Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente / Reconhecimento de Padrões

Título: Mecanismo de *Cyber*-Vigilância com aprendizado baseado em *Deep Learning* visando detectar *botnets IoT*

Orientador – Sérgio Murilo Maciel Fernandes (smurilo@ecomp.poli.br)

Coorientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição

Internet das Coisas (IoT) é uma das tecnologias associadas à Quarta Revolução Industrial. A IoT diz respeito à interconexão de objetos físicos dotados de peças eletrônicas, como sensores e softwares, que são capazes de coletar e trocar dados entre si e com o usuário através da rede mundial de computadores. Por "coisas", entende-se como objetos empregados nas atividades diárias como TV, geladeira, máquina de lavar, lâmpadas, portas, etc. Com a difusão dos dispositivos IoT, a sociedade contemporânea tem tido facilidade e comodidade na execução automatizada dos seus afazeres domésticos e profissionais. Logo, os mecanismos IoT têm a capacidade de executar suas tarefas, efetuando correções em seu próprio trabalho, quando necessárias, sem a necessidade da interferência humana. Tecnicamente, os dispositivos IoT têm seus *firmwares* atualizados automaticamente mediante incrementos e/ou correções de suas funcionalidades.

Como efeito colateral, devido a grande e rápida popularização dos dispositivos de IoT, aplicações maliciosas têm se propagado nestes dispositivos. Há milhares de *malwares* voltados para IoT, em ordem de produção crescente (BEZERRA, 2019). Os *malwares* ("malicioso" + "software") objetivam atividades maliciosas distintas. Há *malwares* especializados no furto de informações automotivas, câmeras de vigilâncias e transações bancárias (BEZERRA, 2019) (SHARMEEN, 2018). Além disso, há o surgimento de várias *botnets* especializadas em IoTs. As *botnets* Mirai, Hajime, Aidra, dentre outras, têm causado prejuízos mundiais irrecuperáveis através da corrupção dos dispositivos IoTs (BEZERRA, 2019) (SHARMEEN, 2018).

Botnets são grupos de máquinas comprometidas por *malwares*, conhecidas como *bots* ou zumbis, controladas remotamente por um indivíduo chamado *botmaster* através de um canal de comunicação de comando e controle (C&C) (LE, *et al.*, 2019). Tecnicamente, o zumbi tem o *firmware* do seu comutador (*hub*, *switch* ...) infectado. Daí em diante, após estabelecimento do canal C&C, o zumbi recebe atualizações e/ou comandos do *botmaster* de modo a participar, de forma inconsciente, de um *cyber*-ataque. O objetivo final de um *botnet* é lançar ataques sincronizados empregando os seus zumbis recrutados.

Portanto, o projeto de pesquisa visa detectar, preventivamente, a atuação de *botnets* em dispositivos em IoT. O reconhecimento de padrão das atividades maliciosas deve ocorrer através de técnicas de *Deep Learning* (redes neurais profundas). As características, dos aplicativos IoT, serão os atributos de entrada das redes neurais artificiais no intuito de tornar o mecanismo proposto capaz de reconhecer técnicas de anti-forense digital que visam dificultar a identificação de atividades maliciosas.

Referências Bibliográficas

BEZERRA, V. E. A. IoTDS: A One-Class Classification Approach to Detect Botnets in Internet of Things Devices, Sensors (Basel, Switzerland). doi: 10.3390/s19143188, 2019.

LE, H.-V.; NGO, Q.-D.; LE, V.-H. Iot Botnet Detection Using System Call Graphs and One-Class CNN Classification, International Journal of Innovative Technology and Exploring Engineering (IJITEE). ISSN: 2278-3075, 8 (10), 2019.

SHARMEEN, S. E. A. Malware Threats and Detection for Industrial Mobile-Iot Networks., Special Section on Security and Trusted Computing for Industrial, IEEE, 2018.