Cómo detectar y eliminar los Troyanos de acceso remoto

Protegé tus dispositivos de los **ciberataques**.

Este tipo de **malware** tiene como objetivo abrir una puerta a la información de tu negocio **sin que tú te des cuenta**.

Los troyanos de acceso remoto (RAT) son un tipo de **malware que se hace pasar por programas o aplicaciones conocidas**, las cuales en segundo plano están creando una vía de acceso remoto a tus dispositivos, y la información que se encuentra en ellos, sin levantar sospechas.

¿Cómo sucede?

En la mayoría de los casos, simplemente hemos sido engañados para **instalarlo nosotros mismos**.

A continuación te enseñamos algunas de las tácticas más comunes que pueden utilizar para confundirnos:

- Pedirte que hagas ***clic en enlaces*** o que descargues archivos, programas o apps maliciosos, por ejemplo: mostrándote un mensaje que te invita a realizar una actualización pendiente.
- Estando oculto en un **software gratuito** en una web de dudosa reputación.
- Haciéndote confiar en una llamada. *Ej. Alguien que se hace pasar por soporte informático te ofrece ayuda para instalar una nueva aplicación.*

El **malware** también puede infectar los dispositivos de su empresa a través de una **vulnerabilidad o fallo de seguridad** en los sistemas.

Minimiza los riesgos

- Únicamente descarga software y apps desde **sitios de confianza** *ej. páginas web y tiendas de apps oficiales*.
- Piensa antes de hacer **clic en email, mensajes y pop-ups**.
- Mantén sistemas operativos, software, programas y apps siempre **actualizados**.

¿Qué hacer si te ves afectado por un RAT?

1. Comprueba si hay programas instalados recientemente y **si hay algo que no reconoces, elimínalo.**
2. **Haz un análisis de seguridad completo** en todos los dispositivos y en la red, no solo de los afectados.
3. Como medida adicional, considera **restablecer la configuración original del fabricante**, y restaurar la información desde una copia de seguridad limpia o plantea si necesitas verificar con un proveedor de servicios de informática que el dispositivo es seguro de usar.
4. **Cambia las contraseñas** de tus cuentas y perfiles, incluida la banca online.
5. **Controla tus cuentas bancarias y movimientos de tarjetas.** Para ayudarte recuerda que puedes configurar alertas.

Detectá comunicaciones maliciosas

Santander

Conocé más en **santander.com.uy**