Por que os ataques de ransomware estão se tornando mais comuns a cada ano?

Resposta rápida: Os ataques de ransomware estão aumentando porque os grupos cibercriminosos evoluíram de agentes desorganizados e oportunistas para operações disciplinadas que usam automação para atacar muitas vítimas com eficiência e extrair pagamento rapidamente.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

De startups caóticas a operações organizadas

Quando o ransomware se tornou pela primeira vez uma ameaça generalizada, muitos atacantes eram inexperientes. Uma onda de indivíduos recém-desempregados durante a era da pandemia tentou a sorte no cibercrime, muitas vezes com resultados inconsistentes. Como em qualquer setor emergente, apenas os operadores mais organizados e capazes sobreviveram àquele período inicial de seleção. Com o tempo, esses grupos passaram a funcionar menos como oportunistas dispersos e mais como empresas estruturadas focadas em receita consistente.

Até 2024, essa maturidade se traduziu em forte dependência da automação. Operações de ransomware já estabelecidas agora usam ferramentas automatizadas para incorporar participantes menos experientes aos seus ataques, mantendo ainda assim processos eficientes e repetíveis. Isso permitiu que escalassem sua atividade muito além do que uma pequena equipe de hackers habilidosos conseguiria realizar manualmente.

Calibrando o ataque para o máximo retorno financeiro

Uma parte fundamental dessa evolução é aprender a dimensionar corretamente um ataque. Se uma invasão for muito pequena, uma equipe de TI bem preparada pode simplesmente restaurar os

sistemas e evitar qualquer pagamento. Se um ataque for muito abrangente, eliminando toda a infraestrutura da empresa, pode não haver nenhum negócio viável restante para efetuar o pagamento do resgate. Os grupos modernos de ransomware buscam um meio-termo: disrupção suficiente para pressionar a empresa a pagar rapidamente, sem causar tantos danos a ponto de tornar a recuperação ou a negociação irrelevantes.

Por que a automação impulsiona esse aumento

Uma vez que o processo de ataque pode ser automatizado, os cibercriminosos deixam de se contentar em perseguir uma única vítima por vez. Usando ferramentas que se assemelham a inteligência artificial, aprendizado de máquina e automação robótica de processos, eles conseguem atingir dezenas ou centenas de organizações em paralelo. Muitas vítimas optam por não divulgar publicamente os incidentes, permitindo que os atacantes concluam um ciclo de extorsão e passem para novos alvos. Esse modelo de negócio escalável e repetível — e não qualquer tecnologia nova isolada — é o principal motivo pelo qual os ataques de ransomware continuam a aumentar.

https://player.vimeo.com/video/1043463561?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Revision #3
Created 2026-07-24 06:14:21 UTC by Dennis Underwood
Updated 2026-11-24 15:50:07 UTC by Dennis Underwood