# Impersonating Power: China's APT41 Targets U.S. Trade Officials Amid High-Stakes Negotiations

September 10, 2025

**As U.S.–China trade talks intensify in 2025, the digital battlefield has opened a new front. State-backed hackers linked to Beijing have mounted a sophisticated campaign of impersonation and spear-phishing, aiming to penetrate the inner circle of American trade policy. By exploiting trust in familiar names and institutions, China's prolific APT41 group sought to steal sensitive data and shape the contours of ongoing negotiations — a reminder that today, diplomacy is as much about defending networks as it is about negotiating across the table.**

The latest wave of cyberespionage targeting U.S. trade policy circles has once again been attributed to APT41, a prolific Chinese state-backed hacking group long associated with both espionage and financially motivated activity. According to congressional warnings and investigative reporting, the operation unfolded in July 2025, just ahead of U.S.–China trade talks in Sweden, and was designed to compromise key nodes of American decision-making.

The attackers impersonated Rep. John Moolenaar, chairman of the House Select Committee on the Chinese Communist Party and a vocal Beijing critic, sending emails from a non-government account to U.S. government agencies, law firms, think tanks, trade associations, and at least one foreign government. The messages requested urgent feedback on draft sanctions legislation, urging recipients that their “insights are essential.” The attachment, however, contained malware linked to APT41, capable of establishing entrenched access and siphoning sensitive data through covert channels. Investigators found that the group abused cloud services and developer tools to disguise exfiltration routes, a hallmark of their evolving tactics.

**Info**

**The United States House Select Committee on Strategic Competition** between the United States and the Chinese Communist Party is a selected committee of the United States House of Representatives established in the 118th Congress, on January 10, 2023. The committee focuses on American economic and security competition with the People's Republic of China, which is ruled by the Chinese Communist Party (CCP). The committee is chaired by Representative John Moolenaar of Michigan, a member of the Republican Party. its purpose is to "investigate and submit policy recommendations on the status of the Chinese Communist Party’s economic, technological, and security progress and its competition with the United States"

💡

APT41’s involvement fits into a longer pattern of Chinese offensive cyber operations. The group, tracked since 2012 and known by aliases such as Double Dragon and Winnti, has targeted logistics, healthcare, utilities, and high-tech industries. Its methods include software supply chain compromises, bootkits, malicious certificates, and even the abuse of platforms like Google Calendar for espionage. While espionage remains its primary mission, members have also engaged in financially motivated hacking, underscoring the blurred lines between state and criminal operations. In 2019 and 2020, the FBI indicted five of its operatives, who remain fugitives.

The impersonation of a sitting lawmaker marked an escalation in both ambition and symbolic weight. By choosing Moolenaar — a known adversary of Beijing — as a persona, the attackers lent urgency and legitimacy to their messages, increasing the likelihood of quick responses. Experts noted that adversaries often bypass official channels by exploiting personal or non-

official accounts, making detection far more difficult. The attack echoes earlier 2025 campaigns, including January spear-phishing attempts against committee staffers posing as a representative of ZPMC, a Chinese state-owned crane manufacturer.

That earlier incident was not without context. In September 2024, the committee had published a report warning that ZPMC's dominance in the ship-to-shore crane market could serve as a "Trojan horse," giving Beijing covert access to U.S. port operations and maritime technology. The impersonation of ZPMC officials in phishing campaigns was seen as a natural extension of this strategy — embedding cyber intrusions into economic and industrial leverage. By September 2025, the impersonation of congressional leadership demonstrated how China-linked actors were applying the same playbook to legislative processes themselves.

This most recent campaign was exposed on September 7 by the Wall Street Journal, which revealed that trade groups and government bodies had received the weaponized emails. The following day, the House Select Committee publicly warned of "ongoing" China-linked operations and confirmed FBI involvement in the investigation. While the extent of successful compromises remains unclear, the episode underscores Beijing's relentless pursuit of sensitive U.S. deliberations, particularly when high-stakes trade and foreign policy negotiations are underway.

For Washington, the message was clear: cyber intrusions are no longer limited to industrial espionage or covert collection, but now directly exploit the democratic process itself. The continuity between port cranes, supply chain compromises, and political impersonation shows a coherent strategy — one where digital operations are weaponized to give Beijing asymmetric leverage in negotiations. The Chinese Embassy in Washington rejected the allegations, insisting that China opposes cyberattacks and accusing the U.S. of smearing without evidence. Yet the timing, methods, and repeated targeting strongly reinforced what outside analysts and investigators already assess: that cyberespionage has become a core instrument of statecraft in the U.S.–China rivalry.