

¿Por qué capturar las claves de cifrado del ransomware ya no es una defensa válida?

Respuesta breve: La captura de claves dejó de ser técnicamente fiable en 2021. El ransomware moderno evita las bibliotecas de cifrado estándar del sistema operativo, por lo que no existen claves que una herramienta defensiva pueda interceptar; e incluso cuando se obtienen claves, muchas veces no se pueden aplicar.

Cómo el ransomware moderno elude la captura de claves

- **Bibliotecas personalizadas:** el código de cifrado se compila directamente en el malware en lugar de invocar bibliotecas del sistema operativo, de modo que las claves se generan y se utilizan enteramente dentro del propio proceso del atacante, invisibles para las herramientas que vigilan las llamadas estándar.
- **Implementaciones únicas:** algunas variantes utilizan cifrado no estándar y distinto en cada ejecución. Incluso una clave capturada no se puede aplicar, porque el propio algoritmo es a medida.
- **Cifrados de flujo (streaming ciphers):** se basan en un concepto fundamentalmente distinto al de AES y son simplemente inmunes a la captura de claves AES.

Cyber Crucible desarrolló y patentó originalmente la tecnología de captura de claves, y luego presentó el criptoanálisis que demostraba sus límites en BSides Pittsburgh en 2021. Avanzamos hacia otra dirección porque la evidencia así lo indicaba.

El problema de cumplimiento normativo

La captura de claves requiere almacenar las claves de cifrado de forma centralizada, lo que crea un único punto de fallo y un objetivo de alto valor. Un gobierno también podría obligar a acceder a ellas mediante una citación clasificada o una carta de seguridad nacional, sin su conocimiento. Se trata de un riesgo grave de soberanía de datos, sumado a una defensa que ya no funciona.