Who Actually Runs Ransomware Attacks and How Do They Operate?

Short answer: Ransomware attacks are carried out by a loosely organized network of developers, resellers, and operators who function much like a business supply chain, and the most effective ones treat extortion as a professional trade rather than a personal grudge.

Ransomware as an Organized Supply Chain

Ransomware is rarely the work of a single hacker acting alone. Instead, it operates more like a distributed industry made up of malware developers who build the tools, resellers or affiliates who distribute access to that malware, and operators who carry out the actual attacks against victims. Each group plays a distinct role, similar to how a legitimate software vendor might rely on manufacturers, distributors, and sales teams. This layered structure is part of what makes ransomware resilient: disrupting one link in the chain doesn't necessarily stop the broader operation.

The Professionals vs. the Emotional Attackers

Not all attackers behave the same way once their attempts are blocked. Cyber Crucible has directly experienced this contrast. In one case, an attacker linked to Eastern Europe called after being stopped, treating the encounter as a technical puzzle to solve rather than a personal insult. That individual even referenced internal software details to prove they had reverse-engineered the product, then continued reaching out periodically afterward, discussing their operations almost as a peer would.

By contrast, another attacker connected to Bangladesh reacted with anger and hostility after being thwarted, resorting to insults rather than problem-solving. That contact did not continue engaging over time.

Why This Matters for Defense

These experiences suggest that the more "successful" and persistent threat actors tend to be the ones who approach ransomware as a business challenge—methodical, patient, and focused on finding workarounds. Understanding attackers as businesslike adversaries, rather than purely chaotic criminals, helps inform how defensive technology like Cyber Crucible's FortressAI is designed: to anticipate calculated attempts to bypass protections, not just isolated or emotionally driven attacks.

https://player.vimeo.com/video/1047715866

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

Revision #4
Created 2026-07-23 23:17:53 UTC by Dennis Underwood
Updated 2026-07-24 00:31:15 UTC by Dennis Underwood