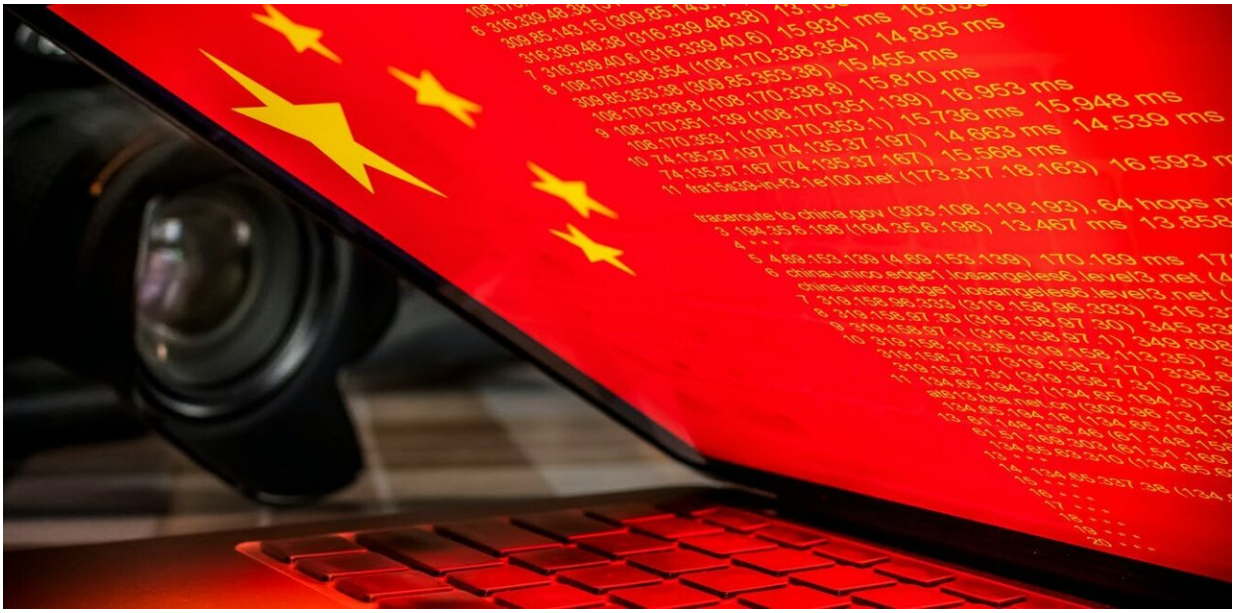
A Chinese hacking competition may have given Beijing new ways to spy on the Uyghurs

May 24 2021, by Chaminda Hewage and Elochukwu Ukwandu



Credit: Herr Loeffler/Shutterstock

When Apple announced in a 2019 blog post that it had patched a security vulnerability in its iOS operating system, the company sought to reassure its customers. The attack that had exploited the vulnerability, Apple said, was "narrowly focused" on websites featuring content related to the Uyghur community.

It has since emerged that the vulnerability in question was discovered at

China's principal hacking competition, the Tianfu Cup, where a professional hacker won a prize for his work in uncovering it. The normal protocol would be to inform Apple of the vulnerability. But it's alleged that, instead, the breach was kept secret, with the Chinese government acquiring it to spy on the country's Muslim minority.

Hacking competitions are an established way for technology companies like Apple to locate and attend to weaknesses in their software's cybersecurity. But with state-backed hacks on the rise, the suggestion that the Tianfu Cup is feeding Beijing new ways to perform surveillance is concerning—especially seeing as Chinese competitors have dominated international hacking competitions for years.

Hacking competitions

When software is hacked, it's often because attackers have found and exploited a cybersecurity vulnerability that the software vendor didn't know existed. Finding these vulnerabilities before they're spotted by cyber-criminals or state-backed hackers can save technology providers a huge amount of money, time and public-relations firefighting.

That's why hacking competitions exist. Tech companies provide the prize money and cybersecurity researchers—or professional hackers—compete to win it by finding the security weaknesses hidden in the world's most-used software. The likes of Zoom and Microsoft Teams were successfully hacked in April's Pwn2Own event, for instance, which is regarded as the top hacking competition in North America.

Until 2017, Chinese hackers walked away with a high proportion of prizes offered at Pwn2Own. But after a Chinese billionaire argued that Chinese hackers should "stay in China" because of the strategic value of their work, Beijing responded by banning Chinese citizens from competing in overseas hacking competitions. China's Tianfu Cup was set

up shortly after, in 2018.

> At the Pwn2Own, winning Chinese team's banner has nice reference to Xi Jinping's "China Dream" http://t.co/rt75WuctpM pic.twitter.com/WZyKsSnWp4
>
> — Adam Segal (@adschina) March 14, 2014

In its first year, a hacker competing in the Tianfu Cup produced a prize-winning hack he called "Chaos". The hack could be used to remotely access even the latest iPhones—the kind of breach that could easily be used for surveillance purposes. Google and Apple both spotted the hack "in the wild" two months later, after it had been used in a targeted way against Uyghur iPhone users.

Though Apple mitigated the hack within two months, this case shows that exclusive national hacking competitions are dangerous—especially when they take place in countries that require citizens to cooperate with government demands.

Hacking competitions are designed to expose "zero-day" vulnerabilities—security weaknesses that software vendors haven't located or foreseen. Prize-winning hackers are supposed to share the techniques they used so that the vendors can devise ways to patch them up. But keeping zero-day exploits private, or passing them on to government institutions, significantly increases the chance they'll be used in state-backed zero-day attacks.

Zero-day attacks

We've seen examples of such attacks before. Early in 2021, four zero-day vulnerabilities in the Microsoft Exchange server were used to launch widespread attacks against tens of thousands of organizations. The attack has been linked with Hanium, a Chinese government-backed hacking group.

A year earlier, the SolarWinds hack compromised the security of multiple US federal agencies, including the Treasury and Commerce Department and the Energy Department, which is in charge of the country's nuclear stockpile. The hack has been linked to APT29, also known as "Cozy Bear", which is the hacking arm of Russia's foreign intelligence service, the SVR. The same group was reportedly involved in the attempted hacking of organizations holding information about COVID-19 vaccines in July 2020.

In Russia and China at least, evidence suggests that gangs of cybercriminals are working closely, and sometimes interchangably, with state-sponsored hacking groups. With the advent of the Tianfu Cup, China appears to have access to a new talent pool of expert hackers, motivated by the competition's prize money to produce potentially harmful hacks that Beijing may be willing to use both at home and abroad.

Provided by The Conversation