Beitrag ID: **47** Beitragskennung: **66** Typ: **Poster**

Spoki: A Reactive and Scalable Network Telescope

Internet-wide scans are cheaply and quickly performed in IPv4. They are not only used to analyze the Internet ecosystem but abused to find vulnerable systems. We developed Spoki, a reactive-network telescope built on top of native actors in C++. It accepts TCP connections and collects payloads to look beyond the source addresses and get deeper insight into scanners.

Spoki is deployed at four prefixes in two regions, which helps us to study topological and regional differences. Designed as a long-term project, Spoki has collected TBs of data. This large-scale collection allows us to analyze unforeseen events, such as the Log4Shell incident. Clustering Log4Shell scanners by their infrastructure revealed a large-scale campaign responsible for more than 50% of events in 2022.

Find me @ my poster

Keywords

Internet Measurement
Scanners
Scalable Systems
Data Analysis
Security

TentID

Autor: HIESGEN, Raphael (HAW Hamburg)