

What actually happens when ransomware hits a company server?

Short answer: When ransomware strikes a server, attackers typically disable its services first, then encrypt its data while cutting off IT and security teams from stepping in—sometimes using dozens or even hundreds of compromised workstations to carry out the encryption remotely.

The First Signs of an Attack

One of the earliest indicators that a server has been compromised is a sudden loss of service. Because attackers understand that ransomware can accidentally corrupt files mid-encryption, many deliberately shut down the applications running on a server before the encryption process begins. This means employees or customers relying on that system—whether it's a payroll platform, a web application, or another business-critical service—may notice an outage before anyone realizes a security incident is underway.

Locking Out Defenders While Encryption Spreads

Once the attack is in motion, the ransomware begins encrypting the data stored on the server. To prevent security teams or administrators from intervening, attackers frequently block network access to the server, isolating it from the people who would normally respond to the threat. This tactic buys the attacker time to finish encrypting files before defenders can act.

Workstations Can Be the Real Weak Point

Interestingly, the server itself is not always where the danger originates. In many cases, attackers compromise a large number of employee workstations—sometimes 50, 70, or more—that already have legitimate access to the server. These workstations are then used simultaneously to encrypt the server's data remotely. Because the attack is launched from multiple endpoints at once, the

workstations connected to the server often represent a greater vulnerability than the server infrastructure itself.

This pattern highlights why ransomware defense can't focus solely on servers. Endpoint security across every device with server access plays a critical role in stopping attacks before encryption spreads. Cyber Crucible's FortressAI is built to identify and interrupt these behaviors at the earliest stages, whether the threat originates on a server or spreads from connected workstations.

<https://player.vimeo.com/video/1041172405?texttrack=en>

[Watch on Vimeo](#) · Captions: English, Français, Español, العربية

Revision #5

Created 2026-07-23 23:17:47 UTC by Dennis Underwood

Updated 2026-08-06 18:33:40 UTC by Dennis Underwood