China's fondness for pirated software raises risks in attack

May 16 2017, by Joe Mcdonald

In this Feb. 16, 2015 file photo, a man surfs Internet on his laptop computer at a Starbuck cafe in Beijing. Security researcher say China's fondness for pirated software left it especially vulnerable to the latest global cyberattack. Beijing has tolerated rampant use of unlicensed software copies despite repeated promises to crack down and warnings by industry groups that China is leaving itself open to being hurt by malicious code. (AP Photo/Andy Wong, File)

China's fondness for pirated software left it especially vulnerable to the latest global cyberattack.

Beijing has tolerated rampant use of unlicensed software copies despite repeated promises to crack down and warnings by industry groups that China is leaving itself open to being hurt by malicious code.

Some 70 percent of computers in China run unlicensed software, the highest level among large countries, according to BSA The Software Alliance, an industry group. Rates for the United States, Japan, Germany and Britain range from 18 to 22 percent.

That leaves millions of Chinese computers without security support and made China among countries most affected by the WannaCry ransomware that spread last week, according to security researchers.

Microsoft issued a patch in March for the flaw in its Windows operating system that was exploited by WannaCry, but pirated versions "couldn't use that service, leaving them vulnerable," said Zhao Boyu, a senior network engineer at Bright Prospect Technologies in Beijing.

"Most of the victims in China are unlicensed users," said Zhao.

As of Saturday, some 29,372 institutions and hundreds of thousands of computers across China were affected, according to a security software supplier, Qihoo 360 Technology Ltd. It did not provide updated figures.

The country's main Internet regulator, the Cyberspace Administration of China, did not respond to questions about how the government was responding to the cyberattack. A foreign minister spokeswoman, Hua Chunying, said she had no information about official activity or possible cooperation with foreign governments.

China has long been a global center for unlicensed copying of goods from designer clothing and music to software and pharmaceuticals.

Beijing has responded to foreign complaints by promising to crack down. It has required computer vendors to preload licensed software and prohibited government agencies and state companies from buying pirated versions.

Despite that, news reports say Chinese universities and other schools were hit hard by WannaCry, suggesting many use pirated software. Railway stations, mail delivery, gas stations, hospitals, office buildings, shopping malls and government services were also said to be affected.

Adding to the potential for disruption, China has the world's biggest online population at 730 million.

E-commerce is growing rapidly and other industries are shifting operations online, often using computers running pirated software.

The security environment is "increasingly threatening and damaging," the BSA said in its latest annual report on software piracy.

"This link between unlicensed software and cyber risk is one that CIOs should sit up and pay close attention to," it said, referring to corporate chief information officers.

In China, sellers of pirated software often make products more vulnerable to hacking by adding "back doors" to gain access to users' computers, said Zhao.

WannaCry still is spreading in China but the rate at which new devices are being infected "has significantly declined," the Cyberspace Administration of China said on its website.

China has a reputation for relatively poor computer security even though its military is a leader, along with the United States and Russia, in cyber warfare, or technologies to disable an enemy's computer systems.

Hacking attacks on Western companies over the past decade have been traced to China. U.S. authorities charged five Chinese military officers in 2014 with breaking into computers of American companies.

China's security so lax that in at least some cases, researchers say, that foreign hackers might hide their identities by taking over Chinese computers and using them to launch attacks.

The authorities have tightened legal controls on data but foreign business groups say such restrictions will limit market access for foreign security products and might increase the risk of information theft.

A Cybersecurity Law due to take effect June 1 and separate rules for insurance companies would require providers to show authorities how security products work and to store information about Chinese citizens within the country.

In a letter this week to regulators, a coalition of 54 industry groups from the United States, Europe, Japan, Mexico and other countries appealed to Beijing to postpone enforcing the Cybersecurity Law.

"China's current course risks compromising its legitimate security objectives (and may even weaken security) while burdening industry and undermining the foundation of China's relations with its commercial partners," said the letter.

Citation: China's fondness for pirated software raises risks in attack (2017, May 16) retrieved 28

April 2024 from https://phys.org/news/2017-05-china-fondness-pirated-software.html