What actually happens in the moments during a ransomware attack?

Short answer: A ransomware attack's actual encryption phase is remarkably fast, often completing in roughly 60 to 90 seconds once triggered, though attackers spend significant unseen time beforehand positioning themselves inside a network. By the time visible symptoms appear, the damage is already unfolding in real time, which is why detection has to happen before the final trigger, not after.

The Calm Before the Attack

Before ransomware ever activates, attackers typically spend time quietly moving through a company's systems, identifying valuable data, disabling backups, and setting up the conditions needed for a successful strike. This groundwork can go unnoticed because normal business operations continue as usual. The network may look stable and healthy right up until the moment the attacker decides to launch the final stage. Much like an eerie silence right before something catastrophic happens, this quiet period can be deceiving, since it does not reflect the disruption about to occur.

The Rapid Onset of Damage

Once launched, a ransomware event can unfold in under two minutes. In that short window, employees may notice sudden outages: email stops working, phone systems go silent, applications behave erratically, or network connections become unstable. These are symptoms of encryption and system compromise happening simultaneously across the environment. Because the process moves so quickly, there is typically not enough time for a person to manually intervene once it begins.

Why Some Systems Keep Working

An unsettling detail of many ransomware incidents is that not everything fails at once. Some services may continue running normally even as others collapse. This is often because those unaffected systems are exactly where the attacker is still operating, using them as a foothold or

staging area. Recognizing this pattern matters, since assuming an issue is “only partial” can create a false sense of security while the compromise is actively in progress. Effective prevention depends on identifying and stopping malicious activity before the final destructive stage begins, since once triggered, the window for action is extremely short.

https://player.vimeo.com/video/1046658956

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

Revision #4
Created 2026-07-23 23:17:46 UTC by Dennis Underwood
Updated 2026-07-24 00:31:08 UTC by Dennis Underwood