EXCLUSIVE CYBERSECURITY

U.S. Wiretap Systems Targeted in China-Linked Hack

AT&T and Verizon are among the broadband providers that were breached

By Sarah Krouse , Dustin Volz , Aruna Viswanatha and Robert McMillan

Updated Oct. 5, 2024 12:12 am ET

CHINA'S MULTIPRONGED SPYING OPERATIONS HAVE DRAWN WARNINGS IN THE U.S. ABOUT THEIR ECONOMIC IMPLICATIONS.

A cyberattack tied to the Chinese government penetrated the networks of a swath of U.S. broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests.

For months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful U.S. requests for communications data, according to people familiar with the matter, which amounts to a major national security risk. The attackers also had access to other tranches of more generic internet traffic, they said.

Verizon Communications, AT&T and Lumen Technologies are among the companies whose networks were breached by the recently discovered intrusion, the people said.

The widespread compromise is considered a potentially catastrophic security breach and was carried out by a sophisticated Chinese hacking group dubbed Salt Typhoon. It appeared to be geared toward intelligence collection, the people said.

Spokesmen for AT&T, Verizon and Lumen declined to comment on the Salt Typhoon campaign.

Companies are generally required to disclose material cyber intrusions to securities regulators within a short time, but in rare cases, federal authorities can grant them an exemption from doing so on national security grounds.

The surveillance systems believed to be at issue are used to cooperate with requests for domestic information related to criminal and national security investigations. Under federal law, telecommunications and

broadband companies must allow authorities to intercept electronic information pursuant to a court order. It couldn't be determined if systems that support foreign intelligence surveillance were also vulnerable in the breach.

The attack and its significance was discovered in recent weeks and remains under active investigation by the U.S. government and private-sector security analysts. Investigators are still working to confirm the breadth of the attack and the degree to which the actors observed data and exfiltrated some of it, the people said.

VERIZON IS AMONG THE COMPANIES WHOSE NETWORKS WERE BREACHED BY A RECENTLY DISCOVERED INTRUSION.

The hackers appear to have engaged in a vast collection of internet traffic from internet service providers that count businesses large and small, and millions of Americans, as their customers. Additionally, there are indications that the hacking campaign targeted a small number of service providers outside the U.S., the people said.

A person familiar with the attack said the U.S. government considered the intrusions to be historically significant and worrisome.

Senior U.S. officials have for years warned about the economic and national security implications of China's multipronged spying operations, which can take the form of human espionage, business investments and high-powered hacking operations.

More recently officials have been alarmed by alleged efforts by Chinese intelligence officers to burrow into vulnerable U.S. critical infrastructure networks, such as water-treatment facilities, power stations and airports. They say the efforts appear to be an attempt by hackers to position themselves in such a way that they could activate disruptive cyberattacks in the event of a major conflict with the U.S.

The Salt Typhoon campaign adds another piece to the puzzle.

Investigators are still probing the origins of the Salt Typhoon attack and are exploring whether the intruders gained access to Cisco Systems routers, core network components that route much of the traffic on the internet, The Wall Street Journal previously reported. A Cisco spokeswoman said earlier that the company is looking into the matter but has received no indication that Cisco routers were involved. The spokeswoman didn't immediately respond to a request for comment Friday.

China has routinely denied allegations from Western governments and technology companies that it relies on

China has routinely denied allegations from Western governments and technology companies that it relies on hackers to break into foreign government and business computer networks.

In a statement, Liu Pengyu, a spokesman at the Chinese Embassy in Washington, said: “China firmly opposes and combats cyberattacks and cyber theft in all forms.”

Microsoft is investigating the new Salt Typhoon intrusion along with other cybersecurity companies and what sensitive information might have been accessed. Microsoft helps companies respond to cyber intrusions using data from its vast, globe-spanning network of hardware and software and has assigned some China-linked campaigns the Typhoon moniker.

MICROSOFT SAID MOST OF SALT TYPHOON'S TARGETS WERE BASED IN NORTH AMERICA AND SOUTHEAST ASIA.

“It will take time to unravel how bad this is, but in the meantime it’s the most significant in a long string of wake-up calls that show how the PRC has stepped up their cyber game,” said Brandon Wales, former executive director at the Cybersecurity and Infrastructure Security Agency and now a vice president at SentinelOne, referring to the People’s Republic of China. “If companies and governments weren’t taking this seriously before, they absolutely need to now.”

Salt Typhoon has been active since 2020 and is a nation-state hacking group based out of China that focuses on espionage and data theft, particularly capturing network traffic, Microsoft said in a research note written in August. “Most of Salt Typhoon’s targets are based in North America or Southeast Asia,” Microsoft said, noting that other cybersecurity companies call the group GhostEmperor and FamousSparrow.

The cybersecurity firm ESET calls this group FamousSparrow and says it has previously broken into hotels and government agencies worldwide.

U.S. officials in September said they had disrupted a network of more than 200,000 routers, cameras and other internet-connected consumer devices that served as an entry point into U.S. networks for a China-based hacking group called Flax Typhoon. In January, federal officials disrupted Volt Typhoon, another China-linked campaign that has sought to infiltrate a swath of critical U.S. infrastructure.

U.S. officials warned that Volt Typhoon appeared largely focused on gaining access into networks to later detonate cyberattacks that could cripple operations of infrastructure.

Drew FitzGerald contributed to this article.

Write to Sarah Krouse at sarah.krouse@wsj.com, Dustin Volz at dustin.volz@wsj.com, Aruna Viswanatha at aruna.viswanatha@wsj.com and Robert McMillan at robert.mcmillan@wsj.com