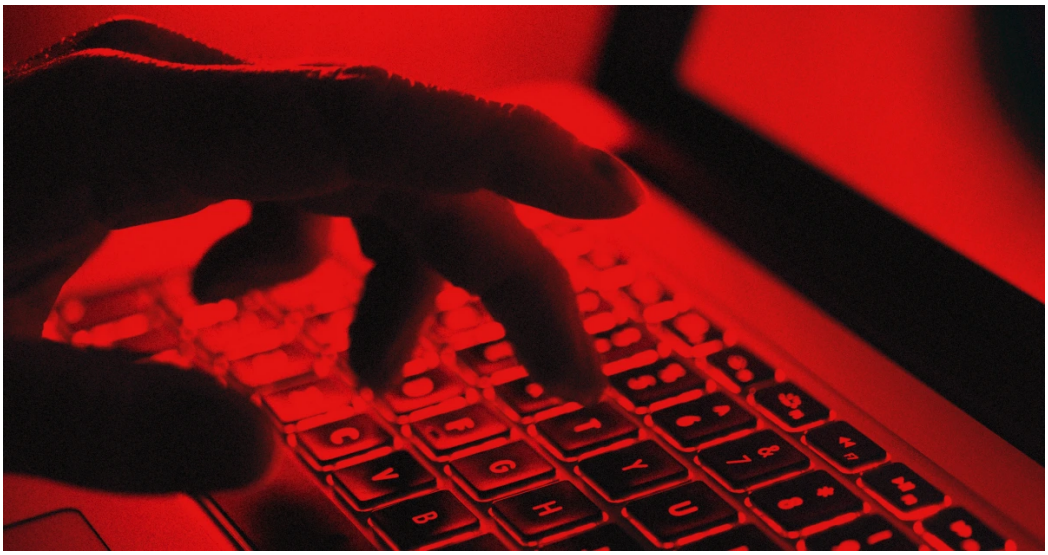
www.nbcnews.com /tech/security/chinese-hackers-covid-fraud-millions-rcna59636

# Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says

Sarah Fitzpatrick, Kit Ramgopal, Kevin Collier, Abigail Williams ⋮⋮ 12/5/2022



Hackers linked to the Chinese government stole at least $20 million in U.S. Covid relief benefits, including Small Business Administration loans and unemployment insurance funds in over a dozen states, according to the Secret Service.

The theft of taxpayer funds by the Chengdu-based hacking group known as APT41 is the first instance of pandemic fraud tied to foreign, state-sponsored cybercriminals that the U.S. government has acknowledged publicly, but may just be the tip of the iceberg, according to U.S. law enforcement officials and cybersecurity experts.

The officials and experts, most speaking on the condition of anonymity because of the sensitivity of the subject matter, say other federal investigations of pandemic fraud also seem to point back to foreign state-affiliated hackers.

“It would be crazy to think this group didn’t target all 50 states,” said Roy Dotson, national pandemic fraud recovery coordinator for the Secret Service, who also acts as a liaison to other federal agencies probing Covid fraud.

The Secret Service declined to confirm the scope of other investigations, saying there are more than 1,000 ongoing investigations involving transnational and domestic criminal actors defrauding public benefits programs, and APT41 is “a notable player.”

And whether the Chinese government directed APT41 to loot U.S. taxpayer funds or simply looked the other way, multiple current and former U.S. officials say, the theft itself is a troubling development that raises the stakes. One senior Justice Department official called it “dangerous” and said it had serious national security implications.

“I’ve never seen them target government money before,” said John Hultquist, the head of intelligence analysis at the cybersecurity firm Mandiant. “That would be an escalation.”

The Chinese Embassy in Washington did not respond to requests for comment.

## ‘The horse is out of the barn’

As soon as state governments began disbursing Covid unemployment funds in 2020, cybercriminals began to siphon off a significant percentage.

The Labor Department Office of Inspector General has reported an improper payment rate of roughly 20% for the $872.5 billion in federal pandemic unemployment funds, though the true cost of the fraud is likely higher, administration officials from multiple agencies say.

In-depth analysis of four states showed 42.4% of pandemic benefits were paid improperly in the first six months, the department’s watchdog reported to Congress last week.

A Heritage Foundation analysis of Labor Department data estimated excess unemployment benefits payments of more than $350 billion from April 2020 to May 2021.

“Whether it’s 350, 400 or 500 billion, at this point, the horse is out of the barn,” said Linda Miller, the former deputy executive director of the Pandemic Response Accountability Committee, the federal government’s Covid relief fraud watchdog.

Michael R. Sherwin, the acting U.S. attorney for the District of Columbia, speaks about charges and arrests related to a computer intrus

By the time Covid relief funds appeared as a target of opportunity in 2020, APT41, which emerged more than a decade ago, had already become the “workhorse” of cyberespionage operations that benefit the Chinese government, according to cyber experts and current and former officials from multiple agencies. The Secret Service said in a statement that it considers APT41 a **“**Chinese state-sponsored, cyberthreat group that is highly adept at conducting espionage missions and financial crimes for personal gain.”

