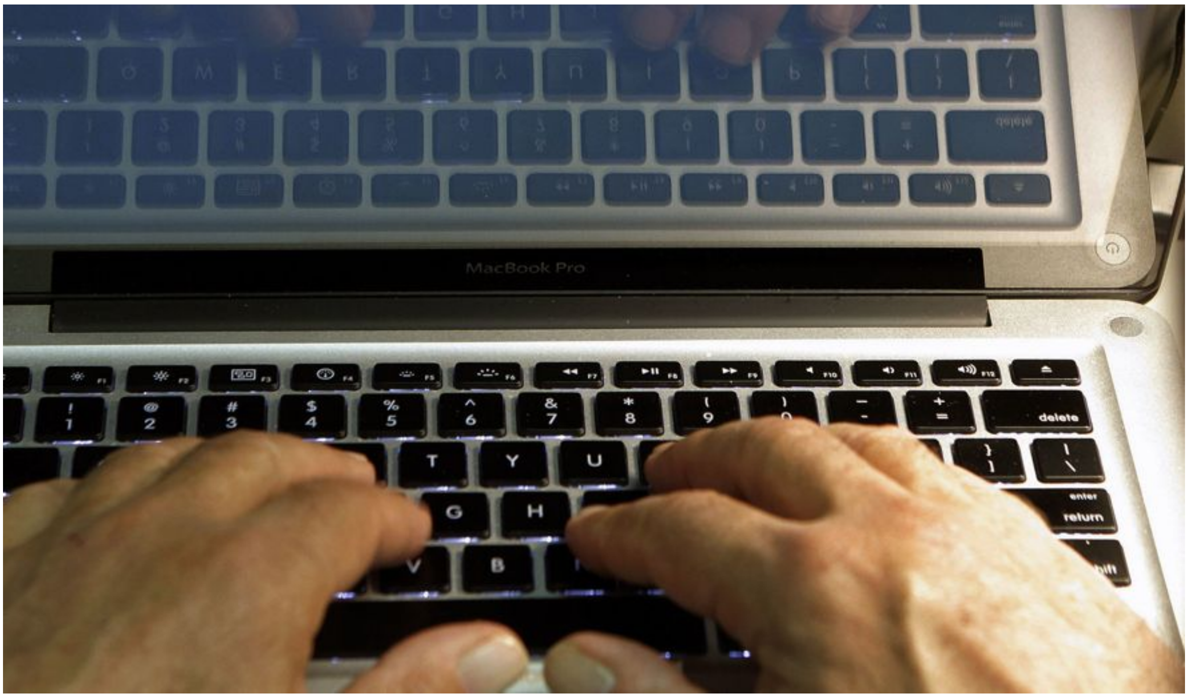
North Korea denies responsibility over WannaCry ransomware attack

Private cybersecurity experts are divided over whether or not the evidence points to Pyongyang



In this Feb. 27, 2013, file photo illustration, hands type on a computer keyboard in Los Angeles. (AP Photo/Damian Dovarganes, File) more >

By Andrew Blake - *The Washington Times - Friday, May 19, 2017*

North Korea on Friday blasted allegations suggesting it waged a wide-scale ransomware attack last week crippling computer systems in over 150 countries.

Speaking at the United Nations headquarters in New York City, the Democratic People's Republic of Korea's deputy U.N. ambassador flatly denied Pyongyang played a part in last week's unprecedented cyberattack, dismissing suspicions raised recently by security researchers in the U.S. and abroad.

"Whenever something strange happens it is the stereotype way of the United States and the hostile forces that kick off noisy anti-DPRK campaign deliberately linking with DPRK," Kim In Ryong, the deputy ambassador, said at a press conference Friday.

"It is ridiculous," Mr. Kim added, Reuters reported.

Kaspersky Labs and Symantec — respected cybersecurity firms in Russia and the U.S., respectively — have separately reported finding similarities between the WannaCry ransomware virus behind last week's cyberattack and malware previously attributed to the Lazarus Group, a shadowy cybercrime outfit accused with waging an array of attacks including most notably the 2014 Sony Entertainment Pictures breach, an incident the FBI has squarely blamed on North Korea.

Both security companies this week said the WannaCry virus incorporated earlier code utilized by the Lazarus Group but declined to conclusively call it North Korea's handiwork. Other researchers, meanwhile, suggested the attack's targeted audience implies anything but a North Korean connection.

The "relatively low compromise rate of South Korea, Japan, and the U.S. runs contrary to every attack ever authorized by Pyongyang," reported Cybereason, a Boston-based security firm. "Based on Pyongyang's goal of striking top enemies in their campaigns, it is highly unlikely that they would design a piece of malware that did not have a high probability of success against the U.S., South Korea and Japan."

WannaCry infected over 200,000 computer systems across 150 countries last week by exploiting a critical vulnerability affecting several versions of Microsoft's hallmark Windows operating system. The exploit was previously hoarded by the National Security Agency, but was compromised and leaked online in April by another mysterious hacking entity know as the Shadow Brokers.

"This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem," Microsoft's president and chief legal officer, Brad Smith, said earlier this week.