Abstrak—Perangkat internet of things (IoT) ekstensif yang terinfeksi oleh malware adalah tujuan yang semakin penting dalam serangan siber IoT misalnya, botnet, virus, trojan, dll. Botnet mendapat pengaruh dari perangkat IoT yang tidak aman (mis., CCTV, Raspberry Pi, Arduino Uno, esp 8266, dll) yang beroperasi dengan menggunakan lalu lintas internet. Dalam beberapa tahun terakhir, perangkat IoT yang terkenal vendor dan peneliti dari seluruh universitas sedang menjajaki kekokohan perangkat IoT terhadap serangan botnet. Penelitian ini menggunakan pendekatan pembelajaran mendalam untuk mencegah serangan botnet di IoT jaringan. CNN satu dimensi sisa dalam (1DCNN) model sebagai metode yang diusulkan digunakan untuk deteksi lalu lintas botnet. Dua algoritma disediakan: pemrosesan data untuk N-BaIoT pelatihan dan pengujian deteksi botnet dataset dan IoT. Untuk data pemrosesan, pelatihan, dan pengujian, kumpulan data dievaluasi, dan model dioptimalkan dengan pengoptimal yang berbeda. Penelitian ini menggunakan RMS Prop, ADaDelta, AdaGrad, AdaMax, dan Adam sebagai pengoptimal dan CNN dibandingkan dengan LSTM, CNN dengan RNN, dan Deep residual 1DCNN, masing-masing. Hasilnya menunjukkan bahwa Deep Residual 1DCNN dengan Adam memiliki pelatihan tertinggi akurasi 88,67, akurasi validasi 88,67, dan 88,53 akurasi tes.