January 24, 2024

# The Microsoft Russian Hack Raises Major Questions for Policymakers

By Merrick Carey

In a legally required filing, Microsoft on January 19 disclosed that senior executives' e-mail accounts had been hacked by "a nation-state associated threat actor" widely believed to be Nobelium, a cybercriminal group affiliated with Russia's government. This is the same group behind the 2015-16 attack on the Democratic National Committee and 2020 SolarWinds attack, which led to data breaches in the federal government and thousands of organizations.

The incident is disturbing on a stand-alone basis. This is compounded by Nobelium's resilience and aggressiveness and the threats posed to U.S. commerce and national security.

Among the major questions that the federal government executive agencies should be asking about the latest cyber-breach incident at Microsoft are the following.

1. Were any government agencies impacted by this latest Nobelium attack?

2. What specific steps has Microsoft taken to protect its national security customers since this latest (apparently) Russian breach?

3. Was the January 12th intrusion at Microsoft a particularly difficult one to detect?

4. There was a long period between breach and detection. Why?

5. Were similar tactics used in this attack as in the summer 2023 hack that stole State Department emails?

6. Why is Nobelium so hard to block?

About the Author: Merrick "Mac" Carey is Chief Executive Officer of the Lexington Institute, a public policy think tank based in Arlington, VA.