ABSTRACT

The rapid digitalization of economies has brought significant productivity benefits but also increased exposure to cyberattacks, especially due to the widespread deployment of Internet of Things (IoT) devices and cloud services. These systems, often implemented with minimal security due to cost or configuration errors, are common targets for at tackers. This paper presents a novel, scalable honeypot platform designed to mimic any HTTP-based service, specifically aimed at addressing vulnerabilities in IoT devices and cloud services by capturing, analyzing, and understanding attacker behavior. By simulating these services, the honeypot provides a safe yet realistic environment for observing attack patterns and collecting critical data. The platform is highly flexible, capable of emulating a wide variety of services, from cloud databases to common IoT devices like network cameras, providing a comprehensive solution for proactive cybersecurity. This adaptability allows it to analyze HTTP-based threats across a broad spectrum of potential targets. During the four-month experimental phase, the system was used to simulate 14 distinct services, including various web and IoT applications, successfully collecting attacker data through enriched data analysis techniques. This data was processed to identify internet scanning services, and to classify types and characteristics of attacks, ultimately helping to distinguish legitimate users from bots and malicious actors. Using novel data enrichment mechanisms, the honeypot system identifies malicious internet scanning activities and delivers a detailed analysis of the data, providing valuable in sights into emerging threats. Key findings include the ability to classify attackers, trace their activities, and visualize the flow of attacks across different services, helping to pre dirt and prevent future attacks.