Quem Corre Maior Risco de um Ataque de Ransomware e Por Que São Alvos?

Resposta curta: O risco de ransomware muitas vezes se resume a quem os "corretores de acesso" criminosos consideram mais fácil de invadir ou são especificamente pagos para invadir, o que significa que escolas, hospitais e fornecedores de infraestrutura com defesas mais fracas ou dados valiosos frequentemente estão no topo da lista.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como os Alvos São Escolhidos, Antes de Mais Nada

Por trás da maioria dos incidentes de ransomware existe um mercado que a maioria das pessoas nunca vê. Um grupo, frequentemente chamado de corretores de acesso inicial, passa seu tempo invadindo redes sem nenhum plano específico para o que acontece a seguir. Assim que conseguem se estabelecer, eles anunciam esse acesso para venda, descrevendo exatamente o que controlam, como direitos administrativos sobre ferramentas de segurança, a capacidade de desativar proteções antivírus, ou acesso a uma grande parcela dos dispositivos de uma organização. Eles podem descrever, por exemplo, ter comprometido a frota de dispositivos de um distrito escolar ou as ferramentas de acesso remoto de um fornecedor de TI. Compradores, que vão desde grupos de roubo de dados até operadores de ransomware e agentes patrocinados por estados, então fazem lances por esse acesso com base em quão valioso e completo ele parece.

Quando os Ataques São Encomendados, Não Apenas Oportunistas

Existe também um segundo padrão, mais direcionado. Aqui, um comprador, como um grupo de ransomware ou um agente estatal, faz um pedido específico: encontrar e comprometer um determinado número de organizações que atendam a certos critérios, como hospitais de um determinado porte em uma determinada região, ou fornecedores de serviços públicos como estações de tratamento de água. Os corretores de acesso então tratam isso como uma tarefa de vendas, caçando ativamente organizações que se encaixem no perfil. Assim que conseguem, vendem esse acesso ao solicitante original, mesmo que os dois lados normalmente nunca interajam diretamente nem saibam a identidade um do outro. É por isso que agrupamentos repentinos de ataques contra organizações semelhantes, como vários hospitais em uma mesma região, frequentemente refletem uma ordem de compra coordenada, e não uma coincidência.

Por Que Isso Importa para a Defesa

Como o direcionamento de alvos pode ser tanto oportunista quanto especificamente encomendado, qualquer organização com controles de segurança fracos, dados sensíveis ou serviços críticos pode se tornar um alvo, independentemente do porte ou do setor. Compreender essa dinâmica entre compradores e vendedores reforça por que defesas proativas e sempre ativas importam mais do que reagir depois que uma violação já foi vendida ao maior lance.

https://player.vimeo.com/video/1047715835?texttrack=pt

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

Revision #3
Created 2026-07-24 06:13:43 UTC by Dennis Underwood
Updated 2026-11-24 15:50:11 UTC by Dennis Underwood