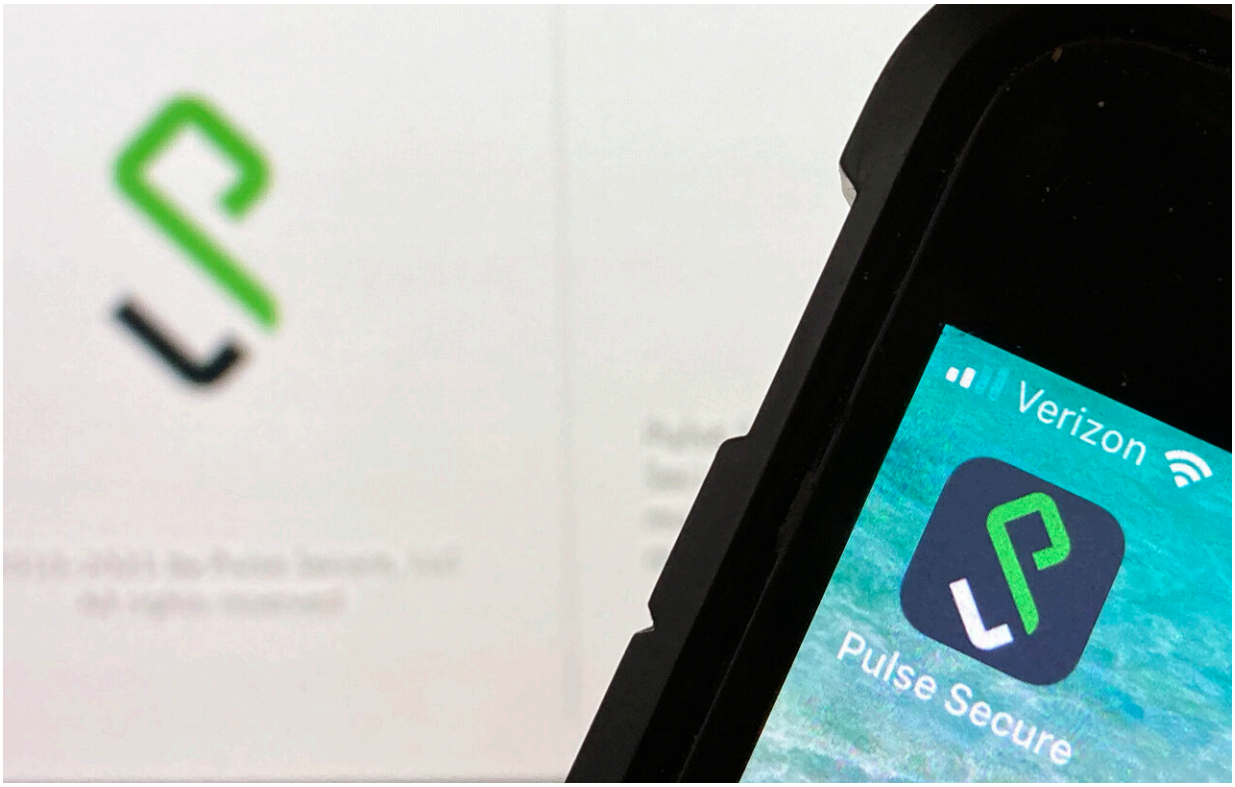
Critical entities targeted in suspected Chinese cyber spying

June 15 2021, by Alan Suderman



An Icon for the Pulse Secure smartphone app, right, and a computer desktop info page, left, are seen in Burke, Va., on Monday, June 14, 2021. Suspected state-backed Chinese hackers penetrated the computer systems of critical U.S. entities in what cybersecurity experts are calling a major Chinese cyberespionage campaign, an episode that's gone largely under the radar amid the clamor of worsening ransomware attacks. The campaign was carried out by exploiting the widely used Pulse Connect Secure networking devices. Pulse Secure is used by numerous companies and governments for secure remote access to their networks. Credit: AP Photo

A cyberespionage campaign blamed on China was more sweeping than previously known, with suspected state-backed hackers exploiting a device meant to boost internet security to penetrate the computers of critical U.S. entities.

The hack of Pulse Connect Secure networking devices came to light in April, but its scope is only now starting to become clear. The Associated Press has learned that the hackers targeted telecommunications giant Verizon and the country's largest water agency. News broke earlier this month that the New York City subway system, the country's largest, was also breached.

