¿A quién atacan realmente hoy los ciberdelincuentes de ransomware?

Respuesta breve: los operadores de ransomware ya no se centran únicamente en organizaciones grandes y de alto perfil. La automatización y las herramientas basadas en IA han hecho rentable atacar a empresas de casi cualquier tamaño, lo que significa que la mayoría de las organizaciones deben asumir que son un objetivo potencial.

Cómo ha cambiado la selección de objetivos desde 2020

En los primeros días del ransomware moderno, llevar a cabo un ataque desde el acceso inicial hasta la extorsión requería hackers expertos y experimentados que trabajaban en gran medida de forma manual. Eso limitaba el número de atacantes capaces y mantenía el foco en objetivos grandes y de alto valor, donde el beneficio justificaba el esfuerzo.

A medida que creció la demanda, los grupos de hackers ya establecidos comenzaron a operar más como negocios en expansión. En lugar de depender únicamente de un pequeño número de operadores expertos, empezaron a crear programas de ransomware como servicio que empaquetan métodos de ataque probados en manuales de estrategias repetibles y automatizados. Esto permitió que operadores con menos experiencia llevaran a cabo campañas efectivas, de manera similar a como un vendedor junior puede tener éxito utilizando un guion elaborado a partir de los métodos de un vendedor destacado.

Por qué las organizaciones más pequeñas ahora están en riesgo

La automatización, el aprendizaje automático y la automatización robótica de procesos permiten a estos operadores ejecutar muchos ataques a la vez, gestionar las negociaciones de rescate y administrar el soporte de pago o recuperación a gran escala. Una vez que estas funciones se automatizaron en gran medida, atacar a empresas más pequeñas también se volvió rentable, ya que son las máquinas —y no las personas— quienes gestionan la mayor parte del contacto y el

seguimiento.

Este cambio significa que los atacantes son menos selectivos. Los objetivos "de gran envergadura" siguen atrayendo atención debido al tamaño de un posible pago, pero la actividad cotidiana de estas operaciones criminales se asemeja cada vez más a la prospección de ventas rutinaria: sistemas automatizados que buscan continuamente cualquier organización que pueda pagar. Los sistemas que realizan la selección de objetivos generalmente no tienen conocimiento alguno de quién o qué es realmente el objetivo, ya sea una gran empresa o una pequeña organización sin fines de lucro.

Qué significa esto para las organizaciones

Dado que la selección de objetivos es en gran medida automatizada e indiscriminada, la pregunta más relevante para la mayoría de las organizaciones no es si podrían ser elegidas específicamente, sino qué tan preparadas están ante un eventual intento. Soluciones como Cyber Crucible, construidas sobre FortressAI, están diseñadas para ayudar a las organizaciones a detectar y detener el ransomware y las amenazas relacionadas, sin importar el tamaño o el perfil del objetivo.

https://player.vimeo.com/video/1047715793

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #1
Created 2026-07-24 02:14:44 UTC by Dennis Underwood
Updated 2026-07-24 02:14:44 UTC by Dennis Underwood