The Washington Post
Democracy Dies in Darkness

TECH POLICY

China's cyber army is invading critical U.S. services

A utility in Hawaii, a West Coast port and a pipeline are among the victims in the past year, officials say

By Ellen Nakashima and Joseph Menn
December 11, 2023 at 6:00 a.m. EST

The Chinese military is ramping up its ability to disrupt key American infrastructure, including power and water utilities as well as communications and transportation systems, according to U.S. officials and industry security officials.

Hackers affiliated with China's People's Liberation Army have burrowed into the computer systems of about two dozen critical entities over the past year, these experts said.

The intrusions are part of a broader effort to develop ways to sow panic and chaos or snarl logistics in the event of a U.S.-China conflict in the Pacific, they said.

Among the victims are a water utility in Hawaii, a major West Coast port and at least one oil and gas pipeline, people familiar with the incidents told The Washington Post. The hackers also attempted to break into the operator of Texas's power grid, which operates independently from electrical systems in the rest of the country.

Several entities outside the United States, including electric utilities, also have been victimized by the hackers, said the people, who spoke on the condition of anonymity because of the matter's sensitivity.

None of the intrusions affected industrial control systems that operate pumps, pistons or any critical function, or caused a disruption, U.S. officials said. But they said the attention to Hawaii, which is home to the Pacific Fleet, and to at least one port as well as logistics centers suggests the Chinese military wants the ability to complicate U.S. efforts to ship troops and equipment to the region if a conflict breaks out over Taiwan.

These previously undisclosed details help fill out a picture of a cyber campaign dubbed Volt Typhoon, first detected about a year ago by the U.S. government, as the United States and China struggle to stabilize a relationship more antagonistic now than it has been in decades. Chinese military commanders refused for more than a year to speak to American counterparts even as close-call intercepts by Chinese fighter jets of U.S. spy planes surged in the western Pacific. President Biden and Chinese President Xi Jinping agreed only last month to restore those communication channels.

“It is very clear that Chinese attempts to compromise critical infrastructure are in part to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to cause societal chaos inside the United States — to affect our decision-making around a crisis,” said Brandon Wales, executive director of the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). “That is a significant change from Chinese cyber activity from seven to 10 years ago that was focused primarily on political and economic espionage.”

Morgan Adamski, director of the National Security Agency’s Cybersecurity Collaboration Center, confirmed in an email that Volt Typhoon activity “appears to be focused on targets within the Indo-Pacific region, to include Hawaii.”

The hackers often sought to mask their tracks by threading their attacks through innocuous devices such as home or office routers before reaching their victims, officials said. A key goal was to steal employee credentials they could use to return, posing as normal users. But some of their entry methods have not been determined.

The hackers are looking for a way to get in and stay in without being detected, said Joe McReynolds, a China security studies fellow at the Jamestown Foundation, a think tank focused on security issues. “You’re trying to build tunnels into your enemies’ infrastructure that you can later use to attack. Until then you lie in wait, carry out reconnaissance, figure out if you can move into industrial control systems or more critical companies or targets upstream. And one day, if you get the order from on high, you switch from reconnaissance to attack.”

The disclosures to The Post build on the annual threat assessment in February by the Office of the Director of National Intelligence, which warned that China “almost certainly is capable” of launching cyberattacks that would disrupt U.S. critical infrastructure, including oil and gas pipelines and rail systems.

“If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide,” the assessment said.

Some of the victims compromised by Volt Typhoon were smaller companies and organizations across a range of sectors and “not necessarily those that would have an immediate relevant connection to a critical function upon which many Americans depend,” said Eric Goldstein, CISA’s executive assistant director. This may have been “opportunistic targeting … based upon where they can gain access” — a way to get a toehold into a supply chain in the hopes of one day moving into larger, more-critical customers, he said.

Chinese military officers have described in internal documents how they might use cyber tools or “network warfare” in a conflict, said McReynolds, who has seen some of the writings. He said military strategists speak of synchronizing air and missile strikes with disruption of command-and-control networks, critical infrastructure, satellite networks and military logistics systems.

They have talked about these tools applying in amphibious invasions, he said. “This is stuff they pretty clearly see as relevant to a Taiwan scenario,” he said, “though they don’t explicitly say this is how we’re going to take over Taiwan.”

This is far from China's first foray into hacking critical infrastructure. In 2012, a Canadian company, Telvent, whose software remotely operated major natural gas pipelines in North America, notified customers that a sophisticated hacker had breached its firewalls and stolen data relating to industrial control systems. The cybersecurity firm Mandiant traced the breach to a prolific PLA hacking group, Unit 61398. Five members of the unit were indicted in 2014 on charges of hacking U.S. companies.

