Why are ransomware attacks becoming more common each year?

Short answer: Ransomware attacks are increasing because cybercriminal groups have evolved from disorganized, opportunistic actors into disciplined operations that use automation to attack many victims efficiently and extract payment quickly.

From chaotic startups to organized operations

When ransomware first became a widespread threat, many attackers were inexperienced. A wave of newly unemployed individuals during the pandemic era tried their hand at cybercrime, often with inconsistent results. As with any emerging industry, only the more organized and capable operators survived that early shakeout period. Over time, these groups began functioning less like scattered opportunists and more like structured businesses focused on consistent revenue.

By 2024, this maturity has translated into heavy reliance on automation. Established ransomware operations now use automated tools to bring less experienced participants into their attacks while still maintaining efficient, repeatable processes. This has allowed them to scale their activity well beyond what a small team of skilled hackers could accomplish manually.

Calibrating the attack for maximum payout

A key part of this evolution is learning how to size an attack correctly. If an intrusion is too minor, a well-prepared IT team can simply restore systems and avoid paying anything. If an attack is too extensive, wiping out entire company infrastructure, there may be no viable business left to issue a ransom payment at all. Modern ransomware groups aim for a middle ground: enough disruption to pressure a company into quick payment, without causing so much damage that recovery or negotiation becomes irrelevant.

Why automation drives the increase

Once an attack process can be automated, cybercriminals are no longer satisfied with pursuing a single victim at a time. Using tools that resemble artificial intelligence, machine learning, and robotic process automation, they can target dozens or hundreds of organizations in parallel. Many victims choose not to publicly disclose incidents, allowing attackers to complete a cycle of extortion and move on to new targets. This scaled, repeatable business model—rather than any single new technology—is the primary reason ransomware attacks continue to climb.

https://player.vimeo.com/video/1043463561

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

Revision #4
Created 2026-07-23 23:17:55 UTC by Dennis Underwood
Updated 2026-07-24 00:31:18 UTC by Dennis Underwood