¿Cyber Crucible recopila claves de cifrado?

La respuesta más breve es: “No”.

Hubo un tiempo en que el software de Cyber Crucible no detenía el cifrado del ransomware antes de que ocurriera. En su lugar, recopilaba posibles claves de cifrado o configuraciones, y luego utilizaba una variedad de técnicas para determinar el paquete de descifrado adecuado (incluidas las claves) para descifrar después de un ataque de ransomware.

Desde el punto de vista de lo que recopilábamos, una buena analogía sería una cámara de video que tomara fotografías de todo lo que pudiera ser una clave para un casillero. Luego, un servidor realizaba los distintos cálculos matemáticos para determinar la clave y configuración adecuadas para el archivo correspondiente. Los científicos informáticos llamarían a esto aprendizaje automático.

Antes de dejar atrás el antiguo modelo de software de “recopilar todo lo que pudiera ser una clave”, organizábamos automáticamente miles de claves y configuraciones de cifrado por máquina durante los ataques.

El módulo de software de análisis criptográfico ha evolucionado ahora hacia un módulo analítico conductual adicional, que se utiliza como una fuente de datos para determinar si un software está intentando acceder de manera indebida a datos de identidad o “datos de datos” con el fin de robarlos o cifrarlos.

Revision #1
Created 2026-07-24 01:51:09 UTC by Dennis Underwood
Updated 2026-07-24 01:51:09 UTC by Dennis Underwood