

¿Por qué el robo de credenciales e identidad es más peligroso que el cifrado de ransomware?

Respuesta breve: El cifrado de ransomware es el paso visible y final de un ataque, pero el daño real suele ocurrir antes, de forma inadvertida, cuando los atacantes recopilan automáticamente contraseñas, tokens de sesión, claves y monederos de criptomonedas. Cyber Crucible se enfoca en detectar y detener esa etapa temprana y oculta, en lugar de esperar al momento en que los datos quedan bloqueados.

Por qué las herramientas de seguridad suelen pasar por alto la amenaza mayor

Muchos productos de seguridad están diseñados para reaccionar ante el cifrado porque esa es la parte del ataque que una empresa realmente percibe: los sistemas dejan de funcionar, los archivos se vuelven ilegibles y las operaciones se detienen. Esta interrupción visible naturalmente atrae la mayor atención e inversión. Sin embargo, el cifrado suele ser la última acción que realiza un atacante, no la primera. Para cuando una empresa nota los efectos del ransomware, el atacante generalmente ya ha completado la parte más consecuente de la intrusión: recopilar silenciosamente datos relacionados con la identidad, como credenciales, tokens de autenticación, claves de cifrado y acceso a monederos digitales. Esta fase temprana no causa una interrupción visible, por lo que tiende a subestimarse, aunque otorga a los atacantes un acceso duradero y repetible a la red.

La silenciosa primera etapa de un ataque

Los ataques modernos son en gran medida automatizados, y la fase de robo de identidad puede completarse en solo unos segundos en toda una organización. Debido a que no hay una interrupción inmediata del negocio, esta etapa carece de la urgencia y la visibilidad que genera el cifrado del ransomware, lo que facilita que pase desapercibida. Sin embargo, es esta etapa la que otorga a los atacantes la capacidad de regresar cuando lo deseen y provocar daños adicionales, incluida la implementación de ransomware más adelante.

Cómo aborda Cyber Crucible esta brecha

Cyber Crucible está diseñado para detectar el acceso no autorizado a datos de identidad en el momento en que ocurre, en lugar de esperar a que comience el cifrado. Debido a que esta actividad ocurre de forma tan rápida y silenciosa, se ha invertido un esfuerzo de ingeniería considerable para lograr que la detección sea tanto rápida como precisa, identificando quién accede a datos de identidad sensibles sin ralentizar las operaciones cotidianas del negocio ni la actividad de los usuarios.

<https://player.vimeo.com/video/1141670023?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

Revision #2

Created 2026-07-24 02:16:16 UTC by Dennis Underwood

Updated 2026-08-06 18:35:04 UTC by Dennis Underwood