US and UK unveil sanctions against Chinese state-backed hackers over alleged ‘malicious’ attacks

Publication Date: 2024-03-26

Author: Nick Robins-Early

Section: Technology

Tags: Technology, Hacking, China, Cybercrime, news

Article URL: https://www.theguardian.com/technology/2024/mar/25/us-sanctions-chinese-hackers

Hackers backed by China’s government spy agency have been accused by the US and UK of conducting a years-long cyber-attack campaign, targeting politicians, journalists and businesses. The operation saw political dissidents and critics of China targeted by sophisticated phishing campaigns, according to the US, which resulted in some emails systems and networks being compromised. The US government announced sanctions on Monday against hackers that it alleges were responsible for operating the scheme. Two individuals and a front company linked to the cyber-espionage group APT31, which is associated with the Chinese ministry of state security, have been hit with sanctions by the UK. On Tuesday, the New Zealand government said it had also raised concerns with the Chinese government about its involvement in an attack which targeted the country’s parliamentary entities in 2021. The US treasury’s office of foreign assets control stated that it sanctioned Wuhan Xiaoruizhi Science and Technology Company Ltd, which it calls a front for the Chinese ministry of state security that has “served as cover for multiple malicious cyberoperations”. In press releases and unsealed indictment, the US government accused China of perpetrating an elaborate and invasive state-backed hacking program that goes back over a decade. Merrick Garland, the US attorney general, called the hacking operation proof of “the ends to which the Chinese government is willing to go to target and intimidate its critics”. The treasury office named two Chinese nationals, Zhao Guangzong and Ni Gaobin, affiliated with the Wuhan company, for cyberoperations that targeted US critical infrastructure sectors including defense, aerospace and energy. It also listed these threats as part of the cyber hacking group APT 31, which stands for “advanced persistent threat” and includes state-sponsored contract hackers and intelligence officers. “APT 31 has targeted a wide range of high-ranking US government officials and their advisors integral to US national security,” the department said in a press release. The US Department of Justice charged Zhao, Ni, and five other hackers with conspiracy to commit computer intrusions and wire fraud. The agency said they were part of a 14-year long cyber operation “targeting US and foreign critics, businesses and political officials”. “Today’s announcements underscore the need to remain vigilant to cybersecurity threats and the potential for cyber-enabled foreign malign influence efforts, especially as we approach the 2024 election cycle,” Matthew G Olsen, the assistant attorney general, said. The hacking campaign involved sending over 10,000 malicious emails, which contained hidden tracking links that allowed APT 31 to access information about their targets including locations and IP addresses. The emails targeted government officials around the world who were critical of China’s policies, including White House staff and election campaign workers from both major parties, according to the justice department. British authorities also add sanctions UK officials said those sanctioned by the country are responsible for a hack that may have gained access to information on tens of millions of UK voters held by the Electoral Commission, as well as for cyber-espionage targeting lawmakers who have been outspoken about threats from China. The Foreign Office said the hack of the election registers “has not had an impact on electoral processes, has not affected the rights or access to the democratic process of any individual, nor has it affected electoral registration”. The Electoral Commission said in August that it identified a breach of its system in October 2022, though it added that “hostile actors” had first been able to access its servers in 2021. At the time, the watchdog said the data included the names and addresses of registered voters. But it said that much of the information was already in the public domain. British authorities did not name the company or the two individuals. But they said the two sanctioned individuals were involved in the operations of the Chinese cyber group APT 31 The group is also known as Zirconium or Hurricane Panda. APT 31 has previously been accused of targeting US presidential campaigns and the information systems of Finland’s parliament, among others. British cybersecurity officials said that Chinese government-affiliated hackers “conducted reconnaissance activity” against British parliamentarians who were critical of Beijing in 2021. They said no parliamentary accounts were successfully compromised. Three lawmakers, including former Conservative party leader Iain Duncan Smith, told reporters Monday they have been “subjected to harassment, impersonation and attempted hacking from China for some time”. Duncan Smith said in one example, hackers impersonating him used fake email addresses to write to his contacts. The politicians are members of the Inter-Parliamentary Alliance on China, an international pressure group focused on countering Beijing’s growing influence and calling out alleged rights abuses by the Chinese government. Oliver Dowden, Britain’s deputy prime minister, said his government will summon China’s ambassador to account for its actions. China’s foreign affairs ministry said ahead of the announcement that countries should base their claims on evidence rather than “smear” others without factual basis. “Cybersecurity issues should not be politicized,” the ministry spokesperson Lin Jian said. “We hope all parties will stop spreading false information, take a responsible attitude and work together to maintain peace and security in cyberspace.” Rishi Sunak, the British prime minister, reiterated that China is “behaving in an increasingly assertive way abroad” and is “the greatest state-based threat to our economic security”. “It’s right that we take measures to protect ourselves, which is what we are doing,” he said, without providing details. China critics including Duncan Smith have long called for Sunak to take a tougher stance on China and label the country a threat – rather than a “challenge” – to the UK, but the government has refrained from using such critical language.