

Big Data Case Study: Malwares and Honeynet Logs Analysis

安興彥

國家高速網路與計算中心

Abstract

To resist the various threats from Internet, NCHC builds a honeynet on TANet. With the help of the honeynet we can observe the hackers who run the botnets to search and attack new victims. As our honeynet grows, the large mount of data cannot be easily handled by the relational databases. In this talk, we will share our experience of malwares and honeynet logs analysis.