Where do ransomware attacks actually come from?

Short answer: Ransomware operators are not confined to a handful of well-known countries; automation and cheap criminal tooling now let attackers operate from almost anywhere in the world.

The simple media story doesn't match the evidence

News coverage often points to a single country or region as the source of ransomware attacks because it makes for a quick, digestible headline. In practice, direct experience responding to live incidents tells a more complicated story. When Cyber Crucible began handling active ransomware cases, our team received a wide range of phone calls tied to the attacks—many originating from prepaid or disposable "burner" phones with no traceable ownership history. These calls came from many different regions, including South Asia, the Middle East, parts of Europe, South America, and even North America. Some callers were low-level operators, while others appeared to be the actual developers of the malware, occasionally engaging in surprisingly professional, peer-to-peer conversations about the technical details of their attacks.

Automation has lowered the barrier to entry

While certain regions of the world may still produce a disproportionate share of skilled ransomware developers, the rise of ransomware-as-a-service kits, automation tools, and basic AI-assisted outreach has made it far easier for less sophisticated actors to participate. Someone with limited technical skill can now rent attack infrastructure, purchase stolen network access from initial access brokers, and run an extortion campaign with minimal upfront investment. This has effectively opened the door for opportunistic criminals located anywhere to take part, rather than restricting ransomware activity to a small set of nation-state-linked groups.

Why this matters for defense

Regional slang, language patterns, and calling behavior observed during these incidents reinforce that attackers are geographically diverse, not limited to one "bad actor" nation. Understanding ransomware as a globally distributed, automation-driven criminal enterprise—rather than a simple geopolitical narrative—leads to better-informed defense strategies and a clearer picture of the real risk organizations face.

https://player.vimeo.com/video/1047715735

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

Revision #4
Created 2026-07-23 23:17:50 UTC by Dennis Underwood
Updated 2026-07-24 00:31:13 UTC by Dennis Underwood