Está circulando un nuevo malware llamado SORVEPOTEL o también conocido como “Water Saci” que se propaga a través de WhatsApp Web y herramientas de Desktop como Selenium y ChromeDriver.

¿Cuál es su objetivo?

Robar credenciales bancarias y de criptomonedas, controlar tu navegador y reenviar el archivo infectado a todos tus contactos de WhatsApp, sin que lo notes.

¿Cómo funciona?

1. Te llega un archivo comprimido (.ZIP) que contiene un acceso directo (.LNK) disfrazado de documento (podría ser un “presupuesto” también.)
2. Si lo abrís, se ejecutan comandos ocultos en PowerShell que descargan otro archivo (.BAT) y lo colocan en la carpeta de inicio para que el malware se mantenga activo.
3. Ese archivo instala un troyano que roba tus credenciales mediante técnicas como superposición de ventanas y captura de pantalla.

Para protegerte, te aconsejamos:

- No abras ni ejecutes archivos ZIP o accesos directos que te llegue por WhatsApp, no importa de quién provenga.
- Desactivá la descarga automática de archivos en WhatsApp Web y otras herramientas Desktop.

Y si sospechas que tu equipo está afectado:

- Ejecutá un análisis de antivirus actualizado.
- Cambiá las contraseñas de todas tus cuentas bancarias o de criptomonedas.
- Mantenete alerta frente a cualquier movimiento que pueda haber en tus cuentas.

Si crees que tu seguridad digital pudo haber sido vulnerada, te sugerimos contactarnos de inmediato por nuestros canales oficiales:

ciberseguridad@ba-csirt.gob.ar
WhatsApp: chateá con Boti al 11-5050-0147