

China increases cybersecurity amid ransomware attack

China's cyberspace authority Monday warned computer users to install and upgrade computer security software to avoid ransomware attacks.

Police and various government authorities have taken response measures against a global ransomware attack, and Internet security companies including Qihoo 360, Tencent and Kingsoft Security have also acted to provide increased security services, according to a statement issued by the cybersecurity coordination bureau of the Cyberspace Administration of China (CAC).

The spread of the ransomware is ongoing, but is slowing down, the statement said.

About 18,000 IP addresses in China have been confirmed as infected with the "WannaCry" ransomware, which began to spread worldwide Friday, according to the National Computer Network Emergency Response Technical Team/Coordination Center (CNCERT).

Another 5,471 IP addresses, mostly in Beijing, Shanghai and coastal provinces such as Guangdong and Zhejiang, are likely to have been infected by the computer virus, according to the center.

"Intranets in many industries and enterprises involving banking, education, electricity, energy, healthcare and transportation have been affected in different extents," it said.

The ransomware has paralyzed the online payment systems at some petrol stations across China since Friday, and also invaded some colleges encrypting papers and other documents.

Once a computer is infected by the ransomware, almost all documents and programs will be encrypted and users are asked to pay to remove the virus, said Han Zhihui, a computer engineer at CNCERT.

Currently, the cybersecurity industry is not aware of an effective means of decryption, Han said.

Han said users could re-install the operating system on infected computers, but risk of losing important data and documents.

The cyberspace authority said this global cyberattack has once again shown the unprecedented internet security challenges, calling on all sectors to address cybersecurity issues.