Por que o ransomware ataca arquivos compartilhados antes de atingir meu desktop?

Resposta rápida: Quando um ransomware infecta uma estação de trabalho individual, essa máquina raramente é o alvo real. Os atacantes usam a infecção inicial como ponto de lançamento para alcançar recursos de rede compartilhados, e só criptografam ou danificam o desktop local depois de já terem atacado dados de maior valor em outros locais.

Por que o desktop é a última parada, não a primeira

Um equívoco comum é achar que, se o ransomware chega ao computador de um funcionário específico, os arquivos desse funcionário são o que os atacantes desejam. Na realidade, o malware é programado para olhar além da máquina local quase imediatamente. Uma vez que consegue se estabelecer, ele começa a escanear a rede em busca de recursos acessíveis com maior valor, como servidores de arquivos, wikis internas ou bancos de dados contendo informações de clientes. Criptografar ou exfiltrar esses dados centralizados é o verdadeiro objetivo, pois isso afeta muito mais a organização do que a pasta de um único usuário.

A nota de resgate chega por último, não primeiro

Como os atacantes priorizam os dados de toda a rede antes de tocar no dispositivo de origem, o funcionário que foi infectado costuma ser a última pessoa a perceber que algo está errado. Quando uma nota de resgate aparece na tela dessa pessoa, os atacantes normalmente já terminaram de criptografar ou roubar dados em grande parte da infraestrutura da empresa. Essa sequência é intencional. Ela permite que os atacantes causem o máximo de dano operacional antes que alguém na organização tenha a chance de detectar a intrusão ou responder a ela. A nota de resgate visível é essencialmente um sinal de que o dano mais sério já ocorreu nos bastidores.

O que isso significa para a defesa

Fotos ou documentos pessoais armazenados localmente em um desktop costumam ser o alvo menos importante em um ataque de ransomware, mesmo que possam ser o sinal mais visível de que ele ocorreu. Uma defesa eficaz precisa levar esse padrão em conta, concentrando-se em detectar e interromper atividades maliciosas o mais cedo possível, antes que possam alcançar sistemas compartilhados. O FortressAI da Cyber Crucible foi desenvolvido levando em conta essa sequência de ataque, com o objetivo de intervir nos estágios iniciais de uma intrusão, em vez de apenas reagir quando a criptografia se torna visível em máquinas individuais.

https://player.vimeo.com/video/1043466243?texttrack=pt

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

Revision #2
Created 2026-07-24 06:12:48 UTC by Dennis Underwood
Updated 2026-08-06 18:37:55 UTC by Dennis Underwood