Ransomware: uma ameaça em expansão

digitalinside.pt/ransomware-uma-ameaca-em-expansao

Nos últimos anos, o ransomware emergiu como uma das ciberameaças mais persistentes e devastadoras do mundo cibernético, impactando diversas esferas da sociedade, sendo que, em Portugal foi particularmente mais expressivo e até “agressivo” junto da administração pública. Esta evolução reflete o avanço tecnológico e a sofisticação crescente das novas ondas de ciberataque, que advém dos cibercriminosos estarem constantemente a inovar tecnologicamente e a adaptar as suas táticas para maximizar o impacto e os lucros. Cabe-nos refletir e saber tirar ilações sobre este momento “quase” constrangedor que estamos a viver, onde a evolução acentuada do mundo digital, com inúmeras vantagens sociais, também veio dar asas ao cibercrime, criando uma fase nunca vista onde o mundo do cibercrime nunca foi tão volumoso, disperso e eficaz. A evolução tecnológica, potenciada com o “salto para o digital” da maioria da sociedade moderna, catalisou também o cibercrime, quer em termos de evolução tecnológica, quer principalmente em volume de ciberataques em curso e da sua própria eficácia. O ciberataque de ransomware é precisamente um excelente exemplo de evolução tecnológica com um crescendo de eficácia que se veio a tornar a grande referência mediática do cibercrime.

Originalmente, o ransomware era relativamente mais “simples” – os cibercriminosos assumiam o controlo dos dados de uma qualquer organização e exigiam um resgate para restaurar o acesso. Contudo, a sofisticação e a ambição dos cibercriminosos cresceram rapidamente e de forma (até) algo desmesurada. Hoje, observamos uma variedade de métodos de ataque por ransomware, que vai desde ataques altamente complexos, personalizados e direcionados a grandes empresas, até a campanhas de ransomware “as a service” (RaaS), onde grupos cibercriminosos que não detenham o seu próprio malware – ransomware – podem comprar um “kit” RaaS através da dark web, inclusive com suporte 24 horas por dia, 7 dias por semana, a baixo custo, e assim aproveitar o malware para desenvolver ciberataques da sua autoria e proveito próprio.

Esta evolução também é visível na metodologia dos ciberataques. Por exemplo, o ransomware de extorsão tripla é um tipo de ciberataque que adiciona um terceiro vetor de ataque e o potencial para um segundo – ou terceiro – resgate. Este terceiro vetor de ataque pode ser um ataque distribuído de negação de serviço (DDoS) ou de intimidação de terceiros (clientes, colaboradores, etc.) cuja exposição dos dados roubados possa também impactar esses mesmos. Os ciberataques de ransomware podem ainda beneficiar do uso de algoritmos mais eficazes assente em inteligência artificial (IA) para identificar alvos cada vez mais valiosos, e em simultâneo, otimizar as suas táticas de infiltração e movimentação lateral dentro da própria organização. Estima-se que, com o recurso a IA Generativa, os ciberataques de ransomware se tornem bastante mais sofisticados e eficazes, através de chatbots – malware desenvolvido pela IA – e algoritmos de Machine Learning.

Em termos de alvos, se antes seriam geralmente, organizações com um baixo nível de cibersegurança, atualmente, os grupos criminosos têm como alvos preferenciais, as grandes organizações e serviços essenciais à comunidade, incluindo hospitais, sistemas de transporte, comunicações, e também, a própria administração pública. A mudança para alvos high profile deve-se, sobretudo, à perceção de que essas entidades possuem maior capacidade económica, ou seja, maior proveito, e igualmente, à necessidade, ou até obrigação, de restaurar a funcionalidade dos seus sistemas no menor espaço de tempo possível, tornando-os mais vulneráveis a chantagem por parte do grupo cibercriminoso.

O impacto do ransomware na administração pública é particularmente grave, uma vez que estas instituições são responsáveis por serviços críticos essenciais à vida em sociedade. Ataques a sistemas governamentais podem paralisar serviços críticos, desde a emissão de documentos até à gestão de infraestruturas vitais como redes de transporte, telecomunicações e saúde pública. Além do transtorno imediato, os efeitos a longo prazo podem incluir a perda da confiança pública, altos custos de recuperação e ainda, um aumento significativo nos investimentos necessários para fortalecer a sua resiliência a ciberataques.

Em resposta a esta ameaça crescente de ransomware, várias medidas preventivas têm sido (e devem ser) adotadas quer ao nível governamental, quer ao nível corporativo. Governos e o tecido empresarial têm feito um esforço assinalável para implementar estratégias de cibersegurança mais rigorosas, que entrelaçam tecnologia com literacia digital. Não existe uma vacina mágica, nem um investimento único, mas sim, a necessidade de implementar um modelo evolutivo constante em todas as matérias que permitam progredir a maturidade em cibersegurança. É um processo continuo, que abrange tecnologia, literacia e cooperação internacional.

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