Cibercrime: quem o financia?

dinheirovivo.pt/8408124211/cibercrime-quem-o-financia

Todos os anos são divulgadas novas estatísticas que nos mostram como o cibercrime continua a aumentar, em número, sofisticação e impacto. Fraudes, roubo de dados, ataques de *ransomware*, são muitos os exemplos de ciberataques que alimentam este negócio altamente lucrativo, dia após dia, nas sombras da sociedade. Contudo, para que estas operações prosperem e permaneçam em ação, precisam de financiamento.

Grupos independentes de cibercriminosos são por norma, os principais atores, no entanto, os Estados também podem desempenhar um papel importante no financiamento e no apoio ao cibercrime, especialmente, em cenários de ciberguerra, espionagem e desestabilização política.

Os Estados podem financiar o cibercrime de várias maneiras, e uma das principais é através do patrocínio de grupos cibercriminosos. Neste primeiro caso, os Estados oferecem suporte financeiro, infraestrutura e, em alguns casos, proteção legal a esses grupos em troca de serviços que vão ao encontro dos seus interesses geopolíticos. Um exemplo disso são os grupos APT28 (Fancy Bear) e APT29 (Cozy Bear), muitas vezes associados ao governo russo, que têm um histórico de envolvimento em ataques contra sistemas governamentais e militares de países ocidentais. Além do patrocínio de terceiros, muitos Estados também formam grupos estatais de *hackers*, compostos por membros das forças armadas ou de agências de serviços de inteligência.

Esses grupos operam sob o comando direto do Estado e conduzem operações altamente coordenadas que englobam ciberespionagem, sabotagem de infraestruturas críticas, roubo de propriedade intelectual, entre outras. A China, por exemplo, foi repetidamente acusada de conduzir atividades de ciberespionagem por meio de grupos como a PLA Unit 61398, com foco no roubo de segredos industriais e militares.

Uma das outras grandes motivações do cibercrime patrocinado por Estados é justamente, a desestabilização e a descredibilização dos rivais. Um exemplo clássico são as campanhas de desinformação, tantas vezes conduzidas por meio de plataformas de redes sociais, e que têm como principais objetivos, minar a confiança da população nas instituições, exacerbar divisões sociais e políticas ou até mesmo, interferir em processos eleitorais.

Ainda assim, os alvos que terão um impacto mais direto na população continuam a ser as infraestruturas críticas. Desde redes de energia, sistemas de transporte, redes de telecomunicações, infraestruturas de saúde, estes são apenas alguns exemplos de alvos mais frequentes de grupos patrocinados por Estados, que procuram atacar um Estado adversário. Este é muito provavelmente um dos exemplos mais graves quando

pensamos nas consequências para a segurança e defesa de um país, ao afetar diretamente a sociedade nos aspetos essenciais que a sustentam e a credibilizam, sobretudo perante o mundo exterior.

Assim, apesar dos vários fatores que acabam por facilitar este processo, desde a evolução das criptomoedas ao anonimato proporcionado pela *dark web*, o próprio envolvimento dos Estados no cibercrime torna o combate ainda mais complexo. Enquanto os cibercriminosos independentes atuam motivados por lucro financeiro, os Estados possuem motivações mais amplas, contando com recursos significativamente maiores, acrescida da proteção legal dentro de seus próprios territórios, o que dificulta a sua responsabilização em âmbito internacional. Combater o cibercrime exige hoje, mais do que nunca, união, resiliência e cooperação internacional.

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