Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated January 23, 2025

Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications

In early October 2024, media outlets reported that People's Republic of China (PRC) state-sponsored hackers infiltrated United States telecommunications companies (including internet service providers). The U.S. government has since confirmed both the PRC's actions and the existence of an ongoing investigation into the hacks. This is not the first time that the PRC has attacked the U.S. communications sector—and reflects a pattern of targeting the sector for both its role in enabling other sectors, and also the value of the systems and data contained within the sector itself.

The methods used by the PRC hackers in the attack have not been publicly disclosed, nor have the specific systems or data that were targeted. But, public reporting suggests that the hackers may have targeted the systems used to provide court-approved access to communication systems used for investigations by law enforcement and intelligence agencies. PRC actors may have sought access to these systems and companies to gain access to presidential candidate communications. With that access, they could potentially retrieve unencrypted communication (e.g., voice calls and text messages).

In January 2025, the U.S. government sanctioned a PRC-based individual and cybersecurity company for their alleged role in enabling the Salt Typhoon hacks.

This In Focus discusses PRC cyber actors as well as broader cybersecurity and risk management considerations for Congress.

PRC Hackers: The Typhoons

The U.S. Intelligence Community (IC) assesses that the PRC is "the most active and persistent cyber threat" to U.S. institutions. The Office of the National Cyber Director has highlighted China's ambitions "to hold at risk U.S. and allied critical infrastructure, shape U.S. decision-making in a time of crisis, and use cyber capabilities to augment PRC geopolitical objectives."

Typhoon is the moniker Microsoft Corporation assigns to attributed threat actors with PRC state sponsorship—a moniker the U.S. government also adopts. There are three publicly disclosed Typhoon threat actor groups.

- ***Volt Typhoon*.** These actors use a technique known as *living off the land*, which involves using built-in tools on the target network to execute objectives without installing malware (which may be detected). Volt Typhoon has been known to target United States critical infrastructure entities. The IC assesses that Volt Typhoon's targeting of these companies carries limited espionage potential, and is instead part of an effort to prepare to disrupt U.S. infrastructure.
- ***Flax Typhoon*.** These actors are associated with PRC information security companies that take directions from the PRC government. They target Taiwan and U.S. critical infrastructure domestically and abroad. Flax Typhoon actors also use living off the land techniques, and have compromised hundreds of internet-of-things (IOT) devices to create a botnet that they used to carry out attacks. The U.S. government said that it had disrupted one such botnet in September 2024.
- ***Salt Typhoon.*** These actors are reportedly responsible for the compromise of U.S. telecommunications companies reported in October 2024. They are being investigated for attacking telecommunications companies, stealing customer communications and law enforcement information, and targeting political figures.

Considerations for Policymakers

Members of Congress in the House and Senate have expressed concerns over these breaches and have called on U.S. companies and federal agencies to provide information about the incident. Congress might also consider oversight of the executive branch's response, particularly the immediate response and discovery of the incident, as the incident raises concerns about the privacy of Americans' communications, the security of critical infrastructure, and cybersecurity deterrence policy. There are other areas policymakers may be interested in, such as the role and use of the Cyber UCG, the Cyber Safety Review Board (CSRB), Sector Risk Management Agencies (SRMAs), and preparedness activities.

Cyber UCGs

The concept of a Cyber UCG comes from Presidential Policy Directive 41 (PPD-41) and its accompanying annex, which states that a Cyber UCG is to be stood up under the auspices of the National Security Council (NSC) to "coordinate the development and implementation of United States Government policy and strategy with respect to significant cyber incidents affecting the United States or its

interests abroad." Recent Cyber UCGs have been used in events to coordinate whole-of-government responses that integrate with private sector companies. In certain incidents, a Cyber UCG may be necessary to assure a coordinated response: while agencies have different authorities and capabilities to bring to bear to respond to an event, they may lack mechanisms to share information, leverage external resources, and deconflict agency activity.

