Why does ransomware attack shared files before it hits my desktop?

Short answer: When ransomware infects an individual workstation, that machine is rarely the actual target. Attackers use the initial infection as a launching point to reach shared network resources, and they only encrypt or damage the local desktop after they've already gone after higher-value data elsewhere.

Why the desktop is the last stop, not the first

A common misconception is that if ransomware lands on a specific employee's computer, that employee's files are what the attackers are after. In reality, the malware is programmed to look past the local machine almost immediately. Once it gains a foothold, it begins scanning the network for reachable resources with greater value, such as file servers, internal wikis, or databases containing customer information. Encrypting or exfiltrating this centralized data is the real objective, because it affects far more of the organization than any single user's folder.

The ransom note arrives last, not first

Because attackers prioritize network-wide data before touching the originating device, the employee who was infected is usually the last person to notice anything is wrong. By the time a ransom note appears on that person's screen, the attackers have typically already finished encrypting or stealing data across much of the company's infrastructure. This sequencing is intentional. It allows attackers to inflict maximum operational damage before anyone at the organization has a chance to detect the intrusion or respond. The visible ransom note is essentially a signal that the more serious damage has already occurred behind the scenes.

What this means for defense

Personal photos or documents stored locally on a desktop are typically the least important target in a ransomware attack, even though they may be the most visible sign of one. Effective defense

needs to account for this pattern by focusing on detecting and stopping malicious activity as early as possible, before it can reach shared systems. Cyber Crucible's FortressAI is built with this attack sequence in mind, aiming to intervene during the early stages of an intrusion rather than only reacting once encryption becomes visible on individual machines.

https://player.vimeo.com/video/1043466243?texttrack=en

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

Revision #5
Created 2026-07-23 23:17:48 UTC by Dennis Underwood
Updated 2026-08-06 18:33:42 UTC by Dennis Underwood