Por que o roubo de credenciais e de identidade é mais perigoso do que a criptografia de ransomware?

Resposta curta: A criptografia de ransomware é a etapa visível e final de um ataque, mas o dano real muitas vezes ocorre antes e passa despercebido, quando os atacantes coletam automaticamente senhas, tokens de sessão, chaves e carteiras de criptomoedas. A Cyber Crucible concentra-se em detectar e interromper essa fase inicial e oculta, em vez de esperar pelo momento em que os dados são bloqueados.

Por que as ferramentas de segurança muitas vezes não percebem a ameaça maior

Muitos produtos de segurança são desenvolvidos para reagir à criptografia, pois essa é a parte do ataque que uma empresa realmente percebe—os sistemas param de funcionar, os arquivos ficam ilegíveis e as operações são interrompidas. Essa interrupção visível naturalmente atrai mais atenção e investimento. No entanto, a criptografia costuma ser a última ação tomada pelo atacante, não a primeira. Quando a empresa percebe os efeitos do ransomware, o atacante geralmente já concluiu a parte mais importante da invasão: coletar silenciosamente dados relacionados à identidade, como credenciais, tokens de autenticação, chaves de criptografia e acesso a carteiras digitais. Essa fase inicial não causa nenhuma interrupção visível, por isso tende a ser subestimada, mesmo proporcionando aos atacantes acesso duradouro e repetível à rede.

O primeiro estágio silencioso de um ataque

Os ataques modernos são amplamente automatizados, e a fase de roubo de identidade pode ser concluída em apenas alguns segundos em toda a organização. Como não há interrupção imediata

dos negócios, essa etapa carece da urgência e da visibilidade que a criptografia de ransomware gera, tornando-a fácil de ser ignorada. No entanto, é essa etapa que dá aos atacantes a capacidade de retornar quando quiserem e causar mais danos, incluindo a implantação de ransomware posteriormente.

Como a Cyber Crucible aborda essa lacuna

A Cyber Crucible foi projetada para detectar acessos não autorizados a dados de identidade no exato momento em que ocorrem, em vez de esperar que a criptografia comece. Como essa atividade acontece de forma tão rápida e silenciosa, um esforço significativo de engenharia foi dedicado a tornar a detecção rápida e precisa—identificando quem está acessando dados sensíveis de identidade sem retardar as operações comerciais cotidianas ou a atividade dos usuários.

https://player.vimeo.com/video/1141670023?texttrack=pt

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

Revision #2
Created 2026-07-24 06:15:09 UTC by Dennis Underwood
Updated 2026-08-06 18:38:14 UTC by Dennis Underwood