



香港大學

THE UNIVERSITY OF HONG KONG

About SHIELD

Distributed Denial-of-Service (DDoS) attacks continued to escalate in recent years with new motivation, tactics, and vectors, it's a malicious attempt to bring down networks, web-based applications, or online services by overwhelming it with traffic from multiple sources. In order to protect the businesses, organizations and critical infrastructures against increasing number of sophisticated DDoS attack from organized cyber-criminals, our research lab CISC which stands for Center for Information Security and Cryptography has worked with several stakeholders in the society to build the product SHIELD.

The Smartbox SHIELD is built to perform intelligent packet filtering in order to protect the clients against DDoS attack and ensure their business are not being impacted. It's a portable, plug-n-play unit that can resist mechanical shocks. It allows field engineers and frontline technical support teams to deploy the units in a non PC-friendly environment without any needs to setup and configuration of the units. The SHIELD can be installed even when a system is undergoing a cyber-attack and previous DDoS protection is missing, and it will take effect immediately so normal services can be resumed.

After the SHIELD is deployed, even when there is no attack, the SHIELD will sample and collect data packets to learn the basic pattern of traffics. The collected packets will then be sanitized at the SHIELD by removing the sensitive contents from the packets. The sanitized data packet then sent to the SHIELD Central Control server named TESTUDO for cyber attack profiling analysis. When there is small scale attack, the SHIELD can collect sanitized data packet and send to TESTUDO server to determine the potential sources of attack, based on the cyber attack profiling model. The platform SHIELD with TESTUDO server not only defend the customer from DDoS attack but also differentiate from other commercial products available in the region by providing data sanitization, traceback planning and cyber attack profiling to help all related stakeholders to be better prepared for potential cyber-attacks, and improve the response time when facing attacks.

The SHIELD is the perfect solution for SMEs looking for hassle free DDoS protection solution. The Law Enforcement (LE) edition of SHIELD is a valuable tool for law enforcement departments or cyber security firms to collect attack data which can be analysed without any delay.

CISC is working with Cyberport to provide free trial of SHIELD for tenants of the Cyberport FinTech Center which is one of the largest innovation and technology co-working spaces in Hong Kong. After this large-scale trial, CISC Limited, the research-based spin-off of the CISC research lab, targets to launch the SHIELD to the commercial market by end of 2018.