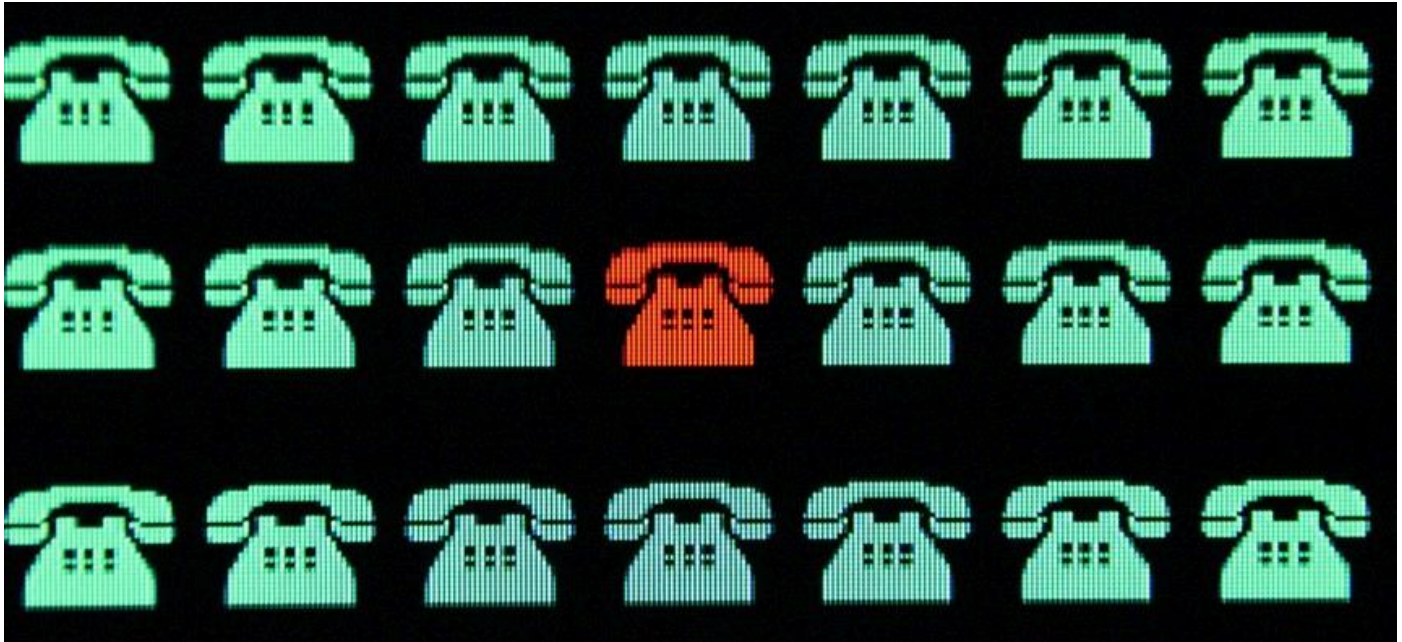


## Chinese telecom espionage began with ‘much broader’ aims, officials say



HAILSHADOW/GETTY IMAGES

By DAVID DIMOLFETTA // DECEMBER 3, 2024

The U.S. has been investigating the Salt Typhoon hackers since late spring and early summer this year, a senior FBI official said.

CYBER THREATS   FBI   NSA



A prolific Chinese hacking group launched sweeping intrusions into U.S. telecom networks with “much broader” aims than just compromising the systems that facilitate court-authorized wiretap requests, a senior FBI official said Tuesday.

National security and law enforcement intercepts — which monitor, capture and collect communications data as they are transmitted — were just one of several targets the hacking collective, dubbed Salt Typhoon, sought to exploit, said the official, who spoke on background under press guidelines issued in a Tuesday news conference.

The Wall Street Journal [first brought](#) Salt Typhoon’s campaign to light in October. The group used [sophisticated methods](#) to penetrate dozens of telecom firms inside and outside the U.S. over the course of several months. The hackers have not been entirely jettisoned from the networks, said the FBI official, as well as Jeff Greene, the executive assistant cybersecurity director at the Cybersecurity and Infrastructure Security Agency.

The revelations about Salt Typhoon’s targets lay bare the hackers’ sophisticated operation aimed at accessing the backbone of U.S. spying systems used for tracking critical individuals at home and possibly abroad. The intrusions were first investigated in late spring and early summer of this year, the senior FBI official said.

engineered their system for regular access, but remained requests — had access to the penetration, but not necessarily the initial entry vector used by the hackers in all cases, said the senior FBI official.

