RANSOMWARE DEFENSE

The Technical and Business Failures of Ransomware Key Capture Defense

A truly effective defense must focus on the entire attack lifecycle, not just the final act of encryption.

Dennis Underwood, Founder & CEO, Cyber Crucible · November 2026

EXECUTIVE SUMMARY

Ransomware defense that relies on capturing encryption keys has been both a technically invalid strategy since 2021 and an unsound business risk strategy from the start. A truly effective defense must focus on the entire attack lifecycle, not just the final act of encryption.

01 The Flawed Business Risk Model

The most significant business risk from a ransomware attack is not the ransom payment itself, but the substantial revenue loss and reputational damage resulting from a prolonged business continuity outage. The ransomware attack is the final, most visible step in a multi-stage intrusion. It begins with digital identity theft, where attackers compromise credentials to gain unauthorized network access. This is followed by data theft, where sensitive intellectual property, customer data, and other critical information are exfiltrated.

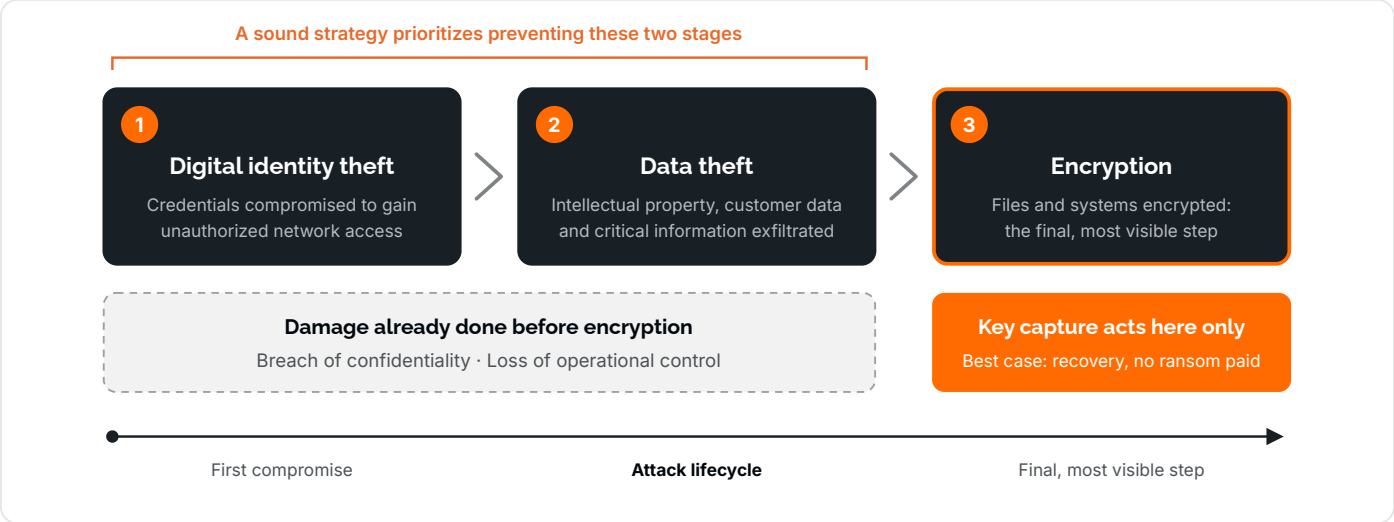

Figure 1. The three stages of a ransomware intrusion, and the one key capture can address

The encryption of files and systems is the third and final stage. At this point, the victim has already suffered a catastrophic breach of confidentiality and a loss of operational control. A key capture strategy, by its very nature, can only address the final stage of the attack. Its best-case outcome is to enable recovery and prevent ransom payment, but it does nothing to mitigate the prior damage from identity and data theft. A sound business risk strategy must prioritize preventing the initial compromise and data exfiltration to protect the company's most valuable assets and maintain continuous operations.

02 The Technical Inadequacy of Key Capture

Background: The Rise and Evolution of Key Capture

Between 2019 and 2020, ransomware groups, including state-sponsored actors and top-tier criminal syndicates, relied on AES encryption variants. Their methods evolved from using a single key for an entire campaign to generating a random AES key for each file or folder.

In response, Cyber Crucible developed and patented[1] an endpoint security product that could capture these encryption keys and encryption settings, collectively known as cryptovariables. The technology worked by monitoring the operating system's standard encryption libraries. It could detect ransomware, organize the thousands of keys and variables generated on each single machine, and automatically create and deploy decryption packages. This approach had notable successes, with one enterprise victim recovering company-wide in minutes. However, these successes prompted ransomware developers to design new techniques to bypass these defenses.

