ABSTRAK

MITIGASI SISTEM KEAMANAN DARI SERANGAN BOT MENGGUNAKAN CLOUDFLARE

Ihsanul Muttaqiin – NIM 1177050053

Jurusan Teknik Informatika

Dalam era digital saat ini, internet membawa berbagai manfaat dan inovasi teknologi yang signifikan, namun juga memunculkan tantangan baru seperti kejahatan siber. Salah satu jenis kejahatan siber yang sangat merugikan adalah serangan BOT *Attack*. Serangan ini dapat menyebabkan server mengalami gangguan signifikan bahkan tidak berfungsi, yang berdampak buruk bagi perusahaan dan mengancam integritas layanan online. Sebagai contoh, insiden *Cloudflare* pada tahun 2021 menunjukkan kemampuan serangan DDoS terbesar yang dilaporkan, melibatkan 20.000 bot dari 125 negara, menegaskan besarnya skala dan potensi kerusakan dari serangan tersebut. Serangan bot dapat hadir dalam berbagai bentuk, termasuk serangan *brute force*, kampanye *phishing*, dan pengikisan data, dengan tujuan mengganggu layanan, mencuri data, atau merusak reputasi. Penggunaan bot untuk membanjiri server dengan lalu lintas, misalnya, dapat menyebabkan gangguan layanan yang serius dan kelumpuhan operasional. Penelitian ini bertujuan untuk mengkaji efektivitas *Cloudflare*, sebagai solusi *Content Delivery Network* (CDN), dalam mencegah dan mengatasi serangan Bot. Dengan analisis yang mendalam, penelitian ini diharapkan dapat memberikan wawasan yang lebih baik tentang metode pencegahan serangan Bot, mengidentifikasi langkah-langkah mitigasi yang optimal, dan mengevaluasi kontribusi *Cloudflare* dalam melindungi webserver dari ancaman siber tersebut. Tujuan utamanya adalah untuk memberikan rekomendasi strategis bagi organisasi dalam meningkatkan keamanan siber mereka dan meminimalkan dampak dari serangan Bot terhadap keberlangsungan operasional layanan online.

Kata KuncI : Bot *Attack*, serangan siber, *webserver*, Keamanan siber, *Cloudflare*,

ABSTRACT

SECURITY MITIGATION SYSTEM FROM

BOT ATTACKS USING CLOUDFLARE

Ihsanul Muttaqiin – NIM 1177050053

Informatics Engineering Department

In the current digital era, the internet brings various benefits and significant technological innovations, but also raises new challenges such as cyber crime. One type of cyber crime that is very detrimental is a BOT attack. These attacks can cause servers to experience significant disruption or even malfunction, which has a negative impact on the company and threatens the integrity of online services. For example, the Cloudflare incident in 2021 demonstrated the largest reported DDoS attack capability, involving 20,000 bots from 125 countries, highlighting the scale and potential damage of such attacks. Bot attacks can come in many forms, including brute force attacks, phishing campaigns, and data scraping, with the goal of disrupting services, stealing data, or damaging reputations. The use of bots to flood servers with traffic, for example, can cause serious service disruptions and operational paralysis. This research aims to examine the effectiveness of Cloudflare, as a Content Delivery Network (CDN) solution, in preventing and overcoming BOT attacks. With in-depth analysis, this research is expected to provide better insight into BOT attack prevention methods, identify optimal mitigation measures, and contribute to Cloudflare in protecting webservers from these cyber threats. The main objective is to provide strategic recommendations for organizations to improve their cyber security and minimize the impact of BOT attacks on the continuity of online operational services.

Keywords: BOT Attack, cyber attack, webserver, Cyber security, Cloudflare,