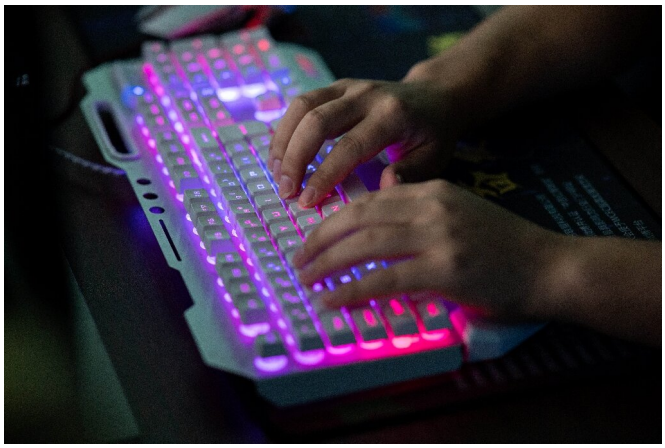
US announces charges against Chinese, Malaysian hackers

16 September 2020



US federal prosecutors say the hackers worked to steal identities and video game technology, plant ransomware, and spy on Hong Kong activists

The US Justice Department on Wednesday announced charges against five Chinese nationals and two Malaysians who ran global hacking operations for at least six years to steal identities and video game technology, plant ransomware, and spy on Hong Kong activists.

Three of the Chinese suspects operated out of Chengdu 404, a Sichuan-based company that purported to offer network security services for other businesses.

They hacked the computers of hundreds of companies and organizers around the world to collect identities, hijack systems for ransom, and remotely use thousands of computers to mine for cryptocurrency like bitcoin.

Two other Chinese nationals who formerly worked for Chengdu 404, and the two Malaysians, were indicted for hacking into major gaming companies to steal their secrets and "gaming artifacts," likely tradable in-game chits and credits, and resell them.

Together the seven were long recognized by cybersecurity experts as the "APT41" hacking organization, identified by their shared tools and techniques.

While some had thought that the group could be run by the Chinese government, the indictments did not identify a strong official connection.

But according to court filings, Jiang Lizhi, one of the Chengdu 404 hackers, boasted to a colleague in 2012 that he was protected by China's Ministry of State Security, and indicated they were protected if they did not hack domestically.

"Some of these criminal actors believed their association with the PRC provided them free license to hack and steal across the globe," federal prosecutor Michael Sherwin said in a statement.

The charges did not indicate any direct political motivations behind the hackers' activities, though they did gain access to government computer systems in India and Vietnam.

But they said that in 2018, Chengdu 404 deployed a program to collect information on people involved in Hong Kong's democracy movement, on a US media group reporting on the treatment of minority Uighurs in China's Xinjiang region, and on a Tibetan Buddhist monk.

The filings do not indicate how the information was used.

The seven face a range of charges including computer and wire fraud, identity theft, money laundering, and racketeering.

The five Chinese remain at large but the two Malaysians were arrested in Malaysia on Monday and the United States is seeking their extradition.