# Ransomware: mais que um ataque, um modelo de negócio

linktoleaders.com/ransomware-mais-que-um-ataque-um-modelo-de-negocio-bruno-castro-visionware

Link to Leaders August 29, 2025

Bruno Castro, fundador e CEO da VisionWare

> Por muito que se fale de ransomware como uma ameaça técnica, o que enfrentamos hoje é, na verdade, um fenómeno económico e criminoso global.

Os ataques de ransomware deixaram de ser apenas uma questão de encriptação de dados ou indisponibilidade de sistemas. Tornaram-se parte integrante de um modelo de negócio altamente rentável, sustentado por um ecossistema cujo sucesso se baseia essencialmente em ataques escaláveis e dirigidos, pagamentos anónimos via criptomoedas, lavagem financeira sofisticada e uma estrutura organizacional cada vez mais profissionalizada. Os principais grupos de ransomware – como LockBit, BlackCat, REvil, RansomHub – operam com níveis de organização próximos de empresas tecnológicas, com funções claras.

Estes grupos não só exploram vulnerabilidades técnicas, como também, ou até principalmente, as fragilidades humanas e institucionais, incluindo a dependência digital crítica. Utilizam métodos como a dupla extorsão (encriptação e ameaça de divulgação de dados) ou a tripla extorsão (com ataques a clientes ou parceiros), forçando assim as vítimas a pagar não apenas para recuperar, mas para evitar danos reputacionais.

No centro deste negócio está o uso de criptomoedas, que facilitam a transferência de fundos de forma quase impossível de averiguar. Estas moedas digitais são convertidas através de mixers, exchanges de baixa regulação e redes de “money mules”, que tornam os lucros limpos e indistinguíveis. Estimativas recentes indicam que milhares de milhões de euros são movimentados anualmente através destes esquemas sendo que, grande parte dos quais permanece fora do alcance das autoridades.

É aqui que o ransomware deixa de ser apenas um problema de segurança informática e passa a ser um problema geopolítico e financeiro. O financiamento de grupos criminosos – e em alguns casos, a possível ligação a regimes estatais ou organizações sancionadas – levanta questões sérias sobre soberania digital e segurança nacional. Pagamentos de resgate, mesmo que aparentemente pequenos, podem acabar a alimentar estruturas envolvidas em espionagem, sabotagem ou destabilização política.

Apesar dos esforços de investigação de entidades como a Europol, FBI, e diversas equipas de threat intelligence, a verdade é que o combate ao ransomware exige colaboração internacional, legislação coordenada e responsabilidade partilhada entre sector público e privado. É necessário ir atrás, não só dos operadores, mas também dos

facilitadores: as infraestruturas tecnológicas usadas para distribuição de malware, os canais financeiros onde os lucros circulam e os mercados onde se vendem credenciais roubadas e acessos iniciais.

Num contexto onde os ataques continuam a evoluir em sofisticação, é fundamental que deixemos de pensar no ransomware como um problema exclusivamente técnico. Trata-se de um mercado negro bem estruturado, onde as vítimas são vistas como clientes relutantes, mas inevitáveis, e onde o silêncio, muitas vezes motivado pela tentativa de proteger a reputação, só perpetua o problema.

Enquanto líderes de cibersegurança, temos de assumir um papel mais ativo na educação, prevenção e dissuasão. Não basta responder aos ataques, é preciso romper o modelo económico que os sustenta, ao recusar pagamentos de resgates, partilhar informação de forma rápida e promover medidas de transparência e resiliência. O ransomware é já uma indústria (obscura), mas não tem de continuar a sê-lo.