

De onde realmente vêm os ataques de ransomware?

Resposta curta: Os operadores de ransomware não estão confinados a um punhado de países bem conhecidos; a automação e as ferramentas criminosas baratas agora permitem que os atacantes operem a partir de praticamente qualquer lugar do mundo.

A história simplista da mídia não corresponde às evidências

A cobertura noticiosa frequentemente aponta para um único país ou região como a origem dos ataques de ransomware, pois isso resulta em uma manchete rápida e fácil de assimilar. Na prática, a experiência direta na resposta a incidentes ativos conta uma história mais complexa. Quando a Cyber Crucible começou a lidar com casos ativos de ransomware, nossa equipe recebeu uma ampla variedade de chamadas telefônicas relacionadas aos ataques—muitas originadas de telefones pré-pagos ou descartáveis ("burner phones") sem histórico de propriedade rastreável. Essas chamadas vinham de diversas regiões diferentes, incluindo o Sul da Ásia, o Oriente Médio, partes da Europa, a América do Sul e até mesmo a América do Norte. Alguns interlocutores eram operadores de baixo nível, enquanto outros pareciam ser os verdadeiros desenvolvedores do malware, ocasionalmente participando de conversas surpreendentemente profissionais, entre pares, sobre os detalhes técnicos de seus ataques.

A automação reduziu a barreira de entrada

Embora certas regiões do mundo ainda possam produzir uma parcela desproporcional de desenvolvedores de ransomware habilidosos, o surgimento de kits de ransomware como serviço, ferramentas de automação e alcance básico assistido por IA tornou muito mais fácil a participação de agentes menos sofisticados. Alguém com habilidade técnica limitada agora pode alugar infraestrutura de ataque, comprar acesso roubado à rede de corretores de acesso inicial e conduzir uma campanha de extorsão com investimento inicial mínimo. Isso efetivamente abriu as portas para que criminosos oportunistas localizados em qualquer lugar possam participar, em vez de restringir a atividade de ransomware a um pequeno grupo de agentes vinculados a estados-nação.

Por que isso importa para a defesa

A gíria regional, os padrões linguísticos e o comportamento de chamadas observados durante esses incidentes reforçam que os atacantes são geograficamente diversos, não limitados a uma única nação "agente malicioso". Compreender o ransomware como uma empresa criminosa globalmente distribuída e impulsionada pela automação—em vez de uma narrativa geopolítica simplista—leva a estratégias de defesa mais bem informadas e a uma visão mais clara do risco real que as organizações enfrentam.

<https://player.vimeo.com/video/1047715735?texttrack=pt>

[Assistir no Vimeo](#) · Legendas: Inglês, Francês, Espanhol, Árabe

Revision #2

Created 2026-07-24 06:13:15 UTC by Dennis Underwood

Updated 2026-08-06 18:37:59 UTC by Dennis Underwood