SSBG IT Solutions
Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

China Hacked a Navy Contractor and Stole 600GB of Data

Hackers working for the Chinese government compromised a US Navy contractor and stole a massive cache of highly sensitive data, including details about a planned supersonic anti-ship missile, American officials said Friday.

The hack, reported by the Washington Post, took place in January and February and resulted in more than 614 gigabytes of data being stolen. The contractor that was breached was not disclosed but reportedly worked with the Naval Undersea Warfare Center, a research and development group that works on submarines and underwater weapons.

Of particular interest in the treasure trove of stolen documents—all of which government officials said were unclassified, per The New York Times—were details about a project known as Sea Dragon. First proposed in 2012, the Postsaid Sea Dragon is part of a Pentagon initiative to adapt existing US military technologies for new applications. The Defense Department described Sea Dragon as a weapon with “disruptive offensive capability” that will integrate “an existing weapon system with an existing Navy platform.”

While public details regarding the project are few and far between, the Pentagon has reportedly requested or used more than $300 million for the Sea Dragon project since 2015. Underwater testing is planned to start this September.

The Post also reported that plans for a supersonic anti-ship missile were also stolen (it’s not clear if those plans are the same or related to the Sea Dragon project). The missile was intended to be introduced for use on US submarines by 2020.

Per the Post, the stolen files also contained the following:

Signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit’s electronic warfare library.

The breach certainly isn’t good—reportedly, data on hundreds of mechanical and software systems were stolen by the Chinese hackers—but the Timespointed out that it’s “hardly the largest, or the most sensitive” hack

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

carried out in an escalating cyberwar between the US and China. That distinction likely belongs to the hack of the Office of Personnel Management—also tied to the Chinese government—which resulted in the personal information of as many as 25 million federal workers and contractors being compromised.

Still, the breach highlights the ongoing trouble the federal government has had not just defending against breaches but also getting contractors to stop playing fast and loose with sensitive data. Last year, a defense contractor Booz Allen Hamilton left sensitive Pentagon files on an Amazon server with no password protection in place. Contractor VendorX left billions of social media posts scraped by the Pentagon on an unprotected server, and another contractor publicly exposed "highly sensitive" US military data.

[Washington Post, New York Times]

Source: https://gizmodo.com/china-hacked-a-navy-contractor-and-stole-600gb-of-data-1826689038

Author: AJ Dellinger

PRIVACY AND SECURITY