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

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Uma proposta baseada em Representação Textual Simplificada para minimizar ataques de Phishing

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

Descrição – De acordo com (Konduto, 2019), metade dos golpes relacionados a cartões de crédito são aplicados através de ataques de *phishing*, e protagonizados em ambientes de *e-commerce*. No mesmo estudo, é descrito que no Brasil, o *e-commerce* em 2019 sofria um ataque de *phishing* a cada 7 segundos. Através da engenharia social, o atacante traça perfis de suas vítimas com base em características inerentes ao contexto, como termos ou palavras-chave de uma determinada marca, para registrar domínios com erros tipográficos propositais, a exemplo dos domínios http://netf**ll**ix.com ou http://netfl**ii**x.com, prática conhecida como *typosquatting* (Spaulding et al, 2017). Tal manobra visa tornar o *phishing* mais fidedigno, fazendo com que o usuário final, muitas vezes levado pelo ímpeto do momento, acabe não levantando suspeitas sobre a procedência da página acessada.

Além disso, é possível observar que ataques de *phishing* também exploram aspectos sazonais para enganar suas vítimas (Silva et al, 2019). Como exemplo, pode-se citar os sites que, durante o distanciamento social causado pelo COVID-19, supostamente sugerem disponibilizar o auxílio emergencial do banco Caixa Econômica Federal (G1, 2020), explorando termos e palavras-chave relacionadas a uma determinada marca. Essa exploração é feita através de domínios e subdomínios de uma URL, a exemplo de: http://auxilio-caixa.com.liberacao-imediata.xyz. Outros eventos sazonais são suscetíveis à prática, a exemplo do Natal e Black Friday.

Diante o exposto, esse projeto propõe utilizar técnicas de *Natural Language Processing* (NLP), como o modelo estatístico *Latent Dirichlet Allocation* (LDA) ou métodos de *deep learning*, como estratégia para representação simplificada da recuperação de informações. A abordagem sugere que certos termos sejam previamente relacionados a um conjunto de palavras semanticamente relacionadas. A proposta é oferecer um mecanismo sensível ao contexto que identifique ataques de *phishing* considerando eventos sazonais e suas relações tipográficas a uma determinada marca.

Referências Bibliográficas

1. Bird et al, Natural Language Processing with Python, O'Reilly Media, 2009.
2. G1, Golpe do auxílio emergencial faz vítimas em todo o Brasil. Veja como identificar a fraude. Disponível em: https://bit.ly/2mv2uvN, 2020.
3. Konduto. Raio-X da Fraude. Terceira Edição, 2019. Disponível em: https://bit.ly/2mv2uvN
4. Ramage et al, Labeled LDA: A Supervised Topic Model for Credit Attribution in Multi-Labeled Corpora, Conference on Empirical Methods in NLP: Volume 1 - Volume 1, 2009.
5. Silva et al, Heuristic-based strategy for Phishing prediction: a survey of URL-based approach, Computers & Security, 2019.
6. Spaulding et al, Understanding the Effectiveness of Typosquatting Techniques, Proceedings of the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies, 2017.