Segurança em Redes e Interligência Artificial Será que “dá match”? - 8 de Setembro

Diogo C. T. Batista[1]

[1]Universidade Federal do Paraná (UFPR)
Curitiba – Paraná – Brasil

diogo@diogocezar.com

1. Resenha

Na apresentação do Professor Lucas Sampaio, foi discutido se a combinação entre segurança em redes e inteligência artificial são uma combinação eficiente e eficaz. A apresentação foi dividida em 4 principais pontos: Uma breve revisão sobre IA, uma revisão sobre os segurança em ambientes corporativos, a explanação de uma proposta de aplicação de IA em Segurança da Informação e suas considerações finais.

Lucas inicia apresentando que a IA é um campo da ciência da computação que se dedica a criar sistemas computacionais capazes de realizar tarefas que, normalmente, precisam de ação de humanos. Na sequência, mostra-se que apesar das confusões, Deep Learning é uma forma de classificação dentro de uma área maior chamada de Aprendizagem de Máquina, que por sua vez é uma das áreas de inteligência artificial.

Atualmente a área de IA tem sido destaque pois, nos últimos 5 anos, o poder de processamento em hardware aumentou consideravelmente. Isso proporciona uma combinação de fatores que agora pode ser explorados pela comunidade científica: uma grande quantidade de dados coletados todos os dias, elevado poder computacional mais acessíceis e tarefas que podem ser automatizadas e/ou reproduzidas.

Foram apresentados alguns exemplos de onde a IA pode atuar: jogos, reconhecimento de caracteres, corretor ortográfico, seleção de colaboradores em empresas, score de clientes em instituições financeiras ou até mesmo em veículos autônomos.

Ao introduzir a segurança em redes de computadores, são destacados os prejuísos causados em 2017, os valores estão entre 445 e 608 bilhões de dólares. Isso indica um mercado muito grante, e para ilustar, Lucas mostra que a pirataria física correspende apenas uma fração deste valor.

Este montante é formado por dados que valem ou envolvem dinheiro, com foco em instituições financerias. Ou em outros casos dados que são roubados de empresas que são especializadas em vender dados de usuários.

Na sequência, são mostradas as frequências com que os ataques ocorrem. E destaca-se os tipos de ataques mais frequentes: DDOS que tem como objetivo paralizar o serviço em questão; Man-in-the-middle que representa algum atacante analisando uma comunicação entre 2 pontos; Ataques utilizando DNS; Spoofing que significa que que um atacante se passa por outra pessoa e Zero-day exploids que são as vulnerabilidades exploradas no dia em que são identificadas.

Então destaca-se como a IA pode ser aplicada em segurança, mostrando que com algumas técnisas é possível: identificar contas maliciosas, identificar falhas de segruança

em software, identificar ataques quando ocorrem e principalmente treinar um sistema para utilizar um software de maneira interligente, de forma a identificar possíveis problemas ou vulnerabilidades.

Segue-se então com alguns exemplos de onde estas técnicas já são aplicadas. O Google removeu 700 mil apps da playstore e 100 mil contas, utilizando aprendizagem de máquina para reconhecer padrões e detectar códigos maliciosos ou ocorrências que infringíssem os termos de uso da plataforma. Outro exemplo citado foi em relação a sistemas de detecção de intrusão, nos quais após um monitoramento da rede, um sistema extrai as informações que são a entrada para softwares que usam IA para responder se o que ocorreu é ou não um ataque. E por fim, os sistema de prevenção de intrusão, tem o mesmo comportamento dos sistemas de detecção, com a diferença que podem tomar uma ação automatizada com base nas informações inferidas.

Mas estes métodos, já conhecidos, não necessáriamente precisam de IA para funcionar. Podem encontrar uma anomalia pela deteção de assinaturas (características dos ataques). Por exemplo: Aumento de tráfego, pode configurar um ataque de DDOS. Desvio de fluxo pode caracterizar um ataque do tipo Man-in-the-middle.

O grande problema são para ataques que nunca ocorreram. Para isso a proposta demonstrada, analisa o comportamento da rede. A principal dificuldade é extrair o que caracteriza um comportamento "normal" da rede. Essas características são altamente voláteis. Como por exemplo, o próprio crescimento de uma empresa imprime diferentes características de rede.

A utilização de aprendizagem de máquina através do treinamento de classificados CNN foi uma abordagem demonstrada para identificar as características de tráfego consideradas normais, bem como na deteção de anomalias.

A proposta de trabalho tenta responder as perguntas: Dado o que aconteceu nos utltimos n intervalores o que acontecerá no próximo intervalo t? Se uma anomalia for identificada, o que deve ser feito?

Com isso é possível notar as vantagens na utilização de IA aliada a segurança de redes, pois é possível detectar ataques que são ou não conhecidos, além de ser adaptável a cenários diferentes. E se utilizado em um sistema de prevenção é capaz de interrompoer vulnerabilidades não conhecidas anteriormente.

Termina-se com a resposta da pergunta: Segurança em Redes e Interligência Artificial, será que "dá match"?

Com certeza, são aliadas que podem funcionar, entretando, as mesmas técnicas de IA podem ser utilizadas para quem pretende realizar os ataques.