The Summer of Cyber – A Malware Story

Peter Hannay
Edith Cowan University

A huge amount of effort has gone into producing open source malware analysis tools. These works include sandboxes, orchestration tools, static analysis libraries, automation utilities, and more. Despite the amount of effort that has gone into producing these utilities, we have seen very limited deployment of these utilities outside of large security-focused organisations. In this talk, we discuss the reasons behind the lack of uptake and present the results of our efforts to address the identified issues.

In early 2018, the ECU Security Research Institute placed six students in paid positions for seven weeks to develop a tool to automate the deployment of malware collection, analysis, and reporting systems across common environments. At the conclusion of this talk, the results of this work will be publically released, including all documentation and source code.