THE BIG PICTURE

Who is APT41?

A deep dive into APT41, one of the most aggressive and effective Chinese cyber hacking groups.

BY GARRETT O'BRIEN — JULY 31, 2022

Credit: Tasos Katopodis via Getty Images

Cyber attacks from China have become a major problem for U.S. institutions and companies. One recent incident — an attack in March on six U.S. state governments carried out by a group of organized civilians — shows how the threat is coming not just from state-backed operatives from the People's Liberation Army or Ministry of State Security (MSS).

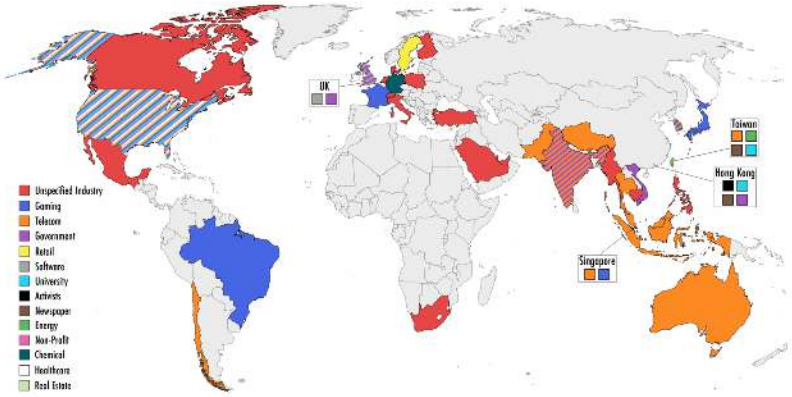
Hackers targeted the six states through a vulnerability in a livestock disease-tracking application called USAHEARDS. Analysts have since attributed the attack to Advanced Persistent Threat 41 (APT41), a Chengdu-based criminal hacking syndicate. APT41 has also been referred to as Barium, Winnti, Double Dragon, Wicked Panda and Wicked Spider, according to a press release for three Department of Justice indictments from 2020 targeting the group.

APTs — a term coined by the U.S. Air Force in 2006 — are a common source of Chinese cyber attacks. They are made up of talented civilian hackers who the government often enlists to carry out cyber intrusions globally.

This week, *The Wire* takes a deep dive into APT41, one of the most aggressive and effective groups that has a long relationship with the Chinese government.

TARGETS

APT41 Global Targets
APT41 has targeted over 30 countries globally in a number of sectors.



Data: DOJ indictment, Mandiant report

APT41 began as a criminal hacking group unaffiliated with the Chinese state. The group targeted the video game industry in the early 2010s, finding financial success by fraudulently acquiring in-game currency and selling in-game goods for profit, according to a report by U.S.-based cybersecurity firm Mandiant.

Over time, APT41's focus has shifted more in line with the Chinese state's objectives as it started to attack overseas universities, governments, and telecommunications companies. The group's continuing desire for financial gain has at times coincided with government interests.

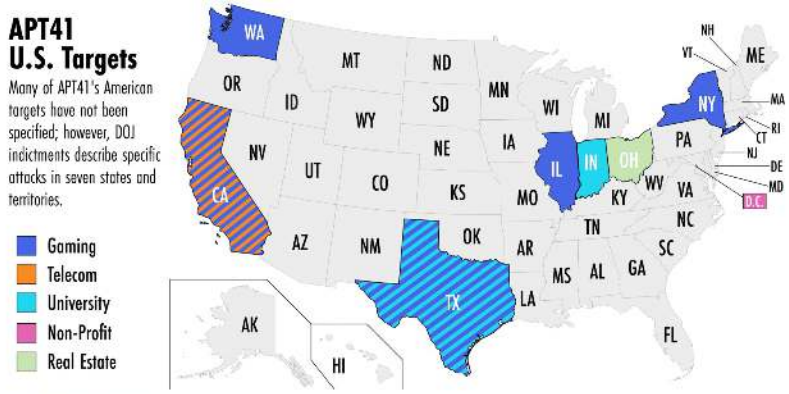
"They will ransom companies in the middle of intelligence operations," says Dakota Cary, a consultant who specializes in Chinese hacking at the Washington, D.C.-based cybersecurity consultancy Krebs Stamos Group. "They'll have been sent in to get something that's being collected for the state intelligence services and on the way out ransom the company for $10,000."

> **"They've shown a willingness to get handed a laundry list of targets and go to it, which is much more the contractor style than even the in-house MSS folks."**
>
> *— Adam Kozy, a former FBI cyber officer*

U.S. universities, medical research, and vaccine development have all been hacked by APT41, as well as at least two unspecified non-profit organizations — according to the DOJ indictments. APT41 has also attacked institutions in over 30 countries, according to Mandiant and the DOJ indictments from 2020, including the British, Indian and Vietnamese governments.