At the time, the U.S. government wasn't sure whether China's aim was to collect intelligence or pre-position itself to disrupt. Today, based on intelligence collection and the fact that the facilities targeted have little intelligence of political or economic value, U.S. officials say it's clear that the only reason to penetrate them is to be able to conduct disruptive or destructive actions later.

Threat researcher Jonathan Condra of security company Recorded Future — which during the summer found Volt Typhoon probing the Texas grid — said the secrecy with which the Chinese have conducted the attacks argues against any notion that they wanted the United States to know their capabilities.

The hackers "were doing this a lot more stealthily than if they were trying to get caught," he said.

The U.S. government has long sought to improve coordination with the private sector, which owns most of the nation's critical infrastructure, and with tech companies that can detect cyberthreats. Companies such as Microsoft share anonymized information about adversary tactics, indicators that a system has been compromised, and mitigations, said CISA's Goldstein. Generally, these companies are not seeing the hacker's presence within the customer's networks, but rather are detecting it through communications to the servers the hacker is using to direct the attack, he said.

In some cases, the victims themselves seek assistance from CISA. In others, Goldstein said, CISA is alerted by a software or communications vendor to a victim and the government must seek a court order to compel the vendor to reveal the victim's identity.

In May, Microsoft said it had found Volt Typhoon infiltrating critical infrastructure in Guam and elsewhere, listing a number of sectors. Those included telecommunications firms, according to people familiar with the matter. The hacks were especially concerning, analysts said, because Guam is the closest U.S. territory to the contested Taiwan Strait.

The intrusions into sectors such as water and energy systems come as the Biden administration has sought to strengthen industries' ability to defend themselves by issuing mandatory cybersecurity rules. In the summer of 2021, the administration rolled out first-ever oil and gas pipeline cyber regulations. In March, the Environmental Protection Agency announced a requirement for states to report on cyberthreats in their public water system audits. Soon after, however, three states sued the administration, charging regulatory overreach.

The EPA pulled back the rule and has asked Congress to act on a regulation. In the meantime, the agency must rely on states to report threats voluntarily.

In a joint advisory issued in May, the Five Eyes intelligence alliance of the United States, Britain, Canada, Australia and New Zealand offered advice on how to hunt for the intruders. One of the challenges is the hackers' tactic of evading detection by firewalls and other defenses by using legitimate tools so that the hackers' presence blends in with normal network activity. The technique is called "living off the land."

"The two toughest challenges with these techniques are determining that a compromise has occurred, and then once detected, having confidence that the actor was evicted," said the NSA's Adamski, whose Cybersecurity Collaboration Center coordinates with private industry.

The NSA and other agencies recommend mass password resets and better monitoring of accounts that have high network privileges. They have also urged companies to require more secure forms of multifactor authentication, such as hardware tokens, rather than relying on a text message to a user's phone, which can be intercepted by foreign governments.

Despite the heightened scrutiny growing out of the May advisory, the hackers persisted, seeking new targets.

In August, according to Recorded Future, the hackers attempted to make connections from infrastructure that had been used by Volt Typhoon to internet domains or subdomains used by the Public Utility Commission of Texas and the Electric Reliability Council of Texas, which operates that state's electric grid. Though there is no evidence the attempts succeeded in penetrating the system, the effort highlights the kinds of targets the Chinese military is interested in. The two Texas agencies declined to answer questions about the incidents from The Post.

The Reliability Council said it works closely with federal agencies and industry groups and that it has redundant systems and controlled access as part of a "layered defense."

In the weeks leading up to the Biden-Xi meeting last month, NSA officials speaking at industry conferences repeated the call to the private sector to share information on hacking attempts. The NSA can peer into adversaries' networks overseas, while U.S. companies have visibility into domestic corporate networks. Together, industry and government can have a fuller picture of attackers' goals, tactics and motives, U.S. officials say.

China "is sitting on a stockpile of strategic" vulnerabilities, or undisclosed security flaws it can use in stealthy attacks, Adamski said last month at the CyberWarCon conference in Washington. "This is a fight for our critical infrastructure. We have to make it harder for them."

The topic of Chinese cyber intrusions into critical infrastructure was on a proposed list of talking points to raise in Biden's encounter with Xi, according to people familiar with the matter, but it did not come up in the four-hour meeting.