REZUMATUL TEZEI DE DOCTORAT

„STRATEGII DE APĂRARE ÎMPOTRIVA BOTNET-URILOR ÎN CONTEXTUL CONFLICTELOR CIBERNETICE”

Autor: Cpt.ing. **Ioana-Daniela APOSTOL**
Email: ioana.apostol@mta.ro, tel.: +40755 548 704
Conducător de doctorat: Prof.univ.dr.ing. **Victor-Valeriu PATRICIU**

Botnet-urile și-au făcut simțită prezența în spațiul cibernetic de mai bine de două decenii și până în prezent au evoluat și s-au diversificat considerabil, reușind să pătrundă în aproape toate mediile interconectate, nu doar în rețelele de calculatoare, ci și în rândul telefoanelor mobile sau a dispozitivelor IoT. În ciuda mecanismelor de protecție dezvoltate și utilizate până în prezent pentru apărarea împotriva lor, botnet-urile continuă să reprezinte una dintre cele mai mari amenințări din spațiul cibernetic, iar combaterea acestora constituie un subiect de importanță deosebită în domeniul securității cibernetice.

Teza de față urmărește completarea metodelor actuale de prevenire și combatere a botnet-urilor cu strategii menite să aducă îmbunătățiri la nivelul conceptelor ce țin de apărarea împotriva acestor amenințări. Contribuțiile aduse în această teză sunt reprezentate de trei direcții diferite de cercetare: o direcție proactivă determinată de creșterea nivelului de pregătire pentru apărarea împotriva botnet-urilor, anticipând noi variante ale acestora ce ar putea apărea în viitor, o direcție de cercetare operațională ce implică modelarea matematică în vederea identificării factorilor ce influențează extinderea botnet-urilor și o direcție reactivă axată pe metodele de detectare a activităților specifice botnet-urilor.

Prima direcție de cercetare a condus la propunerea și implementarea unei noi arhitecturi specifice botnet-urilor ce combină avantajele arhitecturii centralizate cu cele ale arhitecturii descentralizate, fiind considerată o arhitectură hibridă. Arhitectura propusă are la bază o topologie centralizată ce facilitează diseminarea rapidă a comenzilor, organizată pe mai multe niveluri ierarhice, în cadrul căreia se folosește un protocol de comunicație special conceput pentru a asigura atât coordonarea între entitățile botnet-ului și transmiterea comenzilor prin toate nivelurile ierarhice, cât și refacerea rețelei malițioase în contextul indisponibilizării uneia dintre entități.

Din cea de-a doua direcție de cercetare a rezultat propunerea unui nou model de propagare a *malware*-urilor specifice botnet-urilor destinat analizei botnet-urilor ce folosesc mecanisme active de propagare. Modelul propus ia în considerare rata de infectare a programelor malițioase, activitatea în rețea a dispozitivelor 4, rata de recuperare a dispozitivelor și rata de imunizare a dispozitivelor.

Cea de-a treia direcție de cercetare s-a concretizat prin propunerea unei soluții de detecție a anomaliilor generate de botnet-urile din rețelele IoT. Soluția propusă se bazează pe algoritmi

de învățare profundă cu ajutorul cărora traficul benign este diferențiat de cel cu anomalii. Rezultatele experimentale obținute prin antrenarea și evaluarea soluției propuse folosind un set de date disponibil public au demonstrat eficiența soluției propuse.

Teza de față abordează, așadar, un subiect de interes pentru comunitatea științifică, contribuind în cercetarea strategiilor de apărare împotriva botnet-urilor.