PhD THESIS ABSTRACT

„DEFENSE STRATEGIES AGAINST BOTNETS IN THE CONTEXT OF CYBER CONFLICTS”

Author: Cpt.eng. **Ioana-Daniela APOSTOL**
E-mail: ioana.apostol@mta.ro, tel.: +40755 548 704
PhD supervisor: **Victor-Valeriu PATRICIU**, PhD Professor engineer

Botnets have been present in cyberspace for more than two decades and, to date, they have evolved and changed permanently, managing to penetrate almost all interconnected environments, not only computer networks but also mobile phones or IoT devices. Despite the protection mechanisms developed and used so far to defend against them, botnets continue to represent one of the biggest threats in cyberspace and combating them is an important topic in the field of cybersecurity.

The present thesis proposes to supplement the current methods used to prevent and combat botnets with strategies aimed at bringing improvements to the concepts related to the defense against these threats. The contributions brought by this thesis follow three different research directions: a proactive one determined by increasing the level of preparedness against botnets by anticipating new versions of them that may appear in the future, an operational research direction that involves modeling in order to identify factors influencing botnets' expansion, and a reactive direction focused on methods of detecting botnet-specific activities.

The first research direction led to the proposal and implementation of a new botnet architecture that combines the advantages of the centralized architecture with those of the decentralized architecture, thus being considered a hybrid architecture. The proposed architecture is based on a centralized topology facilitating the rapid dissemination of commands, which is organized on hierarchical levels within which a customized communication protocol is used to ensure not only the coordination between the botnet's entities and the command transmission through the entire hierarchy but also restoring of the malicious network if one of the entities becomes unavailable.

The second research direction resulted in the proposal of a new botnet-specific malware propagation model intended for analyzing botnets that use active propagation mechanisms. The proposed model takes into consideration the malware infection rate, the device network activity, the recovery rate, and the immunization rate.

The third research direction led to the proposal of a solution that detects anomalies generated by botnets in IoT networks. The proposed solution is based on deep learning algorithms used to differentiate benign traffic from abnormal traffic. The experimental results obtained by training and evaluating the proposed solution using a publicly available dataset

demonstrated the effectiveness of the proposed solution by detecting anomalies with high accuracy.

This thesis, therefore, addresses a topic of interest to the scientific community, contributing to the research on defense strategies against botnets.