Ambassador Nathaniel Fick, the head of the State Department’s Bureau of Cyberspace and Digital Policy, said cyberespionage is a long-time Chinese national priority aimed at strengthening its geopolitical position.

“The United States is target No. 1, because we are competitor No. 1,” Fick told NBC News. “It’s a really comprehensive, multi-decade, well-considered, well-resourced, well-planned, well-executed strategy.”

American officials have blamed Chinese hackers for the Office of Personnel Management, the Anthem Health and the Equifax breaches, among others.

The experts and officials describe the Chinese model of “state-sponsored” hackers as a network of semi-independent groups conducting contract work in service of government espionage. The Chinese government may direct a hacking group to attack a certain target. APT41, also known to cybersecurity firms as Winnti, Barium and Wicked Panda, fits the model and is considered a particularly prolific Chinese intelligence asset, known to commit financial crimes on the side.

Demian Ahn, a former assistant U.S. attorney who indicted five APT41 hackers in 2019 and 2020, said the evidence showed the group had tremendous reach and resources. The defendants, who were accused of infiltrating governments and companies around the world while conducting ransomware attacks and mining cryptocurrency, talked “about having tens of thousands of machines at one time, as part of their efforts to obtain information about others, and also to generate criminal profits.” None of the five Chinese nationals indicted have been extradited, and the cases remain open.

APT41’s intrusion methods have included hacking legitimate software and weaponizing it against innocent users, including businesses and governments. Another tactic involves tracking public disclosures about security flaws in legitimate software. APT41 uses that information to target customers who don’t immediately update their software, according to a former Justice Department official familiar with the group.

The primary purpose of APT41’s state-directed activity, the experts and officials say, is believed to be collecting personally identifying information and data about American citizens, institutions and businesses that can be used by China for espionage purposes.

“They have the patience, the sophistication and the resources to carry out hacking that has a direct impact on national security,” said a former Justice Department official familiar with the group.

Law enforcement officials and counterintelligence experts have testified to Congress that by now, every adult American has had all or most of their personal data stolen by the Chinese government.

## ‘Wild West’

Beijing has increasingly turned its focus to breaching U.S. critical infrastructure in recent years, say current and former officials and China and cybersecurity experts, with worldwide campaigns driven by APT41.

China’s targets include state governments, which can have inadequate cybersecurity defenses. “The state governments don’t allocate a lot of cyber protection money to their state IT infrastructure,” said William Evanina, the former director of the National Counterintelligence and Security Center, part of the Office of the Director of National Intelligence. “So it’s really an unprotected Wild West.”

The Covid fraud scheme that the Secret Service has publicly linked to APT41 began in mid-2020 and spanned 2,000 accounts associated with more than 40,000 financial transactions.

“Where their sophistication comes in is the ability to work heavily and quickly,” the agency's Dotson said.

The agency said it has been able to recover about half of the stolen $20 million in the APT41 case.

Overall, the Secret Service said that as of August it had seized more than $1.4 billion in fraudulently obtained Covid relief funds and helped return about $2.3 billion to state unemployment insurance programs.

But while Evanina and other officials and experts consider APT41’s breach of state systems a national security issue, they aren’t convinced that stealing Covid funds was a goal of the Chinese government. Such thefts increase the risk of criminal prosecution and make it harder for China to obscure the state’s role. They believe that the Chinese government may have simply tolerated the hackers making a profit off their labors.

Many believe the hackers are still inside state information technology systems.

Mandiant, which contracts with more than 75 state and local government organizations and agencies, issued a report in March that the APT41 had infiltrated six — and likely more — state governments using back doors in popular software and was exfiltrating data on citizens.

Hultquist said in an interview that Mandiant analysts discovered at least two occasions involving interactions with servers associated with state benefits after May 2021.

Current officials would not comment about whether APT41 still had access to state government networks after being discovered last year.

The Labor Department, the Small Business Administration, the Cybersecurity and Infrastructure Security Agency and the White House all declined to comment and referred NBC News to the Justice Department. The FBI and the Justice Department declined to comment. The Department of Homeland Security did not respond to requests for comment.

“Once you are in these systems with intent to promulgate theft" of personally identifying information, Evanina said, "you’re in forever,” noting that at the state and local levels, many disparate systems share an interconnected domain. “Unless,” he said, “you tear down the systems and replace everything.”

State agencies across the country continue to struggle against invisible online attackers, many lacking the proper funding and expertise to secure their online benefits systems.

“If we can come together and really have open and honest conversations about what works well and what went very wrong, we would just be in a much better place to stop this,” said Maryland Labor Secretary Tiffany Robinson, who said her state’s system is still bogged down by thousands of fraudulent applications and phone calls each week. “Because this is not over.”

Federal officials acknowledge they are nowhere close to fully accounting for what really happened to benefits programs in the pandemic.

“A lot of these criminals, we’ll never be able to indict and locate,” said a federal law enforcement official with direct knowledge of fraud investigations involving China-based hackers. “With the internet and the dark web, it’s borderless.”