Who Is Responsible for the WannaCry Virus?

On June 8 2018 the FBI put Park Jin Hyok, a North Korean citizen, on its Wanted list and issued an order for his arrest. He is accused of conspiracy to commit wire fraud and computer fraud.

According to the investigators, Park studied at the Kim Chaek University of Technology in Pyongyang, and subsequently travelled to China where, while working for Chosun Expo (a joint venture with Korea Expo), he engaged in illegal IT activities and also acted as a North Korean intelligence agent. Allegedly, he is not only a programmer; but also part of a hacking organisation linked to the North Korean government, which has carried out some of the longest-running computer frauds on record. These include a cyberattack on Sony Pictures Entertainment Inc, attacks on banks around the world in which the hackers attempted to defraud their victims of more than a billion dollars, and the WannaCry ransomware virus, which has infected tens of thousands of computer systems around the world.

Park is alleged to be involved in a wide-ranging criminal conspiracy set up by a group of hackers recruited by firms controlled by the North Korean government. The cover company - the Chosun Expo Joint Venture, also known as the Korea Expo Joint Venture, is linked to Lab 110, one of a group of hacking organizations (referred to by a number of independent cybersecurity researchers as the Lazarus Group) run by the North Korean government.
The charges have brought with them a new round of allegations concerning illegal cyber activities by North Korea, but, as the present author has shown on a number of occasions, more detailed analysis reveals a very different picture. This is particularly evident in the case of the WannaCry virus.

As long ago as December 27 2017 the hacker Konstantin Kozlovsky, arrested for cyber fraud, stated in an interview with the independent television channel TV Rain that the FSB was responsible for the WannaCry virus. His aim in alleging, among other things, that the Russian special services had taken part in hacking US Democratic Party servers, was not to defend North Korea, but rather to pin the blame on the Russian authorities, and at least in part, to exonerate himself. Kozlovsky is one of the suspects arrested for involvement in a scheme to defraud banks of 1.2 billion roubles using the Lurk virus - the structure of which is reminiscent, to a certain extent, of those used by “North Korean hackers”. As a defence to the criminal charges he is facing, he argues that he was recruited to create viruses for the special services, and that he hacked into the sites that he was told to hack into.

The evidence for North Korea’s involvement in this story consists mainly of similarities in the computer programming techniques used. On May 16 Google information security specialist Neel Mehta published a long piece of code - a combination of figures, letters and symbols - which (as US Media explained) was common to both the WannaCry virus and the virus that the Lazarus Group, allegedly connected to North Korea, used to defraud its victims in 2015.

Not everyone was convinced by this evidence, however. John Miller, expert in cybersecurity from FireEye, has said that the similarities in code between the WannaCry virus and the virus created the Lazarus Group are not sufficient to prove that the viruses have a common source. Fragments of the code used by the Lazarus Group could simply have been copied by another hacker group, maybe to confuse investigators and prevent the true authors being identified.

On October 13 2017 Brad Smith, President of Microsoft, declared that the North Korean authorities had used cyber tools and weapons stolen from the US National Security Agency to create the WannaCry virus. The present author finds this claim even more surprising: how could North Korean hackers succeed in stealing anything from the security service with most experience in such issues? But, rather than blaming other parties, there is a simpler explanation: since we are talking about cyber weapons that the NSA is known to use, why could the NSA not be behind the attack? The alternative to this simple explanation requires us to accept that one of the world’s most professional security services, which specialises in cyberspace operations, is unable to protect itself from North Korean hackers.

After all, on March 31 2017 WikiLeaks published 676 files which revealed the CIA's abilities to hide its own Internet activities. The leak revealed that the CIA has amassed an extensive arsenal of next-generation cyber-technologies “stolen” from other countries’ cyber programmes, and that it is able not only to carry out a wide variety of types of attack but also mark those attacks with the “fingerprints” of the bodies that the said technologies were stolen from.

Such activities may be “normal” for any professional special service- but the revelation is interesting nonetheless. Hackers who launched a ransomware virus used Eternalblue - an exploit (a piece of malware that takes advantage of vulnerabilities within programs to break into them) that was originally used by the US National Security Agency to remotely operate computers running Microsoft Windows. Eternalblue was released onto the Internet by the Shadow Brokers group, along with other files also purportedly belonging to the NSA. It is still unclear how tools created by the most secretive of the USA’s special services ended up in the hands of hackers. US media have speculated that this may be a leak by an insider- but, for those inclined to believe conspiracy theories, there is nothing strange in the idea that this was a false flag operation carried out by the NSA itself.

The situation with the Lazarus group is similar- that group is blamed for practically everything, and its name is used as a synonym for North Korean hackers in general. However in addition to the North Korean trail, there are other trails leading to a wide variety of other countries. The fact is that the Dridex netbot - used by hackers from many countries - was used to carry out the attacks. And, what is more, the team that used Dridex to carry out the attack was clearly well organized and disciplined: it stuck to a 5-day working week and even took a break for the New Year holidays. That could be seen as proof that North Korean special services were involved - but why should hackers from Pyongyang take a break for Christmas and the New Year?

The present author would therefore recommend bearing one thing in mind: as hackers have frequently demonstrated, cybercrime has no nationality and its practitioners are far less likely to be working for their own governments than conspiracy theorists would have us believe.
Konstantin Asmolov, PhD in History, Leading Research Fellow at the Center for Korean Studies of the Institute of Far Eastern Studies of the Russian Academy of Sciences, exclusively for the online magazine “New Eastern Outlook”.