Computer networks connected to the Internet are prone to numerous types of attacks from malicious actors. Distinguishing between malicious and benign network traffic is typically complex and resource intensive. To aid in that effort, my project sought to create a supervised learning model to classify network traffic as either benign or one of 12 types of malware. I used a K-nearest neighbors (KNN) model to train intrusion detection data from the Canadian Institute for Cybersecurity, which included approximately 2.8 million observations spanning 84 variables. Principle component analysis (PCA) was used to reduce the data to five features. About 0.10% of the observations were discarded due to NaN or infinite values. The data was split into 70% training data, 30% validation data, and trained using five-fold cross-validation. A KNN model was trained using parameters nearest neighbors (3, 6, 9, or 12), leaf size (15 or 20), and weight (uniform or distance). Additionally, the number of PCA features was varied from two to five. In total, 320 model runs were executed over approximately 3.5 hours. Each run was scored using the macro average of F1 score (harmonic mean of precision and recall) and the mean of the area under the curve (AUC) of the receivers operating characteristics (ROC), using a one-versus-rest (OVR) strategy. The best model used 9 nearest neighbors, a leaf size of 15, distance-based weights, and five PCA features. The model performed well, with a macro mean F1 score of 0.82 and a mean AUC ROC OVR score of 0.962. Bot traffic was the most difficult to differentiate from benign traffic, and denial-of-service (DoS) Hulk traffic was the most prone to false positives. The model is generally suited for malware classification but is too slow to be used for real-time analysis without enhancement techniques such as downsampling or parallel processing.