A huge proportion of modern malicious software uses Internet connections. Therefore, it is possible to detect infected computers by inspecting network activity. Since attackers hide the content of communication by communicating over encrypted protocols such as HTTPS, communication must be analysed purely on the basis of metadata. Cisco provided us a dataset containing aggregated metadata with additional information as to whether or not each sample contains malicious communication. This work trains neural networks to distinguish between infected and benign samples, comparing different architectures of neural networks and providing a comparison with results achieved by different machine learning methods tried by colleagues. It also seeks to create a mapping which maps samples of communication into a space where different samples of malicious communication created by a single malware family form clusters. This may make it easier to find different computers infected by a virus with known behaviour, even when the virus cannot be detected by the detection system.