INFORMACIÓN IMPORTANTE

Análisis Técnico y Guía de Contención: Incidente Instructure/Canvas

Cronología del Incidente

- **30 de Abril, 2026:** Fecha inicial del compromiso por parte de ShinyHunters.
- **7 de Mayo, 2026:** Fase de ataque activo con publicaciones no autorizadas dentro de la plataforma.

A diferencia de otras filtraciones pasivas, este incidente se mantiene como un ataque activo. Al día de hoy, se ha confirmado que los atacantes están publicando mensajes no autorizados directamente dentro de la plataforma Canvas. Esta capacidad de manipulación interna permite a los criminales interactuar con la comunidad académica desde una fuente "confiable", elevando exponencialmente el riesgo de ataques de ingeniería social dirigidos.

Perfil del Atacante

- **Actor:** ShinyHunters.
- **Modus Operandi:** Exfiltración masiva de bases de datos y toma de control de interfaces de comunicación interna.

Datos Comprometidos

- Inventario detallado de la información filtrada (Personal Identifiable Information - PII).

Como expertos con más de 20 años en el mercado, recomendamos:

- **Evaluación de Impacto:** Determinar si los IDs y correos de su institución figuran en los repositorios de ShinyHunters.
- **Revisión de Postura SaaS:** Auditar las configuraciones de seguridad actuales en plataformas de terceros.
- **Refuerzo de Identidad:** Implementar controles estrictos de acceso y revisión de privilegios para mitigar el uso de credenciales comprometidas.

Como expertos con más de 20 años protegiendo a las organizaciones más exigentes de México , nuestra prioridad es mantenerlo informado y brindarle el apoyo necesario para evaluar el alcance de este impacto. En Data Warden, estamos listos para colaborar con su equipo en la revisión de sus plataformas y el refuerzo de sus controles de seguridad, garantizando que su institución opere con total confianza.

Data Warden **+52 55 5438 2115**