

¿De dónde provienen realmente los ataques de ransomware?

Respuesta breve: Los operadores de ransomware no se limitan a un puñado de países conocidos; la automatización y las herramientas delictivas económicas permiten ahora que los atacantes operen desde casi cualquier parte del mundo.

La historia simplificada de los medios no coincide con la evidencia

La cobertura noticiosa suele señalar a un solo país o región como origen de los ataques de ransomware porque eso permite un titular rápido y fácil de digerir. En la práctica, la experiencia directa respondiendo a incidentes en curso cuenta una historia mucho más compleja. Cuando Cyber Crucible comenzó a gestionar casos activos de ransomware, nuestro equipo recibió una amplia variedad de llamadas telefónicas relacionadas con los ataques, muchas de ellas provenientes de teléfonos prepago o desechables ("de usar y tirar") sin historial de propiedad rastreable. Estas llamadas provenían de muchas regiones diferentes, incluyendo el sur de Asia, Oriente Medio, partes de Europa, Sudamérica e incluso Norteamérica. Algunos de los interlocutores eran operadores de bajo nivel, mientras que otros parecían ser los verdaderos desarrolladores del malware, quienes en ocasiones mantenían conversaciones sorprendentemente profesionales, de igual a igual, sobre los detalles técnicos de sus ataques.

La automatización ha reducido la barrera de entrada

Si bien ciertas regiones del mundo pueden seguir produciendo una proporción desmedida de desarrolladores de ransomware con gran habilidad técnica, el auge de los kits de ransomware como servicio, las herramientas de automatización y el uso básico de asistencia de IA para las comunicaciones ha facilitado enormemente la participación de actores menos sofisticados. Alguien con habilidades técnicas limitadas puede ahora alquilar infraestructura de ataque, comprar acceso robado a redes a través de intermediarios de acceso inicial ("initial access brokers") y ejecutar una campaña de extorsión con una inversión inicial mínima. Esto ha abierto efectivamente la puerta a que delincuentes oportunistas ubicados en cualquier lugar participen, en lugar de restringir la actividad del ransomware a un pequeño conjunto de grupos vinculados a estados-nación.

Por qué esto importa para la defensa

La jerga regional, los patrones de lenguaje y el comportamiento de las llamadas observados durante estos incidentes refuerzan la idea de que los atacantes están geográficamente dispersos, y no limitados a una sola nación "actor malicioso". Entender el ransomware como una empresa criminal distribuida globalmente e impulsada por la automatización, en lugar de una narrativa geopolítica simplista, conduce a estrategias de defensa mejor fundamentadas y a una visión más clara del riesgo real que enfrentan las organizaciones.

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

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

Revision #2

Created 2026-07-24 02:14:29 UTC by Dennis Underwood

Updated 2026-08-06 18:34:48 UTC by Dennis Underwood