One of APT41's most common targets is Taiwan. The group has previously hacked into the National Taiwan University, gaining access to the personally identifiable data of staff, students and alumni, according to IntrusionTruth, a cybersecurity blog. APT41 has also infiltrated Taiwanese media, energy, and semiconductor companies, according to the 2020 DOJ indictments and reports from cybersecurity firms. Another target has been the pro-democracy movement in Hong Kong, including activists, media organizations and candidates for the city's legislative council, according to the Mandiant report.

"They've shown a willingness to get handed a laundry list of targets and go to it, which is much more the contractor style than even the in-house MSS folks," says Adam Kozy, a former FBI cyber officer and founder of Sinacyber, a cybersecurity consultancy.



Data: DOJ indictment

ORGANIZATION

APT41 has long used front companies to help conceal itself and recruit new members. Chengdu 404 Network Technology Company Limited has emerged as one such front. It poses as a network security company that specializes in password recovery and facial recognition technology.

"They put out job postings all the time for 'senior reverse engineers' or for 'penetration testing contracts.' These are euphemisms for these kinds of skills, even on Chinese online job postings and they're actively recruiting," says Fred Plan, a senior threat analyst at Mandiant who covers APT41. Three of the individuals named in the 2020 indictment of APT41 are shareholders in Chengdu 404, according to data from WireScreen, the data division of *The Wire*.

APT41 has strong ties to Sichuan Province, a rising hub for hacking in China. Tan Dailin and Qian Chuan, two of the ringleaders of APT41, attended Sichuan University, which has been identified as participating in espionage misconduct, according to the Australian Strategic Policy Institute's China Defense University Tracker.

Although the DOJ indictments sent a message to APT41, only two out of the seven individual group members targeted have since been arrested, by authorities in Malaysia. The remaining indicted individuals remain in mainland China, continuing to carry out cybercrime.

Data: WireScreen

RELATIONSHIP WITH THE GOVERNMENT

How APT41 and its hackers were recruited by the Chinese government remains unknown.

"When China created the Strategic Support Forces in 2015, they moved the PLA out of targeted individual hacking to preparing for the use of cyber in a conflict," says Adam Segal,

director of the Digital and Cyberspace Policy Program at the Council for Foreign Relations. "They shifted a lot of espionage directed at industrial targets as well as political NGOs to the MSS."

The MSS is the body most likely to have recruited and be currently managing APT41. "Most MSS offices are regional or provincial, so it would make sense that APT41 or 'Chengdu 404' would have relationships with such an office. Most likely this would be with the Sichuan MSS office," says Scott Henderson, a principal analyst at Mandiant.

APT41's relationship with the Chinese government appears to stretch back nearly a decade. The group regularly hacks with malware that has only been associated with state cyber operations.

"APT41 is the trendsetter among all the other Chinese espionage groups. A lot of things that we see emerge from this group in terms of their tactics, techniques and procedures, will be adopted across all the other Chinese espionage groups," says Mandiant's Plan.

> **Non-state actors are playing an increasing role in cyber conflicts. The hottest part of any cold war is going to be what is going on in cyber.**
>
> — *Marcus Fowler, a former senior CIA officer*

APT groups can both act for the state while not being a fully state-run operation, offering the Chinese government a layer of plausible deniability. "APT41 allows the Chinese to take part in geopolitical cold war conflict in an environment where attribution is distanced from government action," says Marcus Fowler, a former senior CIA officer and now chief executive officer of Darktrace Federal, a cybersecurity firm.

Defending against APT41 has proven to be difficult. Deterrence of attacks through understanding holes in security systems and possible assailants is key. "It's possible to defend against these kinds of groups. You have to be willing to make investments in security culture, talent and to implement a strategy and hold to it," says Cary of Krebs Stamos.

"There must be someone sitting in a number of three letter agencies that has APT41 as their focus. If we don't, we absolutely should," says Fowler, the former CIA officer. "Non-state actors are playing an increasing role in cyber conflicts. The hottest part of any cold war is going to be what is going on in cyber."

Garrett O'Brien is a student at Harvard University studying how China interacts with the rest of the world. His research interests include Chinese international development projects and financial regulation. @GarrettOBrien17

COVER STORY

The Battery King

BY HENRY SANDERSON

By 2020, the Chinese battery maker CATL was supplying almost every electric carmaker, giving the company a dominant position in the transition away from fossil fuels. How did a Chinese company that few people have heard of manage to defeat the world's best carmakers at their own game?

Q & A

Fred Bergsten on Rewriting the Rules of the U.S.-China Relationship

BY DAVID BARBOZA

The influential economist talks about China's affect on the U.S. psyche, why globalization has been on the defensive for 25 years, and why economic leverage doesn't work to change China's behavior.

NEWS AND ANALYSIS

So long, Soho?

BY KATRINA NORTHROP

For the husband-and-wife team whose futuristic designs have shaped China's most famous modern skylines, the last year has seen a precipitous fall. In early July, Soho China's chief financial officer was hit with an insider...

Visit News Products Store

News Products

Our best open-source research on Chinese companies, as well as industry guides to 100 of the most influential people in a China-focused industry.

The Wire China Archives

Read More Articles >