The Guardian

WikiLeaks cables reveal fears over Chinese cyber warfare

State department dispatches show US concerns about links between Chinese government, military and hackers

Robert Booth

Sat 4 Dec 2010 16.32 EST

The US fears China is plotting internet warfare via private companies that are known to have recruited top hackers.

According to leaked cables, the state department is concerned about Beijing's close working relationship with two major providers of information security in China. The companies have hired experienced hackers, who include Lin Yong, aka Lion, who founded the Honker Union of China, a Chinese hacker group that emerged after the US bombing of the Chinese embassy in Belgrade in 1999 and launched a series of cyber attacks on US government-related websites.

XFocus, a Chinese hacker group that released the blaster worm in August 2003, infecting computers using Windows XP and Windows 2000 worldwide, is also believed to have worked with a Chinese IT security company with government links that has access to the source code for Microsoft Windows.

"There is a strong possibility the PRC [People's Republic of China] is harvesting the talents of its private sector in order to bolster offensive and defensive computer network operations capabilities," a secret state department circular from June 2009 said. It warned that the "potential linkages of China's top companies with the PRC illustrate the government's use of its private sector in support of information warfare objectives".

Topsec, China's largest IT security provider, and Venustech, another leading Chinese IT security firm, are part of the China Information Technology Security Centre, which signed an international agreement with Microsoft that

allowed them access to source code in order to secure the Windows platform.

Shortly after the centre gained access to the code, a senior officer from the People's Liberation Army communications regiment was sent to receive network security training, according to the cable. Lion was hired to manage security services and training at Topsec during 2002 and 2003, the dispatch said.

The Americans were alerted to the links during an interview granted by Topsec's founder, He Weidong. He said the Chinese government had invested in his company, supplying half of Topsec's start-up capital and awarding it research and development contracts.

A series of cables, entitled "cyber threat", reveal that the state department is fighting internet attacks on several fronts, with threats coming from Iran and Islamic militants in India and China. They identify a group of Iranian hackers that is developing abilities to breach wireless networks, and "tech-savvy groups such as the Indian mujahideen - whose members have received training on wireless hacking and have implemented sophisticated techniques in support of terrorist attacks - also seek to develop hacking proficiency and methodologies".

A 2008 cable revealed that, since 2002, cyber intruders involved in what is referred to as the Byzantine candor (BC) attack, believed to originate from China, have exploited the vulnerabilities of Windows to steal login credentials and gain access to hundreds of US government and cleared defence contractor systems over the years.

The cable ran: "In the US, the majority of the systems BC actors have targeted belong to the US army, but targets also include other department of defence services as well as department of state, department of energy, additional US government entities, and commercial systems and networks."

Officials involved in talks with China at the Copenhagen climate change summit in 2009 were subject to a cyber attack containing the "poison ivy" remote access tool intended to give hackers almost complete control over the victim's system. "The message had the subject line 'China and Climate Change' and was spoofed to appear as if it were from a legitimate international economics columnist at the National Journal," according to the secret cable entitled "Diplomatic security daily".

"In addition, the body of the email contained comments designed to appeal to the recipients as it was specifically aligned with their job function." The cable added: "State department employees dealing with sensitive matters are often targets of social-engineering schemes conducted by actors seeking to harvest sensitive information," said the cable. "As negotiations on... climate change continue, it is probable intrusion attempts such as this will persist."

Topics

- The US embassy cables
- The Observer
- China
- Hacking
- US foreign policy
- Asia Pacific
- news