O que realmente acontece quando o ransomware atinge um servidor de empresa?

Resposta curta: Quando o ransomware atinge um servidor, os invasores normalmente desativam primeiro os seus serviços e, em seguida, encriptam os seus dados enquanto cortam o acesso das equipas de TI e de segurança, impedindo qualquer intervenção — por vezes utilizando dezenas ou mesmo centenas de estações de trabalho comprometidas para executar a encriptação remotamente.

Os Primeiros Sinais de um Ataque

Um dos primeiros indicadores de que um servidor foi comprometido é a perda súbita de serviço. Como os invasores sabem que o ransomware pode corromper acidentalmente ficheiros durante o processo de encriptação, muitos optam por desligar deliberadamente as aplicações em execução num servidor antes de iniciar a encriptação. Isto significa que os funcionários ou clientes que dependem desse sistema — seja uma plataforma de processamento salarial, uma aplicação web ou outro serviço crítico para o negócio — podem notar uma interrupção antes de alguém perceber que um incidente de segurança está em curso.

Bloquear os Defensores Enquanto a Encriptação se Propaga

Assim que o ataque está em curso, o ransomware começa a encriptar os dados armazenados no servidor. Para impedir que as equipas de segurança ou os administradores intervenham, os invasores bloqueiam frequentemente o acesso à rede do servidor, isolando-o das pessoas que normalmente responderiam à ameaça. Esta tática dá ao invasor tempo para concluir a encriptação dos ficheiros antes que os defensores possam agir.

As Estações de Trabalho Podem Ser o Verdadeiro Ponto Fraco

Curiosamente, o servidor em si nem sempre é a origem do perigo. Em muitos casos, os invasores comprometem um grande número de estações de trabalho de funcionários — por vezes 50, 70 ou mais — que já têm acesso legítimo ao servidor. Estas estações de trabalho são depois utilizadas simultaneamente para encriptar remotamente os dados do servidor. Como o ataque é lançado a partir de múltiplos pontos finais em simultâneo, as estações de trabalho ligadas ao servidor representam muitas vezes uma vulnerabilidade maior do que a própria infraestrutura do servidor.

Este padrão evidencia por que razão a defesa contra ransomware não pode centrar-se apenas nos servidores. A segurança de terminais em todos os dispositivos com acesso ao servidor desempenha um papel fundamental para impedir os ataques antes que a encriptação se propague. O FortressAI da Cyber Crucible foi concebido para identificar e interromper estes comportamentos nas fases mais iniciais, quer a ameaça se origine num servidor, quer se propague a partir de estações de trabalho ligadas.

https://player.vimeo.com/video/1041172405?texttrack=pt

Ver no Vimeo · Legendas: Inglês, Français, Español, العربية

Revision #2
Created 2026-07-24 06:12:36 UTC by Dennis Underwood
Updated 2026-08-06 18:37:53 UTC by Dennis Underwood