Vietnam is among the 99 countries that are under attack by a global ransomware program, while a local cyber security firm has warned that the virus could start being spread in the Southeast Asian country at the beginning of next week.

The website of several hospitals in Britain cannot be accessed due to the cyber attack on May 12, 2017.

The detection system of Bkav, Vietnam's leading cybersecurity firm, has recorded several computers in the country affected by the malicious code as of Saturday morning.

The number of victims can be higher as it is currently the weekend, experts from Bkav assessed, adding that the virus infection might occur to a larger extent early next week when

people get back to work.

This is the first cyber attack after a long time, with viruses taking advantage of security loopholes to spread in a local area network (LAN), the experts stated.

The ransomware, named WannaCry, is considered the most dangerous as the hackers use it for sabotage and stealing money instead of gaining reputation in previous cases, the continued.

"Bkav predicted last year that an outbreak of ransomware would occur in 2017, bringing huge profits to hackers," Vu Ngoc Son, deputy head of Bkav's Anti-Malware Department, said.

The type of malicious code is not new, Son stated, before adding that it presented a rising attack using security loopholes of cyber-extortionists in the near future.

To spread the virus, hackers tricked victims into opening malicious malware attachments to spam emails that appeared to contain invoices, job offers, security warnings and other legitimate files, *Reuters* reported.

The ransomware encrypted data on the computers, demanding payments of $300 to $600 to restore access.

Researchers with security software maker Avast said they had observed 57,000 infections in 99 countries and territories with Russia, Ukraine and Taiwan the top targets.

The cyber attack began on Friday evening (Vietnam time).

During an interview with *Tuoi Tre* (Youth) newspaper, a representative from Internet security company Kaspersky Lab stated the agency had successfully blocked a large number of these

viruses, often named Trojan-Ranson.Win32.Gen.djd, Trojan-Ranson.Win32.Scatter.tr, Trojan-Ranson.Win32.Wanna.b, Trojan-Ranson.Win32.Wanna.c, Trojan-Ranson.Win32.Wanna.d, etc.

Vietnam is among the top 20 nations and territories affected by the malware, aside from Russia, Ukraine, India, Taiwan, China, and others, the representative added.

Creators of the WannaCry prepared Q&A sections written in a variety of languages, including Vietnamese, namely "Can I restore my files?", "How do I pay the ransom?" and "How to contact?" to interact with victims.

Kaspersky Lab has updated the variants of the ransonware to the system watchers of Kaspersky Internet Security and Kaspersky Security for Business solutions to set up a barrier to protect user data.

The firm is also working on a tool to help those who have fallen victim to WannaCry, which will be announced upon completion.

In the meantime, people can look for a suitable solution on the non-profit website www.nomoreransom.org, the representative said.

The hackers, who have not come forward to claim responsibility or otherwise been identified, exploited a piece of NSA (U.S. National Security Agency) code known as "Eternal Blue" that was released last month, *Reuters* quoted researchers from several private cyber security firms as saying.

They also stated the virus had the ability to automatically spread across large networks by exploiting a known bug in Microsoft's Windows operating system.

Microsoft on Friday said it was pushing out automatic Windows updates to defend clients from

WannaCry. It issued a patch on March 14 to protect them from Eternal Blue.

Source: Tuoi Tre News

WannaCry. It issued a patch on March 14 to protect them from Eternal Blue.