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

Proposta de Tese de Doutorado

Área: Computação Inteligente / Reconhecimento de Padrões

Título: Proposta de Sistema Imunológico Artificial visando a Detecção de *Cyber*-Ataques *ZeroDay*.

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

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

Descrição

Atualmente, as organizações têm procurado detectar malwares (“malicioso” + “software”) através do uso de inteligência artificial, aprendizagem de máquina e ciência de dados (SANS, 2019). Os antivírus do estado-da-arte propõem extrair características do aplicativo suspeito, de maneira preventiva, antes de executá-lo. Essa metodologia é capaz de obter taxas médias de acertos superiores a 90% na detecção de malwares (LIMA, et al., 2018).

De forma adversa, os antivírus do estado-da-arte podem ser burlados por um ataque do tipo *ZeroDay*. Tecnicamente, *ZeroDay* ocorre quando uma vulnerabilidade do sistema não é auditada pelo antivírus. Em termos de máquina de aprendizado estatístico, *ZeroDay* corresponde a um atributo que não faz parte da camada de entrada da máquina. Logo, a infecção ocorre porque a vulnerabilidade não está sendo auditada. Em síntese, quando uma nova vulnerabilidade é detectada, cabe ao antivírus prover uma nova etapa de aprendizado (treinamento) do seu mecanismo de inteligência artificial. As novas características, referentes à vulnerabilidade recém-detectada, devem ser agrupadas às características convencionais, previamente conhecidas. Dessa forma, é possível proteger os demais computadores, ainda não infectados, dos malwares os quais explorem essa falha recém-encontrada.

Em média, os melhores *cyber*-vigilantes mundiais levam, em média, 20 (vinte) dias até conseguir diagnosticar novas vulnerabilidades exploradas (JOHNSON, *et al*, 2016). Os *cyber*-vigilantes, em questão, pertencem às companhias; Google, Cert, Mozilla Firefox, Palo Alto, dentre outras (JOHNSON, *et al*, 2016). Contudo, como adversidade, verifica-se que o fato de aguardar 20 (vinte) dias até a detecção de um ataque *ZeroDay* pode provocar prejuízos bilionários em escala mundial.

Dentre as possibilidades de ataques *ZeroDay*, o projeto de pesquisa visa criar uma nova categoria batizada de CIV (*Computational Immunodeficiency Virus* - Vírus da Imunodeficiência Computacional). Imunodeficiência Computacional se trata de uma inspiração na Imunodeficiência Humana a qual degrada o sistema imunológico da vítima (linfócitos, macrófagos). A Imunodeficiência Computacional proposta pretende criar *cyber*-ataques *ZeroDay* (inéditos) almejando desabilitar os mecanismos de defesa do sistema (antivírus, *firewall*, atualizações automáticas...). A justificativa é que tal proposta poderia permitir que malwares de domínio público infectassem a vítima. Cabe ressaltar que há cerca de 30 milhões de malwares catalogados pelos institutos de pesquisa. Em síntese, qualquer um desses milhões de malwares poderia infectar o sistema visto que os mecanismos de defesa (antivírus e *firewall*) estariam em estado de desordem.

Em paralelo a criação dos malwares CIV autorais, objetiva-se o desenvolvimento de um Sistema Imunológico Artificial, inspirado no mecanismo de defesa biológico, de modo a criar uma resposta imune adaptativa através da criação de anticorpos artificiais produzidos através dos antígenos artificiais. Biologicamente, antígenos correspondem a substâncias com potencial de produzir uma resposta imunológica específica, enquanto anticorpos são formados como resposta a um estímulo imunogênico e capaz de interagir com o antígeno que levou à sua síntese. Computacionalmente, os antígenos e anticorpos devem ser produzidos mediante um estado de desordem do sistema provocados pelos malwares CIV autorais. A intenção é que *cyber*-ataques *ZeroDay* possam ser detectados em tempo real, i.e., sem que haja a necessidade de aguardar dias até que os melhores *cyber*-vigilantes mundiais consigam diagnosticar novas vulnerabilidades exploradas.

Referências Bibliográficas

JOHNSON, *et al*. Time between vulnerability disclosures: A measure of software product vulnerability. Computers & Security 62 (2016) 278 – 295

LIMA, S. M. L. *et al*. Antivírus dotado de Rede Neural Artificial visando Detectar Malwares Preventivamente. iSys - Brazilian Journal of Information Systems, 11 (4), p. 31-62, 2019.

SANS. Institute InfoSec Reading Room. Out with The Old, In with The New: Replacing Traditional Antivirus, Disponível em: https://www.sans.org/reading-room/whitepapers/analyst/old-new-replacing-traditional-antivirus-37377. Acesso em Junho de 2019.