Security researchers say dozens of other high-value entities that have not yet been named were also targeted as part of the breach of Pulse Secure, which is used by many companies and governments for secure remote access to their networks.

It's unclear what sensitive information, if any, was accessed. Some of the targets said they did not see any evidence of data being stolen. That uncertainty is common in cyberespionage and it can take months to determine data loss, if it is ever discovered. Ivanti, the Utah-based owner of Pulse Connect Secure, declined to comment on which customers were affected.

But even if sensitive information wasn't compromised, experts say it is worrisome that hackers managed to gain footholds in networks of critical organizations whose secrets could be of interest to China for commercial and national security reasons.

"The threat actors were able to get access to some really high-profile organizations, some really well-protected ones," said Charles Carmakal,

the chief technology officer of Mandiant, whose company first publicized the hacking campaign in April.

The Pulse Secure hack has largely gone unnoticed while a series of headline-grabbing ransomware attacks have highlighted the cyber vulnerabilities to U.S. critical infrastructure, including one on a major fuels pipeline that prompted widespread shortages at gas stations. The U.S. government is also still investigating the fallout of the SolarWinds hacking campaign launched by Russian cyber spies, which infiltrated dozens of private sector companies and think tanks as well as at least nine U.S. government agencies and went on for most of 2020.

China has a long history of using the internet to spy on the U.S. and presents a "prolific and effective cyber-espionage threat," the Office of the Director of the National Intelligence said in its most recent annual threat assessment.

Six years ago Chinese hackers stole millions of background check files of federal government employees from the Office of Personnel Management. And last year the Justice Department charged two hackers it said worked with the Chinese government to target firms developing vaccines for the coronavirus and stole hundreds of millions of dollars worth of intellectual property and trade secrets from companies across the world.

The Chinese government has denied any role in the Pulse hacking campaign and the U.S. government has not made any formal attribution.

In the Pulse campaign, security experts said sophisticated hackers exploited never-before-seen vulnerabilities to break in and were hyper diligent in trying to cover their tracks once inside.

"The capability is very strong and difficult to defend against, and the

profile of victims is very significant," said Adrian Nish, the head of cyber at BAE Systems Applied Intelligence. "This is a very targeted attack against a few dozen networks that all have national significance in one way or another."

The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency, or CISA, issued an April alert about the Pulse hack saying it was aware of "compromises affecting a number of U.S. government agencies, critical infrastructure entities, and other private sector organizations." The agency has since said that at least five federal agencies have identified indications of potential unauthorized access, but not said which ones.

Verizon said it found a Pulse-related compromise in one of its labs but it was quickly isolated from its core networks. The company said no data or customer information was accessed or stolen.

"We know that bad actors try to compromise our systems," said Verizon spokesman Rich Young. "That is why internet operators, private companies and all individuals need to be vigilant in this space."

The Metropolitan Water District of Southern California, which provides water to 19 million people and operates some of the largest treatment plants in the world, said it found a compromised Pulse Secure appliance after CISA issued its alert in April. Spokeswoman Rebecca Kimitch said the appliance was immediately removed from service and no Metropolitan systems or processes were known to have been affected. She said there was "no known data exfiltration."

The Metropolitan Transportation Authority in New York also said they've not found evidence of valuable data or customer information was stolen. The breach was first reported by The New York Times.

Nish, the BAE security expert, said the hackers could have broken into networks but not stolen data right away for any number of operational reasons. He compared it to a criminal breaking into a house but stopping in the hallway.

"It's still pretty bad," Nish said.

Mandiant said it found signs of data extraction from some of the targets. The company and BAE have identified targets of the hacking campaign in several fields, including financial, technology and defense firms, as well as municipal governments. Some targets were in Europe, but most in the U.S.

At least one major local government has disputed it was a target of the Pulse Secure hack. Montgomery County, Maryland, said it was advised by CISA that its Pulse Secure devices were attacked. But county spokesman Scott Peterson said the county found no evidence of a compromise and told CISA they had a "false report."

CISA did not directly respond to the county's statement.

The new details of the Pulse Secure hack come at a time of tension between the U.S. and China. Biden has made checking China's growth a top priority, and said the country's ambition of becoming the wealthiest and most powerful country in the world is "not going to happen under my watch."