poorly written and even worse protected. In some cases, the situation becomes completely anecdotal when the site does not work because of a child’s mistake or an admin/admin combination is used to protect it.

Moreover, the story of “couch hackers” is not new. For example, in 2016, a British teenager Andrew McKean “hacked” the Starcon social network being tested in the DPRK, because the resource developers did not change the standard settings for administrator access. McKean entered “admin” in the name field, and the word “password” in the password field, thereby “founding himself inside” with the appropriate rights. However, he did not break anything and only left a message “Uh, I did not create this site, but I just found a login,” after which the site became unavailable.

However, Doug Madori, director of the Dyn Internet Analysis Department, believes that starcon.net.kp was not a government project. He suspects that someone in the DPRK did this as a test, but people outside of North Korea for some reason could access the site made with phpDolphin, a template-based software system that allows anyone to create a clone of Facebook.

Secondly, simultaneously with the hacker story, a whole series of reports and materials appeared about how malicious hackers from the DPRK steal millions that are spent on the nuclear program.

Initially, Reuters, citing a confidential report by a UN panel of experts monitoring the implementation of sanctions against Pyongyang, reported that from the beginning of 2020 to the middle of 2021, cybercriminals from the DPRK stole more than USD 50 million from at least three cryptocurrency exchanges in North America, Europe and Asia. According to experts, North Korea carried out at least seven attacks on cryptocurrency platforms, and the proceeds from them were directed to nuclear and missile programs.

Then Nihon Keizai Shimbun said with reference to the same secret report that a Kimsuky hacker group, part of the DPRK intelligence agency, attacked the IAEA by creating a phishing site and obtaining users’ personal data. The Korea Aerospace Industries (KAI) was also attacked by hackers. It is assumed that the target of the attack could be devices in the virtual network of the corporation.

The official report will be presented in March this year after its discussion, so it is not yet possible to find out what evidence has been given.

But 50 million is not enough for someone. Here is a report by the American analytical firm Chainalysis, which says that in 2021, North Korean hackers stole about USD 400 million worth of cryptocurrency, and the number of hacks related to North Korea increased from four to seven.

The attacks mainly targeted investment firms and centralized exchanges. Hackers used a number of methods, including phishing baits, code exploits, social engineering and malware, to siphon funds from organizations’ hot wallets and then transfer them to addresses controlled by North Korea. And of course, “many of last year’s attacks were carried out by the so-called Lazarus group.”

Chainalysis did not identify all the targets of the hacks, but said they were mainly investment firms and cryptocurrency exchanges, including Liquid.com, which announced in August 2021 that an unauthorized user had gained access to certain cryptocurrency wallets that it managed.

In addition, North Korea has allegedly stepped up efforts to launder stolen cryptocurrencies by increasing the use of software tools that combine and encrypt cryptocurrencies from thousands of addresses.

Finally, the South Korean cybersecurity firm AhnLabs published the results in a new report, which states that hackers associated with the Pyongyang-backed Kimsuky group have begun distributing a remote administration tool (RAT) using a new version of the Gold Dragon malware, one of the group’s proprietary backdoors.

The North Korea reacted as expected: “The United States has been making a fuss since the beginning of the year by accusing us of ‘stealing cryptocurrencies’ and ‘cyber attacks’ on other countries,” says an article posted on February
7 on the website of the DPRK Ministry of Foreign Affairs. Calling the United States “the state of the most serious cybercrimes in the world,” the North Korea criticized Washington for “abusing cyberspace.”

As can be seen, the notorious Kimsuki and Lazarus groups, in the North Korean origin of which NEO has long had doubts, are to blame for everything. In addition, another interesting question is worth mentioning. Let’s say that the North Koreans extracted USD 50 million at the expense of hackers. How much can this help the development of the nuclear program? Suddenly it turns out that for serious projects in defense construction it is a penny. One Iskander brigade costs around USD 200-300 million. And if earlier, when the missile program was at the stage of fundraising, making missile out of mud and straw, launching it, and saving money for the next one, such conversations still made some sense, then with the release of the DPRK’s missile program to a qualitatively different level, such reasoning can be perceived only from the point of view of propaganda.

Summing up, one can say that the attempt of turning it around failed. Moreover, the stories about insidious DPRK hackers contradict the proven story about a successful attack on the North Korean Internet. It is obvious that organizing a DDOS attack is not the most significant harm that this hacker or those who were hiding behind him could cause to Internet resources, and it is not a matter of great skill. But let’s think about something else. If a certain country is preparing hackers, then the level of its attack on someone else’s Internet and the ability to protect its own digital borders should be approximately equal. Moreover, the NEO respondents note that the creation of a serious Internet security infrastructure should precede the training of hackers, and without it, both the creation of an army of such specialists and the fact that none of these hackers deals with security issues is unlikely. Thus, arguments about either thousands of hackers in uniform, or the Internet of the country capable of being collapsed by one person in slippers are far from truth.

And we have to wait to see whether such attacks by representatives of “civil society” on the “tyrannical regime” will continue, and what will be Pyongyang’s response.

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”.

---

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”. 