



NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

OPM Breach: Reinforces Threat From Cyber Foes

June 5, 2015

China's ability to access four million federal employees' personal information within the US Office of Personnel Management (OPM)—including social security numbers, job assignments, performance ratings, and training history—highlights Beijing's status as the US's leading cyber adversary. The breach, which OPM detected in April, does not appear to impact security in the States; it follows a similar attack on OPM, likely carried out by the Chinese, last July. The NJCCIC assesses that China and other advanced cyber adversaries such as Russia value the personal information of US federal employees with access to sensitive programs and data systems because such intelligence positions Beijing and Moscow to make inroads to classified US systems and advance global criminal pursuits.

- According to the US Intelligence Community's Worldwide Threat Assessment for 2015, China is the US's most active and capable cyber adversary, followed by Russia. Notably, the assessment highlights China's and other actors' ability to exploit targets using relatively simple tactics, including social engineering or entering a system through unpatched vulnerabilities.
- Last year, China was implicated in a breach of the National Weather Service and the National Oceanic and Atmospheric Administration, which reportedly interrupted US satellite collection and impacted long-range weather forecasts. In addition, Beijing likely was behind a cyber attack on the US Postal Service, which compromised the personal information of 800,000 employees. Relatedly, according to US media reporting, the US State Department as of April had still not eradicated malicious cyber actors from its unclassified network, which was breached in late 2014, probably by the Russian Government.

State and local governments will remain attractive targets for malicious cyber actors because of increased record digitization and widespread email use across multiple business units and sectors.

The NJCCIC recommends that State and local entities adopt proactive and progressive cyber security initiatives to protect systems' data—such as cyber awareness training for, and regular updates on threats and best practices to, end users.

- Moreover, timely and exhaustive patching or updating of all state and local systems are key to maintaining a robust defensive posture. State and local organizations should also strongly consider adopting stringent encryption policies of all sensitive information.

Contact Information

Any agency with comments or questions about this document should contact the NJCCIC at njccic@cyber.nj.gov.
