Why can't traditional antivirus stop zero-day and fileless ransomware attacks?

Short answer: Signature-based security tools rely on recognizing known attack patterns, but modern attackers deliberately test their tools against those same defenses before deploying them, and increasingly they avoid dropping detectable files altogether. This combination of mutated, unrecognized threats and memory-only techniques has made traditional detection methods far less reliable.

The Problem With Relying on Known Signatures

Zero-day attacks are, by definition, new or altered enough that they fall outside what existing security tools already recognize. Vendors have long promised improvements in catching these threats, but attackers have an inherent advantage: they can access the same commercial security products that defenders use. Before launching a campaign, attackers routinely test their malware against popular detection tools, refining it until it slips past. This turns detection into a constantly moving target rather than a fixed defense.

Fileless Techniques Undermine Whitelisting

Attackers have also moved away from dropping obvious malicious executables onto a system. Instead, they hijack legitimate, trusted applications already approved by application whitelisting tools, running malicious activity through processes that security software assumes are safe. When this fileless approach is paired with rapidly mutating code, attacks can complete in a very short window—sometimes within half an hour—long before a human incident response team could realistically investigate.

Attackers Erase Their Own Tracks

In many cases, because the attack lives in memory rather than on disk, attackers wipe out logs, evidence, and even security sensors before finishing their operation. This is similar to a robber disabling security cameras and alarms before committing a crime: by the time anyone looks for evidence, the most useful visibility has already been destroyed. This mix of unpredictable attack methods and self-erasing evidence is why Cyber Crucible has invested significant effort into building an automated, scalable approach—one designed to capture the critical data needed to make accurate decisions before attackers can erase the trail, rather than depending on recognizing threats after the fact.

https://player.vimeo.com/video/1164197533

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

Revision #4
Created 2026-07-23 23:17:59 UTC by Dennis Underwood
Updated 2026-07-24 00:31:22 UTC by Dennis Underwood