Forensic analysis for two of the victims “indicated that the actors were on other parts of their network conducting reconnaissance before pivoting to the CALEA system and surrounding devices,” the FBI official said.

The official declined to categorize which systems governed by the Foreign Intelligence Surveillance Act, or FISA, were accessed, but noted that CALEA includes court orders for Title I of FISA, which allows the U.S. to electronically surveil foreign powers and their agents, including Americans acting as agents of a foreign power.

Other FISA systems, such as the [controversial](#) Section 702 ordinance, allow the U.S. to target non-U.S. persons abroad without a warrant by compelling communications firms to hand over conversations on that target, which are then stored in query databases for investigations. Beijing could glean insights into highly classified 702 matters if Salt Typhoon had successfully peered into those environments.

CALEA is a [30-year-old legal protocol](#) that has become a mainstay in law enforcement’s surveillance toolkit, but hasn’t undergone a formal update since the Federal Communications Commission last reviewed it in 2005.

Wiretaps have evolved from physically tapping analog phone lines to remotely intercepting digital communications across multiple channels, including calls, texts and internet traffic. The FCC does [not yet appear](#) poised to launch a formal proceeding to rework CALEA, despite calls from Congress to do so in the wake of the intrusions.

So far, the cyberspies have ensnared around 80 providers in the U.S. and abroad, including AT&T, Verizon, Lumen and T-Mobile. They’ve accessed communications of some 150 select, high-value targets, including people affiliated with President-elect Donald Trump, according to previous media reports.

Overseas servers were used to springboard the hackers into some telecom providers’ networks, said the senior FBI official, though they did not break down the specificity of each intrusion and what servers were exploited.

On Tuesday, American cybersecurity and intelligence agencies and their international partners also released a playbook aimed at helping communications operators protect their facilities from further cyberattacks.

The [guidance](#) from CISA, the FBI, the NSA and counterparts in Australia, Canada and New Zealand, shed light on the overlapping techniques and methods that the Chinese operatives used for their break-ins.

The agencies in the document said they’ve observed “Cisco-specific features often being targeted by, and associated with, these PRC cyber threat actors’ activity,” confirming [earlier reports](#) that the hackers leveraged Cisco router vulnerabilities to get into the networks.

They recommended companies using Cisco devices set stronger, more secure passwords. The guide also advised turning off Telnet, a feature that allows administrators to send keystrokes from one device to another when managing multiple servers.

Network engineers are advised to use a separate network for managing devices that is completely isolated from the main operational networks backing their systems. All blocked, inbound traffic should also be logged for later analysis, it said.

Many of the breached systems were [not properly equipped](#) with logging mechanisms to monitor device activity, *Nextgov/FCW* previously reported.

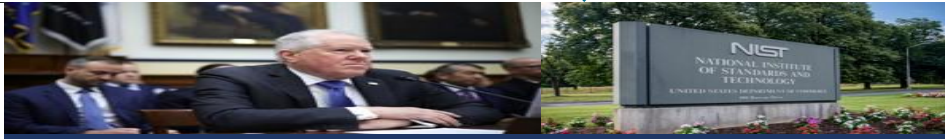
“While there were some commonalities and some common threads, they were not locked into a single playbook here,” a person with knowledge of the hacks previously said, describing how Salt Typhoon carried out the operation.

Hackers can obtain system access credentials through a variety of ways. Operatives may spin up fabricated, plausible-sounding emails that can trick recipients into handing over sensitive account information. Other data may be obtained through sales on dark web forums and similar unpatrolled areas of the internet that often serve as marketplaces for stolen log-in data, personal information and other illicit materials.

“We definitely need to look at what this means long term — how we secure our networks [and] how we work with our telecommunications partners,” Greene said, later adding that “we cannot say with certainty that the adversary has been evicted, because we still don’t know the scope of what they’re doing.” [N](#)

Share This:

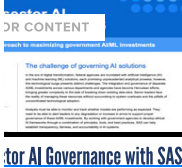




Operators must be held accountable for AI's use in conflicts, Air Force secretary says Why NIST is prioritizing creating a dictionary of AI development



ictures tech shop to center on the CIO How a push to the cloud helped a Ukrainian bank keep faith with customers amid war The people problem behind the government's AI ambitions



for AI Governance with SAS

# US proposes rule to prevent the sale of financial data to foreign adversaries

SANKAI/GETTY IMAGES

By **DAVID DIMOLFETTA** // DECEMBER 3, 2024

Data brokers would have to comply under terms set by the Fair Credit Reporting Act, in an effort that aims to stop exploitation of Americans' data overseas.

