O que realmente acontece nos momentos durante um ataque de ransomware?

Resposta curta: A fase real de encriptação de um ataque de ransomware é notavelmente rápida, muitas vezes concluída em cerca de 60 a 90 segundos após ser desencadeada, embora os atacantes passem um tempo significativo e não observado antecipadamente, posicionando-se dentro de uma rede. No momento em que sintomas visíveis surgem, o dano já está a desenrolar-se em tempo real, razão pela qual a deteção tem de ocorrer antes do desencadeamento final, e não depois.

A Calmaria Antes do Ataque

Antes de o ransomware ser ativado, os atacantes normalmente passam tempo a mover-se silenciosamente pelos sistemas de uma empresa, identificando dados valiosos, desativando cópias de segurança e criando as condições necessárias para um ataque bem-sucedido. Este trabalho preparatório pode passar despercebido porque as operações normais da empresa continuam como habitual. A rede pode parecer estável e saudável até ao momento em que o atacante decide lançar a fase final. Tal como um silêncio inquietante mesmo antes de algo catastrófico acontecer, este período de calma pode ser enganador, uma vez que não reflete a disrupção prestes a ocorrer.

O Início Rápido dos Danos

Uma vez lançado, um incidente de ransomware pode desenrolar-se em menos de dois minutos. Nesse curto período, os colaboradores podem notar quebras súbitas: o e-mail deixa de funcionar, os sistemas telefónicos ficam silenciosos, as aplicações comportam-se de forma errática ou as ligações de rede tornam-se instáveis. Estes são sintomas de encriptação e comprometimento do sistema a acontecer simultaneamente em todo o ambiente. Como o processo se move tão rapidamente, tipicamente não há tempo suficiente para uma intervenção manual depois de este começar.

Por Que Razão Alguns Sistemas Continuam a Funcionar

Um pormenor inquietante de muitos incidentes de ransomware é que nem tudo falha ao mesmo tempo. Alguns serviços podem continuar a funcionar normalmente mesmo enquanto outros colapsam. Isto acontece frequentemente porque esses sistemas não afetados são exatamente onde o atacante ainda está a operar, usando-os como ponto de apoio ou área de preparação. Reconhecer este padrão é importante, uma vez que assumir que um problema é "apenas parcial" pode criar uma falsa sensação de segurança enquanto o comprometimento está ativamente em curso. A prevenção eficaz depende da identificação e paragem da atividade maliciosa antes de a fase destrutiva final começar, uma vez que, uma vez desencadeada, a janela para agir é extremamente curta.

https://player.vimeo.com/video/1046658956?texttrack=pt

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

Revision #2
Created 2026-07-24 06:12:23 UTC by Dennis Underwood
Updated 2026-08-06 18:37:51 UTC by Dennis Underwood