

Público

08-11-2018

Periodicidade: Diário

Classe: Informação Geral

Âmbito: Nacional

Tiragem: 51453

Temática: Sociedade

Dimensão: 878 cm²

Imagem: S/Cor

Página (s): 23

Inteligência artificial trará um “aumento significativo” no cibercrime

Web Summit
João Pedro Pereira

Antigo responsável do FBI diz que os sistemas inteligentes são uma arma poderosa para cibercriminosos

Há mais um sector em que a inteligência artificial está a abrir novos horizontes: o do cibercrime. Para James Trainor, que passou duas décadas a trabalhar no FBI, onde acabou por liderar a divisão de cibercrime, as tecnologias que estão a ser usadas para criar todo o tipo de automatismos vão também dar origem a ataques informáticos mais poderosos.

“A grande questão é passar de uma actividade de cibercrime feita por humanos, em que é uma pessoa e um teclado, para a automação e uso da inteligência artificial. Vai ser possível fazer ataques em grande escala”, antevê Trainor, que convervou com o PÚBLICO durante a Web Summit, que se realiza esta semana em Lisboa.

Os ataques informáticos são crimes em que o factor humano ainda tem um papel fundamental. Há criminosos atrás de um computador, que programam e disseminam *software* malicioso. Muitas vezes usam técnicas para ludibriar as vítimas, como mensagens de *mail* personalizadas. Estas pessoas são, assim, levadas a ceder dados ou a instalar um ficheiro que não é aquilo que pensam, abrindo uma porta ao atacante.

Os sistemas inteligentes, porém, vão dar uma nova dimensão aos ciberataques, argumenta o ex-FBI. “Daqui a cinco anos, pode ser o contrário e a maioria dos ataques serem com base em inteligência artificial, o que vai trazer um aumento significativo na actividade criminosa. Não se traz um humano para uma luta de *software*. Isto é cibersegurança, é uma luta de *software*. Não é uma questão de seres humanos, é uma questão de ter o melhor *software*.”

Entre 2012 e 2016, Trainor encabeçou a divisão de cibersegurança do FBI, antes de se reformar e ir trabalhar para a Aon, uma multinacional de seguros e análise de risco. Durante os anos em que esteve no FBI, viu

a investigação de cibercrimes deixar de ser um trabalho espalhado por vários departamentos para se tornar num departamento específico dentro da organização.

Mesmo com mais recursos e investimento, os desafios para os investigadores do FBI são muitos, reconhece Trainor, e não passam apenas pelas redes sociais e as aplicações de mensagens, onde qualquer pessoa pode criar contas, espalhar desinformação e, em alguns casos, comunicar de forma encriptada. O trabalho é dificultado também pelos países que funcionam como portos

de abrigo para cibercriminosos. E esta é uma lista cujo primeiro lugar, assegura, é da Rússia.

“O crime é uma coisa muito complexa e internacionalizada. A capacidade de recolher informação requer cooperação internacional, o que significa processos legais nos EUA e fora dos EUA. Mas há alguns países que possibilitam o cibercrime, particularmente a Rússia”, diz Trainor. “Não é só uma questão de não estarem a ser cooperantes [com as autoridades de outros países]. Estão a promovê-lo. Os cidadãos russos cuja actividade de cibercrime extravase as fronteiras da Rússia não sofrem quaisquer consequências”.

A protecção e apoio que Moscovo eventualmente dá aos cibercriminosos tornou-se nos últimos anos um tema político e um dos antigos chefes de James Trainor, o antigo director do FBI Robert Mueller, está desde o ano passado a investigar a possível interferência russa nas eleições que deram a vitória a Donald Trump.

Concorrência do privado

Os salários elevados que o sector privado oferece são outro proble-

ma para o FBI. Engenheiros e programadores informáticos são muito procurados por empresas de todo o género. Mas a área da cibersegurança é daquelas em que há mais escassez de mão-de-obra e onde as empresas competem ferozmente por talento (é uma questão que também foi levantada em Portugal pelo ex-director do Gabinete Nacional de Cibersegurança, Pedro Veiga, quando se demitiu em Maio).

“Demora anos a desenvolver as competências técnicas e são competências que podem ser directamente transferidas para o sector privado”, explicou Trainor. “As pessoas podem ficar tentadas a ir para o sector privado, onde também se fazem coisas boas. Mas é diferente. Nada é comparável ao trabalho do FBI”, defendeu.

Então como se aliciam especialistas a trabalhar por menos dinheiro? “Damos-lhes uma grande missão e um sentido de serviço público. É uma carreira fantástica, é desafiante, é preciso ser criativo, inovador, inteligente. E é trabalhar para o público, a proteger as pessoas. Foi por isso que fiquei durante 20 anos.”

joaopedro.pereira@publico.pt



Não se traz um humano para uma luta de *software*. Isto é cibersegurança

James Trainor

Ex-FBI



O antigo chefe da divisão de cibersegurança do FBI está em Lisboa para participar na Web Summit

MIGUEL MANÇO