

Singapore invites cyberattacks to strengthen defences

21 February 2018



Prime Minister Lee Hsien Loong speaks at Singapore's inaugural Cyber Week in 2016: the defence ministry has now held an unusual contest aimed at tightening cybersecurity

Hundreds of hackers have targeted Singapore's defence ministry — but the attacks were at the government's invitation in an unusual attempt to strengthen cybersecurity.

Authorities said Wednesday they had paid out US\$14,750 in [prize money](#) to the best of the 264 so-called "white hat" hackers—specialists who seek to break into networks to check for vulnerabilities—involved in the project.

The programme, which ran from mid-January to early February, was introduced after an embarrassing breach last year which saw hackers steal [personal data](#) from about 850 military servicemen and other employees from a defence ministry web portal.

It was run with cybersecurity network HackerOne, which specialises in coordinating "bug bounty programmes" in which hackers are rewarded for spotting weaknesses in computer systems.

The top [hacker](#) in the contest was a Cyber Security Manager from Ernst and Young Singapore who gave his name only as Darrel and goes by the online moniker "Shivadagger". He was awarded US\$5,000.

A total of 97 vulnerability reports were submitted from 34 participants during the programme, with 35 reports deemed valid, according to the defence ministry.

David Koh, the [defence ministry's cybersecurity](#) chief, hailed the project. "Our systems are now more secure," he said.

While Singapore has some of the most advanced weaponry in the region, Koh said the ministry was at increasing risk of being targeted, and attackers could range from high-school students in their basements to criminals and state-actors.

© 2018 AFP

APA citation: Singapore invites cyberattacks to strengthen defences (2018, February 21) retrieved 24 October 2020 from <https://phys.org/news/2018-02-singapore-cyberattacks-defences.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.