¿Qué es una clave de API y qué ocurre si es robada?

Respuesta breve: Una clave de API es una cadena secreta que identifica y autoriza a un programa —en lugar de a una persona— cuando llama a un servicio. Una clave robada permite a un atacante realizar solicitudes en nombre de su aplicación, a menudo sin interacción del usuario, sin MFA y sin ninguna señal evidente de que algo esté mal.

Por qué son objetivos atractivos

- **No hay un humano en el ciclo.** Las claves están diseñadas para uso automatizado y desatendido, por lo que no hay ninguna solicitud de MFA que pueda interferir.
- **A menudo con un alcance demasiado amplio.** Las claves se emiten con frecuencia con más permisos de los que la tarea requiere.
- **De larga duración.** Muchas nunca se rotan, por lo que una clave robada hoy puede seguir funcionando meses después.
- **Almacenadas en lugares predecibles.** Archivos de configuración, variables de entorno y almacenes de credenciales: todos ellos ubicaciones que la automatización puede enumerar.

Consecuencias típicas

Según lo que autorice la clave: leer o exportar datos de clientes, enviar mensajes en nombre de su organización, gastar dinero contra una cuenta en la nube, o desplazarse hacia otros sistemas conectados.

Dado que las solicitudes están correctamente autenticadas, suelen aparecer en los registros como tráfico normal de la aplicación. La detección suele producirse mucho después de los hechos, mediante una factura o una auditoría.

Reducción de la exposición

Limite el alcance de las claves, rótelas regularmente y manténgalas fuera del control de versiones. Son buenas prácticas, pero limitan el radio de impacto en lugar de prevenir el robo.

Cyber Crucible se enfoca en el propio robo. Las ubicaciones de credenciales y configuración están protegidas, y un programa que las lee se evalúa en contexto: datos falsos o denegación ante una

extralimitación legítima, rechazo o suspensión ante un proceso desconocido o comprometido. En ninguno de los dos casos se entrega la clave.

Revision #1
Created 2026-07-24 01:44:13 UTC by Dennis Underwood
Updated 2026-07-24 01:44:13 UTC by Dennis Underwood