IA ajuda a contornar ataques cibernéticos

Paulo Brito
Para o Valor, de São Paulo

A organização AV-Test, que analisa e compara soluções antivírus, calcula que pessoas mal intencionadas já tenham criado pelo menos 845,37 milhões de programas que trazem algum prejuízo para computadores e outros dispositivos digitais — os malwares. Pior, a expectativa da organização é de que outros 10 milhões de programas similares sejam despejados a cada mês na internet.

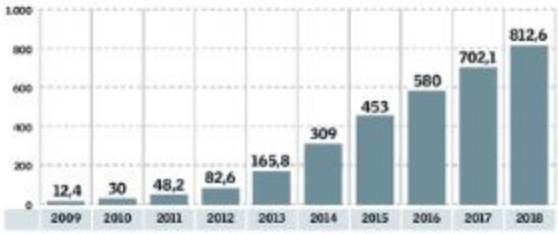
Várias soluções estão disponíveis no mercado para resolver esse problema, mas ele vem se tornando tão complexo, que muitas já se utilizam de Inteligência Artificial (IA) para proteger os sistemas, conta Fábio Campos, líder de security services da IBM para América Latina. Numa pesquisa em que entrevistou 600 executivos da área de TI, a empresa constatou que 52% já estão contratando profissionais com experiência em IA para cibersegurança e outras finalidades.

Embora essa tecnologia tenha aplicação numa grande variedade de temas, que vão de biometria a prospecção de petróleo, não é uma coisa que se compre pronta, alerta o especialista. "Muita gente acha que é só comprar e ligar que se chega ao destino. Mas não é assim. Um sistema desses vai construindo sentidos sobre o material que recebe para com isso aprender. Isso lhe dá o poder de análise e de resposta", explica.

Na avaliação de Fabrizio Pinna, superintendente executivo de segurança do Bradesco, essa busca de soluções para os ciberataques já lembra atualmente um videogame. "Um banco é um enorme desafio para o hacker, que não precisa se armar nem ir para a rua para fazer um ataque. Fica sentado em sua casa, e vai atacar por simples prazer ou por uma motivação política". Para Pinna, muitos ataques já podem ser considerados parte de uma guerra. "Na Primeira Guerra Mundial, os combatentes usaram baionetas, na Segunda aviões e tanques e a na terceira, que já está acontecendo, utilizam computadores", afirma.

Malwares à solta

Evolução dos programas maliciosos no mundo - em milhões



Fonte: AV-Test, 2019

Com a quantidade diária de ataques contabilizada aos milhões, o cenário é de uma tempestade perfeita: "Para sobreviver, precisamos de tecnologia e recursos no estado-da-arte. Isso significa que temos de fazer a detecção do ataque em um minuto, contê-lo em no máximo dez e resolvê-lo de vez em 60", afirma. É para isso que a inteligência artificial precisa ser utilizada, diz Pinna. "Colocamos a IA para descobrir coisas e as correlacionamos para tomar decisão. Para tirar proveito disso, precisamos de uma eficiência brutal. Ou somos eficientes ou perdemos o jogo"

Para Thiago Bordini, diretor de inteligência cibernética da New Space, "a IA ajuda principalmente na análise de grandes massas de dados, permitindo que mais pontos sejam analisados. Só num celular já existe uma enorme massa de dados", comenta. Na análise de crimes, essa tecnologia ajuda a mapear padrões lícitos e ilícitos, fazendo comparações entre eles e localizando desvios, mesmo sutis. A análise dos desvios permite a obtenção de mais pistas e eventualmente a identificação do criminoso. "Mas é preciso lembrar que a gente deve pensar em IA como se pensa num cachorro. É preciso treiná-lo direito para a gente não transformar um rottweiler num pincher ou o contrário", compara.

Campos, da IBM, alerta para o fato de que hoje os cibercriminosos também utilizam IA, podendo inclusive "envenenar" as plataformas da tecnologia, alimentando-as com dados incorretos.

Nuno Pires, vice-presidente da FeedZai, especializada em soluções de IA para o sistema financeiro, diz que um de seus clientes na Europa contratou esse tipo de solução depois de sofrer um ataque de 'bots'. "É uma empresa de comércio eletrônico, que nesse ataque poderia ter perdido US$ 64 milhões em mercadorias. Os robôs geraram 367 mil compras em menos de uma hora. Claro que um ser humano não tem condições de fazer essa operação. Felizmente o cliente reverteu praticamente 100% das transações".