HAFNIUM Compromises MS Exchange Servers

In March 2021, cyber security professionals began reporting on a cyber espionage campaign exploiting four zero-day (previously unknown and unpatched) vulnerabilities in Microsoft's Exchange Server e-mail software. This campaign gave the hackers persistent access to tens of thousands of victim organizations and allowed them to seize control of enterprise networks, thereby enabling follow-on operations.

On 2 March 2021, Microsoft released emergency security updates and remediation instructions to combat the campaign conducted by hackers it dubbed HAFNIUM. Microsoft had previously observed the group's activities and judged HAFNIUM to be based in China and benefitting from state sponsorship. Cyber security reports also refer to this HAFNIUM campaign as ProxyLogon.

On 19 July 2021, the U.S. Government publicly attributed these attacks with high confidence to malicious cyber actors affiliated with the People's Republic of China's Ministry of State Security (PRC MSS). The European Union, the United Kingdom, Australia, Canada, New Zealand, Japan, and NATO joined the United States in condemning the PRC's role in malicious cyber activities.

- **Type:** Global-scale cyber espionage and persistent access.
- **Vector:** Multiple vulnerabilities in Microsoft Exchange Server software.
- **Impact:** PRC MSS-affiliated cyber operators compromised tens of thousands of computers and networks worldwide, resulting in significant remediation costs for mostly private sector victims.
- **Mitigations:** As announced April 2021, the U.S. Government conducted cyber operations and pursued proactive network defense actions to prevent systems compromised through the Exchange Server vulnerabilities from being used for malicious purposes.