

¿Quién corre mayor riesgo de sufrir un ataque de ransomware y por qué son elegidos como objetivo?

Respuesta breve: el riesgo de ransomware a menudo depende de a quién los "corredores de acceso" criminales encuentran más fácil de vulnerar o a quién se les paga específicamente por vulnerar, lo que significa que las escuelas, los hospitales y los proveedores de infraestructura con defensas más débiles o datos valiosos suelen encabezar la lista.

Cómo se eligen los objetivos en primer lugar

Detrás de la mayoría de los incidentes de ransomware existe un mercado que la mayoría de las personas nunca ve. Un grupo, a menudo denominado corredores de acceso inicial, dedica su tiempo a irrumpir en las redes sin ningún plan específico sobre lo que sucederá a continuación. Una vez que han obtenido un punto de apoyo, anuncian ese acceso para su venta, describiendo exactamente qué controlan, como derechos administrativos sobre herramientas de seguridad, la capacidad de desactivar protecciones antivirus o el acceso a una gran parte de los dispositivos de una organización. Podrían describir, por ejemplo, haber comprometido la flota de dispositivos de un distrito escolar o las herramientas de acceso remoto de un proveedor de TI. Los compradores, que van desde grupos de robo de datos hasta operadores de ransomware y actores patrocinados por estados, luego puján por ese acceso según lo valioso y completo que parezca.

Cuando los ataques son encargados, no solo oportunistas

También existe un segundo patrón, más dirigido. Aquí, un comprador, como un grupo de ransomware o un actor estatal, presenta una solicitud específica: encontrar y comprometer un número determinado de organizaciones que cumplan ciertos criterios, como hospitales de un tamaño particular en una región específica, o proveedores de servicios públicos como plantas de

tratamiento de agua. Los corredores de acceso entonces tratan esto como una tarea de ventas, buscando activamente organizaciones que se ajusten al perfil. Una vez que tienen éxito, venden ese acceso al solicitante original, aunque ambas partes por lo general nunca interactúan directamente ni conocen la identidad de la otra. Por eso, los grupos repentinos de ataques contra organizaciones similares, como varios hospitales en una misma región, a menudo reflejan una orden de compra coordinada en lugar de una coincidencia.

Por qué esto importa para la defensa

Debido a que la selección de objetivos puede ser tanto oportunista como específicamente encargada, cualquier organización con controles de seguridad débiles, datos sensibles o servicios críticos puede convertirse en un objetivo, independientemente de su tamaño o sector. Comprender esta dinámica entre compradores y vendedores subraya por qué las defensas proactivas y siempre activas importan más que reaccionar después de que una vulneración ya haya sido vendida al mejor postor.

<https://player.vimeo.com/video/1047715835?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

Revision #2

Created 2026-07-24 02:14:57 UTC by Dennis Underwood

Updated 2026-08-06 18:34:52 UTC by Dennis Underwood