

O que é a automação de hackers e por que ela quebra as defesas tradicionais?

Resposta curta: A automação de hackers é o uso de scripts, IA e automação robótica de processos para executar todas as fases de um ataque à velocidade da máquina. Um ataque automatizado pode infiltrar-se numa máquina, roubar dados e eliminar as suas próprias ferramentas em memória em segundos — muito mais rápido do que qualquer analista humano consegue responder.

O que é automatizado

- **Reconhecimento:** ferramentas analisam a internet em busca de sistemas vulneráveis e mapeiam uma rede-alvo em segundos, além de gerar phishing convincente em grande escala.
- **Exploração:** assim que uma vulnerabilidade é encontrada, os frameworks implantam o exploit imediatamente — um zero-day pode ser utilizado em milhões de máquinas antes de um humano registar o alerta.
- **"Smash and grab":** o malware moderno não avalia quais ficheiros são valiosos. Ele encripta ou exfiltra tudo o que consegue alcançar, tão rapidamente quanto possível.

Por que os humanos não conseguem vencer esta corrida

O limite não é a qualidade da equipa nem o número de colaboradores. É a biologia. O tempo necessário para uma pessoa ver um alerta, processá-lo e agir é maior do que o tempo que o ataque leva para se concluir. O encaminhamento da telemetria para um servidor na nuvem para análise e o respetivo retorno acrescentam ainda mais atraso.

A única resposta viável é uma defesa que decida e atue de forma autónoma, no endpoint, em milissegundos.