In this thesis, we propose a novel approach to detect malicious executables in the network layer using a combination of techniques from bioinformatics, data mining and information retrieval. This approach requires translating malicious code into genome-like representations. Based on their \genetic" formats, we can easily extract features by constructing families for known malicious code using data mining algorithms.

These features then can be stored in a router or another device in the network to measure the similarity between payloads and extracted features. Once the similarity is over a threshold, the security device can block the entire session and report an alert before the threat reaches the intended host(s). Further more, attacks can be identified based on their features and the families where these features come from. Ultimately, our experiments showed that 95% accuracy of detection is possible with an identification rate of 83%.