Abstract—Extensive internet of things (IoT) devices being infected by malware are an increasingly important viable objective in IoT cyberattacks e.g., botnet, virus, trojan, etc. The botnets got leverage from unsecured IoT devices (e.g., CCTV, Raspberry Pi, Arduino Uno, esp 8266, etc) that operates by using the Internet traffic. In recent year, the high-profile IoT device's vendor and the researcher from all over universities are exploring the robustness of IoT devices against botnet attacks. This research uses a deep learning approach to prevent botnet attacks on IoT networks. The deep residual one-dimensional CNN (1DCNN) model as the proposed method is used for botnet traffic detection. Two algorithms are provided: data processing for the N-BaIoT dataset and IoT botnet detection training and testing. For data processing, training, and testing, the datasets were evaluated, and the model was optimized with different optimizers. This research used RMS Prop, ADaDelta, AdaGrad, AdaMax, and Adam as optimizers and the CNN was compared with LSTM, CNN with RNN, and Deep residual 1DCNN, respectively. The results showed that Deep Residual 1DCNN with Adam has the highest training accuracy of 88.67, 88.67 for validation accuracy, and 88.53 for test accuracy.