Quem os atacantes de ransomware realmente visam hoje?

Resposta curta: Os operadores de ransomware já não se concentram apenas em organizações grandes e de alto perfil. A automação e as ferramentas orientadas por IA tornaram lucrativo visar empresas de praticamente qualquer dimensão, o que significa que a maioria das organizações deve presumir que é um alvo potencial.

Como a seleção de alvos mudou desde 2020

Nos primeiros dias do ransomware moderno, executar um ataque desde o acesso inicial até à extorsão exigia hackers experientes e qualificados, trabalhando em grande parte manualmente. Isso limitava o número de atacantes capazes e mantinha o foco em alvos grandes e de elevado valor, onde o retorno justificava o esforço.

À medida que a procura crescia, grupos de hackers estabelecidos começaram a operar mais como negócios em expansão. Em vez de depender apenas de um pequeno número de operadores de elite, começaram a criar programas de ransomware-as-a-service que empacotam métodos de ataque comprovados em manuais repetíveis e automatizados. Isto permitiu que operadores menos experientes conduzissem campanhas eficazes, de forma semelhante a um vendedor júnior que consegue ter sucesso utilizando um guião criado a partir dos métodos de um vendedor de topo.

Por que razão as organizações mais pequenas estão agora em risco

A automação, a aprendizagem automática (machine learning) e a automação robótica de processos permitem que estes operadores executem múltiplos ataques em simultâneo, geram negociações de resgate e gerem o apoio ao pagamento ou à recuperação em grande escala. Assim que estas funções se tornaram largamente automatizadas, atacar empresas mais pequenas também passou a ser lucrativo, uma vez que são máquinas — e não pessoas — que tratam da maior parte do contacto e do acompanhamento.

Esta mudança significa que os atacantes são menos seletivos. Os grandes alvos ("big game") continuam a atrair atenção devido à dimensão do potencial retorno, mas a atividade quotidiana destas operações criminosas assemelha-se cada vez mais à prospeção comercial de rotina: sistemas automatizados procuram continuamente qualquer organização que possa pagar. Os sistemas responsáveis pela seleção de alvos normalmente não têm qualquer conhecimento sobre quem ou o que o alvo realmente é, seja este uma grande empresa ou uma pequena organização sem fins lucrativos.

O que isto significa para as organizações

Uma vez que a seleção de alvos é largamente automatizada e indiscriminada, a questão mais relevante para a maioria das organizações não é se poderão ser especificamente escolhidas, mas sim o quão preparadas estão para uma eventual tentativa. Soluções como a Cyber Crucible, construídas sobre a FortressAI, foram concebidas para ajudar as organizações a detetar e travar o ransomware e ameaças relacionadas, independentemente da dimensão ou do perfil do alvo.

https://player.vimeo.com/video/1047715793?texttrack=pt

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

Revision #2
Created 2026-07-24 06:13:29 UTC by Dennis Underwood
Updated 2026-08-06 18:38:01 UTC by Dennis Underwood