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 baseado em máquinas de aprendizado visando a Detecção de Malwares

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

Coorientador – Sidney Marlon Lopes de Lima (smll@ecomp.poli.br)

Descrição

Pesquisa do MCSI (Microsoft Computing Safety Index WorldWide Report), estima que, no mundo, o impacto financeiro devidos a ataques de malwares, Engenharia Social e de outras formas quanto a roubo digital de identidade ultrapassou US$ 23 bilhões, apenas no ano de 2013. Naquele ano, somente o valor gasto para reparar danos à reputação profissional, causados por golpes digitais, foi por volta de US$ 4,5 bilhões (MICROSOFT, 2014). Acrescido a isso, avalia-se que o tempo perdido devido às informações corrompidas, furtadas ou excluídas pelas pragas virtuais, somente no ano de 2013, é próximo dos 180 mil anos (MICROSOFT, 2014). Logo, por conta dos prejuízos, em grande parte irreversíveis, cada vez mais se vem investindo na segurança digital através de novas tecnologias em antivírus, firewall e biometria. Estima-se que serviços de antivírus estão presentes em 95% dos computadores pessoais, além de 84% dos internautas terem serviços de firewall ativado e 82% possuírem atualizações automáticas ativadas no seu sistema operacional Microsoft (MICROSOFT, 2014).

Apesar da presença massiva de mecanismos de cyber-vigilância na grande maioria dos computadores, os ataques cibernéticos vêm causando prejuízos bilionários e em ordem crescente (MICROSOFT, 2014). Uma das razões desse insucesso é o retardo no catálogo das novas pragas virtuais por parte das fabricantes dos antivírus. Então, caso haja rapidez na aquisição dos malwares, possivelmente adquirida a partir das denúncias dos usuários já infectados, é possível proteger os demais clientes ainda não infectados. Um grande problema dessa estratégia, adotada pelos antivírus comerciais, é para que haja a detecção de uma nova praga virtual é requerido que algumas máquinas já tenham sido infectadas. Cabe ressaltar que não basta apenas a detecção e eliminação do executável malicioso para que a vítima esteja livre de sua atuação. Além da eliminação do malware, é necessário desfazer todas as suas malfeitorias como, por exemplo, ter desabilitado os mecanismos de defesa da vítima, inclui-se firewall, plugins de segurança e os próprios antivírus. Logo, não é apropriada a estratégia de aguardar que uma vítima seja infectada e, em sequência denuncie um comportamento anômalo de seu dispositivo, para, então, tomar-se providências quanto à detecção de um novo malware.

Visando suprir as limitações e imprecisões dos antivírus comerciais, a proposta emprega redes neurais como técnica de inteligência artificial baseada em máquinas de aprendizado estatístico. Na área de segurança da informação, o uso da aprendizagem de máquina ainda está em um estágio inicial (HENKE, et al., 2011). A meta é detectar, estatisticamente, o reconhecimento de padrão do comportamento dos malwares. No tocante aos experimentos, o objetivo será classificar os executáveis em duas classes: sério e malicioso. Logo, a proposta será capaz de identificar o modus operandi das aplicações maliciosas antes mesmo de serem executadas pelos usuários.

Referências Bibliográficas

Microsoft Computing Safety Index WorldWide Report. Available in: https://news.microsoft.com/pt-br/microsoft-lanca-o-indice-de-cidadania-digital-e-incentiva-as-pessoas-a-ter-mais-empatia-online/. Accessed on June 2017, 2014.

HENKE, M.; SANTOS, C.; NUNAN, E.; FEITOSA, E.; SANTOS, E.; SOUTO, E. Aprendizagem de Máquina para Segurança de Computadores: Métodos e Aplicações. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. ISBN: 978-85-7669-259-1, 2011.