

Who Is Most at Risk of a Ransomware Attack, and Why Are They Targeted?

Short answer: Ransomware risk often comes down to who criminal "access brokers" find easiest to breach or are specifically paid to breach, which means schools, hospitals, and infrastructure providers with weaker defenses or valuable data are frequently at the top of the list.

How Targets Get Chosen in the First Place

Behind most ransomware incidents is a marketplace most people never see. One group, often called initial access brokers, spends its time breaking into networks without any specific plan for what happens next. Once they've gained a foothold, they advertise that access for sale, describing exactly what they control, such as administrative rights to security tools, the ability to disable antivirus protections, or access to a large share of an organization's devices. They might describe, for example, having compromised a school district's device fleet or an IT vendor's remote access tools. Buyers, ranging from data-theft groups to ransomware operators to state-sponsored actors, then bid on that access based on how valuable and complete it appears.

When Attacks Are Ordered, Not Just Opportunistic

A second, more targeted pattern also exists. Here, a buyer, such as a ransomware group or a nation-state actor, puts in a specific request: find and compromise a set number of organizations matching certain criteria, such as hospitals of a particular size in a particular region, or utility providers like water treatment plants. Access brokers then treat this like a sales assignment, actively hunting for organizations that fit the profile. Once they succeed, they sell that access to the original requester, even though the two sides typically never interact directly or know each other's identities. This is why sudden clusters of attacks against similar organizations, such as multiple hospitals in one region, often reflect a coordinated buy order rather than coincidence.

Why This Matters for Defense

Because targeting can be either opportunistic or specifically commissioned, any organization with weak security controls, sensitive data, or critical services can become a target, regardless of size or industry. Understanding this buyer-and-seller dynamic underscores why proactive, always-on defenses matter more than reacting after a breach has already been sold to the highest bidder.

<https://player.vimeo.com/video/1047715835?texttrack=en>

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

Revision #5

Created 2026-07-23 23:17:52 UTC by Dennis Underwood

Updated 2026-08-06 18:33:50 UTC by Dennis Underwood