China blamed for data theft from US Navy contractor

By Charlie Osborne

Published: 2018-06-11 · Archived: 2026-04-05 23:51:39 UTC

File Photo

China is being blamed for a cyberattack on a US Navy contractor which has led to the theft of sensitive military information.

As reported by The Washington Post, US officials have claimed that up to 614 Gigabytes of information was stolen, including signal and sensor data, as well as submarine radio information relating to cryptographic systems.

Plans for supersonic missiles which are due to be utilized by US submarines by 2020 were also compromised during the attack.

However, the most critical datasets stolen relate to a mission called Sea Dragon. While little is known about the project, the US Defence Department has described Sea Dragon as research into "disruptive offensive capabilities" by "integrating an existing weapon system with an existing Navy platform."

SEE: Can Russian hackers be stopped? Here's why it might take 20 years (TechRepublic cover story) | download the PDF version

As noted by The Drive, the Sea Dragon project began in the 2015 fiscal year, resulting in in-water tests, ejection bodies, hardware development, and a successful land test.

However, no details on the project's status have been revealed since 2016 in budget documents beyond plans for a "sea-based tactical demonstration" by the end of the 2018 financial year.

An electronic warfare library was also reportedly compromised. If this is the case, hundreds of mechanical and software-based systems may have been placed at risk.

The cyberattack took place across January and February this year. The unnamed contractor that was targeted worked with the Naval Undersea Warfare Center, a research establishment in Newport, Rhode Island.

The New York Times reports that the contractor was working on a Navy submarine and other underwater programs.

TechRepublic: Why AI could make the US and China the two biggest superpowers and change warfare as we know it

While the data -- once compiled -- could be considered classified, the information was reportedly stored on an unclassified network and would otherwise be considered unclassified, according to officials.

"There are measures in place that require companies to notify the government when a 'cyber incident' has occurred that has actual or potential adverse effects on their networks that contain controlled unclassified information," Navy spokesman Commander Bill Speaks told the Washington Post.

However, Speaks would not reveal any further details of the security incident.

The US Navy and FBI are believed to be investigating the espionage case.

We do not hear about every example of military espionage from all sides and states. However, with Chinese missiles reappearing in the South China Sea, it seems the country would take any advantage possible to secure the area and strengthen its dominion over the disputed territory.

The maritime industry, in any form, appears to be just as vulnerable to cyberattacks as any other. Last week, security researcher ken Munro warned that a commonly-used system for navigation, the Electronic Chart Display (Ecdis), is vulnerable to exploit.

CNET: China turns to tech to monitor, shame and rate citizens

Should threat actors choose to target Ecdis, it may result in widespread navigational confusion for ships and shipping lane chaos.

ZDNet has reached out to the Naval Undersea Warfare Center and will update if we hear back.

Previous and related coverage

- Bad passwords and weak security are making ships an easy target for hackers
- Gold Galleon hackers target maritime shipping industry
- Shipping firm warns that hackers may leak confidential information