Diário (Arquivo) | Sabe qual é o tipo de crime organizado mais rentável e danoso?

leitor.expresso.pt/diario/quarta-9/html/caderno1/temas-principais/Sabe-qual-e-o-tipo-de-crime-organizado-mais-rentavel-e-danoso-

Estima-se que em 2022 quase toda a população mundial seja atingida por um só tipo de ataque digital

Os cibercriminosos estão a explorar ao máximo a velocidade e o anonimato da internet para aprofundarem atividades ilegais e criminosas. De tal forma que o cibercrime já é, segundo a Interpol, o tipo de crime que cresce mais rapidamente. E é também o mais rentável e o que maiores danos provoca entre os vários tipos de crime organizado, adianta ao Expresso o presidente executivo da VisionWare, Bruno Castro.

Não só porque "o número de utilizadores conetados à internet é cada vez maior — sejam eles indivíduos, organizações ou empresas e até o próprio Estado —, o que alarga o espectro de alvos", mas também porque "o crescimento de utilizadores não tem sido acompanhado por um crescimento da educação para as boas práticas na utilização das tecnologias", explica o fundador da empresa de cibersegurança.

Se, por um lado, a diminuição do custo da tecnologia alargou o acesso a esta, "a sua complexidade aumentou, tornando o seu manuseamento — e respetiva segurança — ainda mais difícil". Além disso, tecnologias como a inteligência artificial colocam novos desafios e sectores que não estavam tradicionalmente associados à tecnologia — como o automóvel ou a saúde — "passaram a integrá-la", o que os torna alvos mais vulneráveis.

Até porque os criminosos digitais estão cada vez mais sofisticados e organizados, acredita Bruno Castro. Desenvolvem “novos ataques”, contornam “as defesas que iam sendo desenvolvidas como resposta a estas ameaças”, cruzam “vários tipos de ataque para que com uns, secundários, se camuflem outros, os principais”, e trabalham como “ciberespiões ao serviço de empresas e Estados enquanto prestadores de serviços”.

Portugal não foge à regra

Seja organizado ou não, o cibercrime distingue-se do tradicional por ocorrer no universo digital. “Tal como no crime organizado tradicional, que muitas vezes associamos à máfia, também o cibercrime tem repercussões físicas”, sublinha o fundador da VisionWare. E o seu impacto é muitas vezes superior: “consegue maximizar o seu impacto, muitas vezes com o mínimo esforço, não precisando de aplicar grandes ataques para ser efetivo”.

Só no caso do ramsonware (software malicioso que encripta computadores e apenas os desbloqueia mediante um resgate), estima-se que em 2022 seis mil milhões de pessoas — menos 1,6 mil milhões do que a população mundial atual — sejam atingidas por este tipo de ataque e que o número de empregos por preencher na área da cibersegurança triplique.

As previsões, anunciadas recentemente pelo diretor executivo da Agência Europeia para as Redes e Segurança da Informação (ENISA), Udo Helmbrecht, apontam ainda que os custos globais pelos danos causados por ataques de ransomware devem ultrapassar os 11,5 mil milhões de euros anuais já no próximo ano.

Entre os ataques mais comuns destacados pela ENISA não está apenas o ransomware. A VisionWare destaca ainda o malware (software malicioso instalado em computadores para causar danos a hardware, software e dados), o phishing (ataque que pretende levar os utilizadores a entrarem em sites maliciosos para revelarem nomes de utilizadores, palavras-passe e códigos bancários), o denial of service (ataque, muitas vezes secundário, para camuflar um ataque principal, que leva os sistemas e recursos da rede à exaustão tornando-os indisponíveis) e as fugas de informação, intencionais ou voluntárias.

Com motivações financeiras ou de intelligence, “os cibercriminosos são responsáveis por dois terços dos ciberataques”, avança Bruno Castro. Mas não são os únicos. “Ao seu lado agem ciberterroristas, ciberativistas, ciberespiões, insiders com rancor ou motivações económicas, alguns ‘jovens brincalhões’ que procuram reproduzir ataques digitais e até mesmo o Estado (motivado politicamente) e as empresas (motivadas pela concorrência).”

E nem Portugal foge a estes ataques. A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T) e o Ministério Público têm alertado para o aumento dos ataques cibernéticos no país, especialmente através de phishing e o ransomware.

“Mas, infelizmente, esse alerta não tem sido nem regular nem eficaz, pois um pouco por todo o lado, e em particular em Portugal, a consciência do cibercrime e das boas práticas no seu combate é ainda bastante reduzida”, aponta o presidente executivo da VisionWare. “É premente a educação para a segurança e consciencialização dos conceitos nas boas práticas como hábitos recorrentes.”