Executive Summary

During the last few years, there is a constant increase in the occurrence of security breaches focusing both large and small organisations. As companies are becoming more and more dependent on digital systems for their stable operation, the impact that a security incident may have on their business significantly increases.

Common security mechanisms and techniques have been proven effective to some extent against low level attackers, however, they may still fail against advanced and persistent adversaries. One of the reasons of their failure is that they highly rely on the security administrator’s skills and knowledge for their configuration. As a result, most security mechanisms are effective only against already known attacks and remain vulnerable to new or slightly modified attacks. As a result, the I.T. security community needs to immediately identify modifications of already known attacks, and remain informed about new vulnerabilities, techniques and tools.

However, as most common security mechanisms will block an attack on its early stage, security analysts are not able to obtain any further information about the attack’s next steps. This information, could be later used to identify new vulnerabilities or tools and upgrade the deployed security mechanisms. On the other hand, if the security mechanism does not block a detected attack, it will soon result in a security breach. Consequently, there is a trade-off between the amount of information being collected on each intrusion attempt against the level of risk that the organisation is willing to face.

In this report, we present and evaluate a security mechanism that attempts to solve the above problem by combining two popular security mechanisms, Honeypots and Intrusion Detection Systems. This mechanism, using an intrusion detection system, is trying to detect an attack on its early stages, redirect and retain it into a Honeynet. The Honeynet will then, allow the attack to move on its next steps, providing valuable information to the security community while the adversary’s access to the original protected network will be blocked. If the honeynet seems identical to the original network, adversaries will falsely believe that they have successfully infiltrated the security mechanism without being detected. However, they will be detected and redirected to the honeynet soon before their attacks oppose a real threat to the protected network.