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

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Uma proposta para detecção do uso fraudulento de marcas através de reconhecimento de imagem em ataques de phishing direcionado

Orientador – Carlo Marcelo Revoredo da Silva (cmrs@ecomp.poli.br)
Co-orientador – Bruno José Torres Fernandes (bjtf@ecomp.poli.br)

Descrição – De acordo com a Konduto[1], metade dos golpes relacionados a cartões de crédito são aplicados através de ataques de *phishing*. Muitas fraudes exploram a suscetibilidade do usuário final através da fidedignidade, ou seja, através de uma engenharia social ardilosa que investe na riqueza em detalhes visuais, observando logomarcas, estilos e padrões estéticos que rementem a uma determinada marca, essa riqueza em detalhes é o que caracteriza o *phishing* como direcionado [1].

Existem considerações que caracterizam como positiva a prática de detecção de marcas em ataques de *phishing* [1, 2, 3], a saber: (i) tendo ciência da marca, os mecanismos *anti-phishing* baseados em característica detectam o segmento de atuação, obtendo maior sensibilidade sobre as pretensões da fraude; (ii) alguns *phishing* tem poucas informações textuais, quando o mal-intencionado constrói o *template* da página com uma imagem em *background* e flutuante, além de toda informação textual fica fundida na mesma; (iii) as informações visuais extraídas podem ser combinadas com informações textual, contribuindo para um veredito mais preciso sobre a página.

Todavia, existem desafios na detecção de marcas (3, 4): a sensibilidade precisa ser bem calibrada, já que uma mesma página pode conter imagens de marcas distintas, essa colisão de menções a marcas precisa ser tratada. A identidade visual é um elemento dinâmico, ou seja, podem ocorrer mudanças ou variações em uma mesma marca, essa base de conhecimento precisa ser previamente estabelecida. Outro desafio são os padrões de semelhanças entre marcas que podem acarretar em falsos positivos, portanto, é necessário adotar uma estratégia que atenue os equívocos por similaridades.

Diante o exposto, esse projeto propõe utilizar reconhecimento de logomarca e padrões visuais para a detecção de marcas-alvo em ataques de *phishing*. Além de ter como objetivo as considerações positivas apresentadas, a proposta tem a adoção de práticas que visam minimizar os desafios comumente presentes na detecção de marcas.

Referências Bibliográficas

1. Silva et al., Heuristic-based strategy for Phishing prediction: a survey of URL-based approach, Computers & Security, 2020.
2. Liu et al., SSD: Single Shot MultiBox Detector, ECC Vision, Springer, 2016.
3. Geng et al., Combating phishing attacks via brand identity and authorization features, SECURITY AND COMMUNICATION NETWORKS, Wiley, 2014
4. Bozkir and Aydos, LogoSENSE: A companion HOG based logo detection scheme for phishing web page and E-mail brand recognition, Computers & Security, Elsevier, 2020

[1] Terceira edição do raio-x da fraude: https://bit.ly/2mv2uvN (último acesso: 01/07/2021)