DEMONSTRATION VIDEOS

The Cyber Crucible YouTube channel has a variety of demonstration videos.[2]

By 2021, malware developers had released new ransomware strains that rendered key capture an unreliable defense.

BSIDES PITTSBURGH 2021

Cyber Crucible presented the cryptanalysis involving one of these new strains at BSides Pittsburgh in 2021.[3] Key capture was ineffective against these new strains.

How Modern Ransomware Bypasses Key Capture

Modern ransomware programs use sophisticated techniques to bypass traditional key capture tools, primarily by avoiding the use of the operating system's standard encryption libraries.

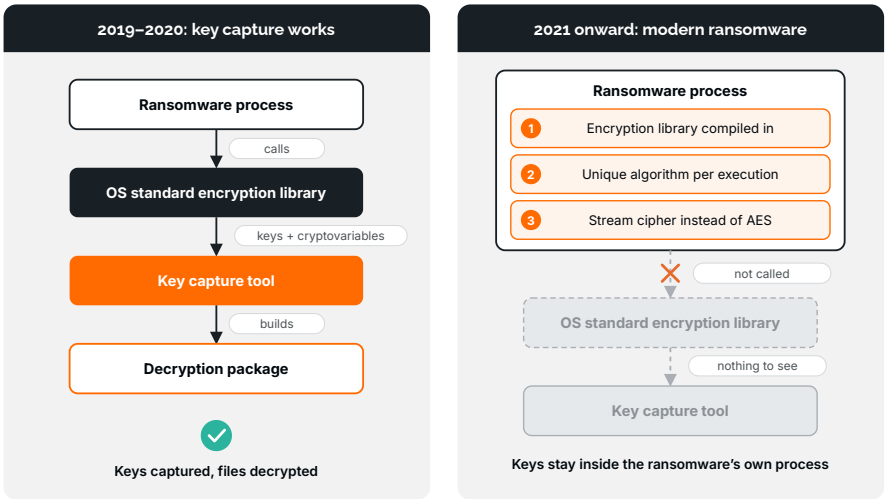

Figure 2. Why key capture stopped working

1. **Custom Libraries:** Programs can compile standard encryption libraries directly into their code rather than calling the operating system's libraries. This removes the visibility for security tools that rely on monitoring those standard calls. As a result, the keys and cryptovariables are generated and used within the ransomware's own process, making them invisible to the defensive tool.
2. **Unique Cryptographic Implementations:** Some ransomware uses customized, embedded encryption libraries. Even if a key capture tool were to somehow acquire the keys, it would not know how to correctly apply them for decryption because the encryption algorithm itself is non-standard and unique on a per-execution basis.
3. **Streaming Encryption Algorithms:** While AES and its peers are considered symmetric ciphers, different types of algorithms of similar strength and even faster speed are available to attackers and commercial users alike. Attackers have the option to include the use of different encryption algorithms such as streaming ciphers, which are completely immune to AES key capture as they are fundamentally built on a different encryption concept.

03 Compliance and Secrecy Risks of Key Capture

Beyond technical shortcomings, key capture solutions introduce significant compliance and security risks. To be effective, these tools must capture all encryption keys used on a machine—not just those generated by ransomware. This includes keys for business data, customer information, and employee files.

1. **Vendor and Regulatory Violations:** Storing and transmitting these highly sensitive keys to a third-party vendor's database can violate vendor EULAs, customer agreements, and regulatory compliance standards like GDPR, HIPAA, and CCPA. Such actions require extensive legal and contractual approvals, which can be difficult to obtain and maintain.
2. **Risk of Secret Access:** Even with all necessary approvals, the centralized storage of encryption keys creates a single point of failure and a high-value target for both criminal and state-sponsored attackers. Furthermore, a foreign or domestic government could use legal means, such as a classified subpoena or national security letter, to gain secret access to these keys without the customer's knowledge or consent. This presents a profound risk to data sovereignty and confidentiality, potentially exposing a company's most sensitive information to external parties without any transparency.

References

1. Cyber Crucible Inc., "Systems and methods for ransomware detection and mitigation," US 11,720,678 B2; EP 3 999 984 B1; CA 3,148,437 C; AU 2020315905 B2; JP 7393517 B2.
2. Cyber Crucible, demonstration videos, YouTube. https://www.youtube.com/CyberCrucible
3. Kyle Nehman, "Reverse Engineering Ransomware Protocols," BSides Pittsburgh 2021. Video recording, SecPgh on YouTube. https://www.youtube.com/watch?v=pfEq6GKjOkY

Read online (six languages): www.cybercrucible.com/intelligence-hub/ransomware-key-capture-defense-failures
Book a live technical demo: www.cybercrucible.com/demo