DATA GOVERNANCE

INTERNATIONAL

PRIVACY



The Consumer Financial Protection Bureau on Tuesday proposed a long-anticipated rule that would require data brokers to comply with credit bureau reporting standards, in an effort to prevent Americans' financial data from being obtained by foreign rivals and cybercriminals that may use the information for intelligence gathering and exploitation.

reporting, next steps also require these lenders to institute protections for personal identifiers used in credit reports — such as income or a FICO score — and mandate explicit consumer consent for sharing credit data.

The proposal — first floated in April by agency chief Rohit Chopra — was born out of an [executive order](#) signed by President Joe Biden earlier this year, which was focused on preventing Americans' sensitive personal data from falling into the hands of foreign adversaries.

The Fair Credit Reporting Act was enacted in 1970 to ensure accuracy, fairness and privacy in the collection and use of consumer credit information. It grants consumers rights to access and dispute their credit reports, limits who can access this data and regulates credit reporting agencies with enforcement by the federal government and state attorneys general.

The data broker industry collects and sells detailed information about individuals and packages their everyday habits and behaviors into data points that are used for targeted advertising, credit scoring, risk assessments and other commercial matters. The CFPB contends that national security threats against the U.S. would increase if such data were to be obtained by nation-state spies or cybercrime operatives.

The dynamic also presents personal safety risks for vulnerable populations, law enforcement, judges and domestic violence survivors, whose sensitive information can be easily purchased and misused, the agency argued.

"Today's proposed rule is a major step forward to ensure that companies trafficking in Americans' most sensitive information face real consequences for violating long-standing law and for putting people and our country at risk," CFPB head Rohit Chopra said in a news conference with reporters.

The Biden administration is seeking to prohibit transactions that data brokers make to "countries of concern" on grounds that such data can be surreptitiously processed by foreign hackers or spies, enabling myriad national security risks and exposing American citizens to surveillance, blackmail and other privacy violations. A separate DOJ rulemaking proposal tied to the executive order was released in October.

A coalition of former officials and groups representing federal employees and military servicemembers last month [pressed CFPB](#) to adequately address national security risks tied to the collection, aggregation and sale of Americans' personal data by data brokers.

"The sale of Americans' financial data is particularly valuable to malicious actors, because it provides exploitable insights — that in some cases, are not found elsewhere — into personal debts, gambling problems, marital fissures, overseas bank accounts, and other sensitive matters that can be opportunities for blackmail, pressure, and recruitment," wrote the group.


A CFPB official, who spoke on background per agency-set guidelines, said that sensitive financial data could be used to target victims more precisely. For instance, a U.S. military member with a low credit score may be targeted with a phishing email, aiming to trick them into handing over data that may improve their creditworthiness, when in reality, the scam would steal their personal information or classified workplace assets.

"The CFPB developed this proposed rule based on extensive market monitoring that revealed widespread evasion of consumer protections," the agency said in a press release Tuesday. "The agency found that data brokers routinely sidestep the [Fair Credit Reporting Act] by claiming they aren't subject to its requirements — even while selling the very types of sensitive personal and financial information Congress intended the law to protect."

An [investigation](#) last month revealed that practically anyone could purchase data that maps the day-to-day patterns of U.S. military servicemembers and intelligence analysts in Germany, as well as contractors that worked on-site at sensitive locations. Last year, Duke University researchers said they were able to [purchase reams of sensitive data](#) on American servicemembers and their families for as little as 12 cents per record.

Myriad hacking incidents over the past decade have exposed the personal data of federal employees, military members and ordinary Americans. An infamous breach of the Office of Personnel Management that surfaced in 2015 helped galvanize attention to the issue after hackers pilfered data on millions of current and former federal workers.

A well-documented 2017 hack at Equifax also compromised the data of some 150 million Americans and received harsh congressional oversight. It was later attributed to Chinese nation-state operatives.

The agency is seeking comments on the proposed rule before March 3 of next year, requiring the incoming GOP administration to oversee its implementation after President-elect Donald Trump takes office in January. The CFPB official said there is "broad bipartisan recognition that data brokers pose real dangers, both to Americans' privacy and to national security." 

Share This:

