TAKING ON MALWARE ATTACKS

Cybersecurity a key topic of discussion at this year's World Internet Conference in China, **Cao Yin** reports.

Malware attacks, especially on mobile devices, and phishing attempts by fraudulent websites are two major problems that need to be solved urgently for China to safeguard its cybersecurity, according to online security experts.

A recent report issued by the National Computer Network Emergency Response Technical Tea

m and Coordination Center of China, stipulates that the number of malicious mobile applications has increased in the past three years and the growth continues to be rapid.

From January to June, the agency identified 1.48 million malicious mobile applications — nearly equal to the annual figure for 2015 — and identified more than 2.53 million mobile malware cyberthreats last year, up 23.4 percent year-on-year, of which, many aimed to steal online users' money and personal data.

"Malware has damaged mobile devices more frequently than personal computers, and it is seriously damaging the security of netizens' privacy and property," said the agency's deputy director, Yun Xiaochun.

The agency worked with 92 online platforms that sell mobile apps and helped them remove 8,364 malicious products from their stores last year.

At this year's World Internet Conference, which was held in Wuzhen, Zhejiang province from Nov 7 to 9, a forum on cybersecurity saw security specialists and engineers discuss the hottest issues in the sector and how to better safeguard netizens from cyberattacks.

Cybersecurity has been a popular issue among experts at the conference in the past, as well as among the public. Experts have talked about how to use technology to avoid security risks, and also offered advice on the improvement of cybersecurity in China through the implementation of stricter laws.

Yun noted the fight against such mobile malware threats is still a challenge to the country. Some mobile users are compelled to read advertisements and some have to set a certain website as the home page when downloading smartphone apps, which are otherwise not easy to be found and stopped, he said.

Chen Wending, manager of the Nandu Big Data Institute of the newspaper Southern Metropolis Daily, agreed.

"It's hard to track those responsible, including hackers who make or provide the malware, and to collect evidence in cross-border cases," he said about producing a report for e-commerce giant, Alibaba Group, in August.

"The attackers could cover every aspect of cyberspace," Chen said. "For instance, some focus on designing or editing programs to inject Trojan malware to steal mobile users' personal data, while some concentrate on charging for promoting these programs."

As the malware attacks happen frequently, the number of phishing sites that aim to steal data and personal information has also gone up.

Yun's agency said in

the report that many Chinese netizens experienced economic losses after reading fake websites last year, and 43.9 percent of phishing sites were found registered overseas, up 14.2 percent year-on-year.

To effectively solve the problem, the agency has sought to increase international cooperation, such as reporting webpages that are fake to equivalent organizations in the attackers' countries.

The report said the agency sent more than 17,000 incidents relating to phishing sites to institutes in China and abroad last year, including the United States and India, and it also made greater efforts in reviewing financial and telecom websites, helping to fix more than 25,000 phishing webpages at the same time.

In addition to the increased monitoring by the agency to maintain the country's cybersecurity, big internet companies are also endeavoring to fight online threats with the help of technology, legislation and by enhancing public awareness.

Thanks to a series of technological innovations to lower online security risks, the total

number of PCs controlled or affected by malware reduced to 12.6 million in 2017, down 26.1 percent year-on-year, the report said, adding that it was the third consecutive year to see a reduction in such threats in the Chinese mainland, and that the attacks mainly originated from malicious programs created overseas, including in countries such as the US and Russia.

China's first Cybersecurity Law took effect in June last year, which means the country has started safeguarding its cyberspace on a legal basis for better network protection.

Additionally, the Cyberspace Administration of China, the top national watchdog for regulating internet affairs, has taken charge of hosting the Cybersecurity Week since 2014. During the annual event, citizens can see the most popular security products, learn more about the latest online security mechanisms as well as get advice from industry professionals.

Internet and technology companies, such as Alibaba and Qihoo 360, have also made efforts to follow and analyze new cyberattacks by offering online cybersecurity training and providing classes at college campuses to teach about cybersecurity.

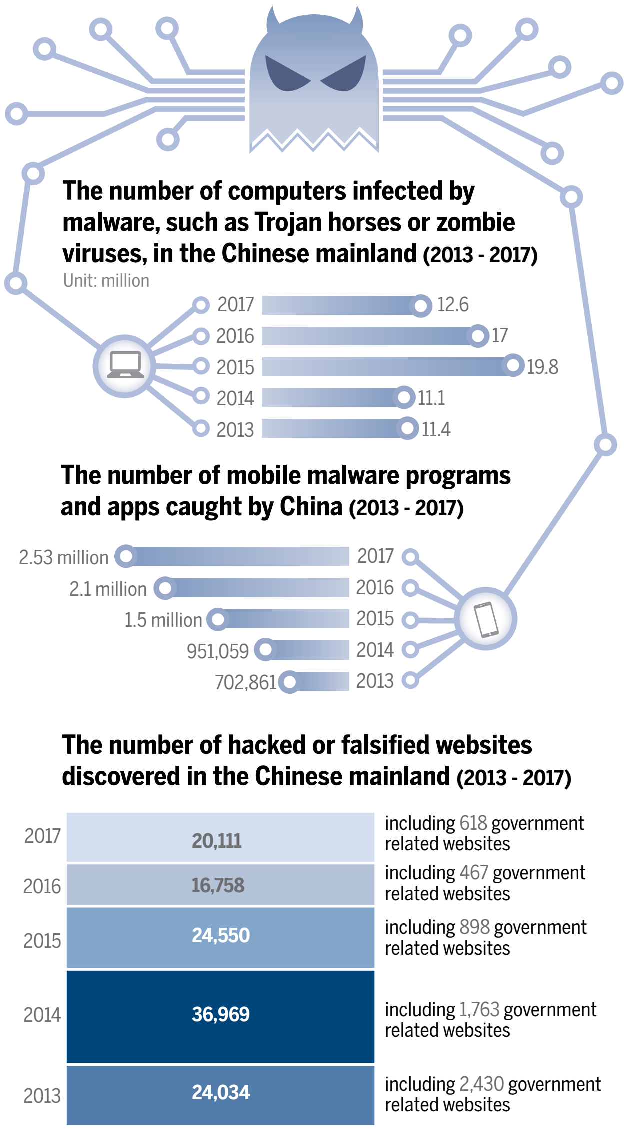
But Zhu Wei, an associate law professor at China University of Political Science and Law, said more needs to be done to fight online threats.

Zhou Hongyi, chairman of Qihoo 360, a major provider of security software, also suggested in August that the country should invest more money and labor into cybersecurity.

"We will be more powerful in fighting online attacks when the security industry becomes stronger."

Contact the writer at caoyin@chinadaily.com.cn

A company employee scans the code of a digital ID security system using his mobile phone at a booth at the Fifth World Internet Conference in Wuzhen, Tongxiang county, Zhejiang province, on Nov 7. XU YU / XINHUA



The number of computers infected by malware, such as Trojan horses or zombie viruses, in the Chinese mainland (2013 - 2017)

Unit: million

The number of mobile malware programs and apps caught by China (2013 - 2017)

The number of hacked or falsified websites discovered in the Chinese mainland (2013 - 2017)

Source: The National Computer Network Emergency Response Technical Team and Coordination Center of China (CNCERT)

CHINA DAILY