Who do ransomware attackers actually target today?

Short answer: Ransomware operators no longer focus only on large, high-profile organizations. Automation and AI-driven tools have made it profitable to target businesses of nearly any size, which means most organizations should assume they are a potential target.

How targeting has changed since 2020

In the early days of modern ransomware, carrying out an attack from initial access through extortion required skilled, experienced hackers working largely by hand. That limited the pool of capable attackers and kept the focus on large, high-value targets where the payoff justified the effort.

As demand grew, established hacking groups began operating more like scaling businesses. Rather than relying solely on a small number of elite operators, they started building ransomware-as-a-service programs that package proven attack methods into repeatable, automated playbooks. This let less experienced operators run effective campaigns, similar to how a junior salesperson can succeed using a script built from a top performer's methods.

Why smaller organizations are now at risk

Automation, machine learning, and robotic process automation allow these operators to run many attacks at once, handle ransom negotiations, and manage payment or recovery support at scale. Once these functions became largely automated, going after smaller companies became profitable too, since machines—not people—handle most of the outreach and follow-up.

This shift means attackers are less selective. Large "big game" targets still attract attention because of the size of a potential payout, but the everyday activity of these criminal operations increasingly resembles routine sales prospecting: automated systems continuously look for any organization that might pay. The systems doing the targeting typically have no awareness of who or what the target actually is, whether that's a major enterprise or a small nonprofit.

What this means for organizations

Because targeting is largely automated and indiscriminate, the more relevant question for most organizations is not whether they might be singled out, but how prepared they are for an eventual attempt. Solutions such as Cyber Crucible, built on FortressAI, are designed to help organizations detect and stop ransomware and related threats regardless of the size or profile of the target.

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

Watch on Vimeo · Captions: English, Français, Español, العربية

Revision #4
Created 2026-07-23 23:17:51 UTC by Dennis Underwood
Updated 2026-07-24 00:31:14 UTC by Dennis Underwood