Gov. Philip D. Murphy | Lt. Gov. Sheila Y. Oliver | Dir. Jared M. Maples

NJOHSP
Intelligence Note

May 29, 2020

Iranian Hackers Committed to Exploiting US Servers

Iranian hackers are using vulnerable US and private-sector computer servers and networks to conceal cyber attacks, steal proprietary information, and disrupt critical infrastructure. In January, the US Office of the Director of National Intelligence affirmed that Iran continues to present a cyber espionage threat using increasingly sophisticated techniques.

- On April 24, hackers linked to Iran targeted Israeli water distribution networks. Officials discovered the perpetrators routed their attack through computer servers located in the United States and Europe to conceal their identities. The hackers targeted two rural water distribution networks that control water flow, wastewater treatment, and regulatory systems serving residential, medical, and commercial customers. Israel retaliated in May, targeting cyber infrastructure at a port terminal in Bandar Abbas, southern Iran.

- Iranian-linked hackers have also targeted employees of US companies, including Gilead, a pharmaceutical company working on a treatment for COVID-19. The hackers used a phishing scheme to attempt to access passwords of high-level company employees. These "password spraying" campaigns have been aimed at healthcare policymakers and medical research organizations in the wake of COVID-19 to steal valuable research. Such cyber attacks highlight the capabilities of foreign adversaries in gaining access to US cyber infrastructure.

- A private cybersecurity firm released a report in February exposing an Iranian espionage campaign that occurred over the last three years. Iranian-backed hacking groups targeted virtual private networks, which were exploited and used to gain access to data storage across information technology, oil, aviation, and defense industries in Israel and the United States. The purpose of the operation appeared to be reconnaissance, but there is potential for the same tactics to be used to spread harmful and destructive malware to these industries.