The NATIONAL INTEREST FOUNDATION

Several U.S. Federal Agencies are Hacked by Entities Tied to the Russian Government

Hackers linked to the Russian government are believed to be behind the breach of computer systems at multiple U.S. federal agencies – including the Treasury Department, the Pentagon, and the Department of Homeland Security. The infiltration may have lasted for months before its recent uncovering, with hackers breaking into the networks by inserting a vulnerability in the updates of a software company which sells technology products to a wide array of federal agencies. The compromise was discovered when the individuals successfully logged into a top cybersecurity firm's network, tipping them off to the broader efforts aimed at the U.S. government. This latest cyberattack appears to be one of the most significant breaches in years and is especially concerning due to the time that it took to unearth. Analysts suspect that the hackers had months of access to internal email accounts in at least a dozen federal agencies during the course of their overall campaign.

According to officials, the hackers belong to a Russian government-affiliated group called Cozy Bear which has ties to the Russian intelligence apparatus. The entity is no stranger to initiating breaches on U.S. government targets, as they were previously behind the 2014 hack of the White House and State Department networks as well as the hack against the Democratic National Committee and Hillary Clinton staffers during her 2016 presidential campaign. Following that election, Cozy Bear was also linked to a series of coordinated phishing campaigns aimed at U.S.-based think tanks and non-governmental organizations. The group is also believed to be the source of recent attacks on several organizations working on developing COVID-19 vaccines.

The latest cyberattack campaign directed at the U.S. federal agencies is thought to have begun as far back as March of this year, when the hackers were able to insert malware into software updates which gave them access to computer systems. Therefore, at a time when the U.S. government was largely focused and preoccupied with detecting possible Russian interference in the presidential election, it seems as though Russian government-linked hackers were stealthily using that distraction to their advantage in order to open the door for them to infiltrate the computer networks of several notable federal agencies. Upon the recent discovery of the breach, all federal civilian agencies were ordered by the U.S. Cybersecurity and Infrastructure Security Agency to review their networks and immediately disconnect the type of software product that was utilized by the hackers.

In the days following the uncovering of the breach, officials are still working to try and understand the scope of the damage done. House and Senate Intelligence Committee members have been briefed on the cyberattack, however the full extent of it is still being pieced together. One of the most important factors to determine is whether or not the affected systems remain accessible to the hackers. Ultimately, cybersecurity experts are hoping that the incident serves as a warning for the incoming Biden administration about the serious threat of foreign government-linked actors continuing to conduct similar attacks in the future.