Ano Novo, Ameaças Novas?

digitalinside.pt/ano-novo-ameacas-novas

Existem cada vez mais vetores de ataque, incluindo código malicioso, disponíveis através do mercado CaaS, tais como kits de Phishing, Ransomware-as-a-Service, DDoS-as-a-Service, e muito mais. O ransomware, e nomeadamente, o Ransomware-as-a-Service, irá continuar a evoluir tornando-se mais agressivo e inovador. Além de encriptação de dados, os cibercriminosos estão a utilizar estratégias de dupla e tripla extorsão, onde ameaçam divulgar informações sensíveis caso o resgate não seja pago – algo que na VisionWare, desencorajamos fortemente. Embora seja possível ver alguns grupos de cibercrime a confiar na Inteligência Artificial (IA) para potenciar as ofertas de CaaS, é bastante provável que esta tendência se desenvolva nos próximos meses. De acordo com dados recentes da FortiGuard Labs prevê-se que os cibercriminosos utilizem os resultados automatizados dos Large Language Models (LLMs) para fomentar as ofertas de CaaS e fazer crescer o seu negócio, como por exemplo, através do reconhecimento de redes sociais e a automatizar essa inteligência em kits de phishing completos.

Nos últimos anos, o trabalho remoto aumentou substancialmente a superfície de ataque e as vulnerabilidades da segurança das empresas face às ameaças, tornando a engenharia social uma tática cada vez mais apetecível. Muitos grupos de cibercrime têm cada vez mais como alvos, os executivos e funcionários de organizações. Ataques como phishing e comprometimento de e-mails corporativos (BEC) foram já alguns dos ciberataques mais prevalentes em 2024 e a tendência para 2025 não será de diminuição. Os agentes de ameaças realizam ataques mais direcionados, de forma mais rápida e precisa graças à Inteligência Artificial Generativa, que é sem dúvida uma tendência em ascensão e graças às suas capacidades crescentes ao nível de processamento é expectável que comece a funcionar de forma mais autónoma. Estes avanços beneficiam também o cibercrime que se serve desta tecnologia para orquestrar ciberataques mais precisos e difíceis de detetar. Ferramentas de IA podem ser usadas para automatizar a kill chain, tornar mensagens de phishing mais credíveis, identificar vulnerabilidades em sistemas e até criar malware adaptável, capaz de evoluir e contornar defesas tradicionais. Existem já inúmeras ferramentas, como é o caso do WormGPT, que apoiam os cibercriminosos em várias componentes e fases do ataque, desde a simples escrita de mensagens, personalizadas, sem erros e barreiras linguísticas, à criação de código malicioso. Além disso, as ferramentas de criação de conteúdo de texto, imagem e voz sintéticas continuam a aumentar e a preços acessíveis a todos. Neste sentido, é expectável que deepfakes continuem a ser utilizados para facilitar ataques baseados em engenharia social, como fraudes financeiras e também para apoiar campanhas de desinformação online.

Assim, em 2025, os ciberataques alimentados por IA continuarão a ser mais sofisticados e generalizados, esperando-se por isso, que os riscos para as organizações aumentem. Este cenário desafia as empresas a implementarem soluções de IA defensiva para

combater essas ciberameaças e reduzir estes riscos. Os investimentos e as inovações no domínio da segurança dos terminais e das redes foram intensificados ao longo do último ano e as iniciativas para automatizar a deteção de ameaças aumentaram, incluindo threat intelligence baseada em IA. O cenário de ciberameaças de 2025 será certamente marcado pela sofisticação dos ataques impulsionados por tecnologias avançadas, maior conectividade global e contexto geopolítico – no fundo, o ano muda, mas as ameaças são as mesmas. Estaremos preparados?

Bruno Castro é Fundador & CEO da VisionWare. Especialista em Cibersegurança e Investigação Forense