By publicly available counts, this is the fourth time that the U.S. government has established a Cyber UCG—which were previously established for China's compromise of Microsoft Exchange services in 2021, Russia's compromise of SolarWinds in 2021, and to facilitate domestic preparedness and response to the Russian-Ukraine war in 2023. It is not clear if Cyber UCGs were established for the Colonial Pipeline, Change Healthcare, or Log4j incidents.

Congress may choose to examine Cyber UCG operations and provide specific authorities for its use. While the Cyber UCG is established by presidential action, it is not required by statute. The criteria for establishing one is equivocal and inconsistently applied. Further, there are multiple triggering definitions agencies might consider: *major* and *significant* incidents. Major incidents are required to be reported to Congress, while significant incidents are not. The establishment of a Cyber UCG does not have to be announced or reported.

Congress could choose to debate whether to authorize the Cyber UCG, which federal entity should operate it, which agencies should participate, what coordinating authorities it has, and what the criteria are for when one is stood up and disbanded. Congress could also allow the Cyber UCG to continue to operate under, and at the discretion of, the NSC.

Cyber Safety Review Board

The CSRB was created by presidential action and is supposed to stand up for events in which a Cyber UCG is established. The CSRB is charged with examining: the incident; related activities; and agency responses so that the government and private sector can learn from the incident and improve operations. This is similar to—but, not exactly like—the investigations conducted by the National Transportation Safety Board. Despite having Cyber UCGs for the Microsoft Exchange server and SolarWinds compromises, CSRBs were not established. The latest CSRB report was on the 2023 Microsoft Exchange Online incident. There has been no announcement of the Board's next review. Media reports state that the CSRB will examine this incident, but the timing is unknown.

Congress has examined the CSRB and may choose to further debate its existence, authorities, and jurisdiction. Of particular interest could be the Board's makeup, how it maintains independence in reviews, the criteria for starting a review, and what instruments are available to implement their recommendations. Further, Congress may choose to expand or contract the CSRB's cybersecurity focus to include foreign relations, deterrence, and elections security.

Sector Risk Management Agencies

SRMAs are federal agencies responsible for coordinating risk management activities with their respective critical infrastructure sectors. Congress established SRMAs to, among other responsibilities, identify sectoral threats and support incident response. The Cybersecurity and Infrastructure Security Agency (CISA) is the SRMA for the communications sector (in which the firms hacked by Salt Typhoon belong).

Congress may choose to further examine, clarify, and define SRMAs' roles in cybersecurity risk management. Factors for consideration could include the extent to which SRMAs understand sector companies and their vendor relationships (e.g., supply chain); the frequency and type of information SRMAs collect, analyze, and disseminate to the sector; the ways in which SRMAs coordinate with one another and other federal agencies; and SRMA responsibilities in incident response. For the communications sector, the Emergency Support Function #2 Annex is supposed to provide a response framework. However, being nearly a decade old, it does not include some current organizations and has responsibilities for others that no longer exist.

Preparedness

Preparedness generally refers to the capabilities necessary to prevent, protect, respond, and recover from threats. Congress repeatedly directed CISA to engage in the explicit preparedness activities of planning and conducting exercises.

Planning and exercising helps to engage stakeholders in thinking through incidents; establish and understand roles and responsibilities; understand capabilities and operations; and develop a shared sense of actions and outcomes.

CISA developed a cyber incident response plan at the end of the Obama Administration and is required to update that plan by the end of 2024. CISA also conducts biennial exercises with federal and nonfederal stakeholders to inform preparedness activities and decisionmaking.

With regard to the communications sector, entity participation in preparedness efforts appear to be primarily focused on their role as an essential service to other sectors (e.g., energy and financial services). Despite IC warnings of adversary intent to target and disrupt the communications sector, U.S. government's focus on the sector's inherent risk (rather than as an enabling sector) is not as evident in these efforts.

Congress may choose to consider CISA's preparedness activities for the communications sector as its SRMA. Particular areas of interest may include how CISA incorporates changes in the sector, federal organizations, and threat actors into preparedness activities; and incorporating lessons learned into how future hacks of telecommunications companies are identified, disclosed (to both Congress and the public), and managed.

Chris Jaikaran, Specialist in Cybersecurity Policy

Disclaimer