

Why is capturing ransomware encryption keys no longer a valid defense?

Short answer: Key capture stopped being technically reliable in 2021. Modern ransomware avoids the operating system's standard encryption libraries, so there are no keys for a defensive tool to intercept — and even when keys are obtained, they often can't be applied.

How modern ransomware bypasses key capture

- **Custom libraries:** encryption code is compiled directly into the malware instead of calling OS libraries, so keys are generated and used entirely inside the attacker's own process — invisible to tools watching standard calls.
- **Unique implementations:** some strains use non-standard, per-execution encryption. Even a captured key can't be applied, because the algorithm itself is bespoke.
- **Streaming ciphers:** these are built on a fundamentally different concept from AES and are simply immune to AES key capture.

Cyber Crucible originally developed and patented key-capture technology, then presented the cryptanalysis showing its limits at BSides Pittsburgh in 2021. We moved on because the evidence said to.

The compliance problem too

Key capture requires storing encryption keys centrally — creating a single point of failure and a high-value target. A government could also compel access through a classified subpoena or national security letter, without your knowledge. That's a serious data-sovereignty risk on top of a defense that no longer works.

Revision #3

Created 2026-07-20 19:23:45 UTC by Dennis Underwood

Updated 2026-07-21 19:32:01 UTC by Dennis Underwood