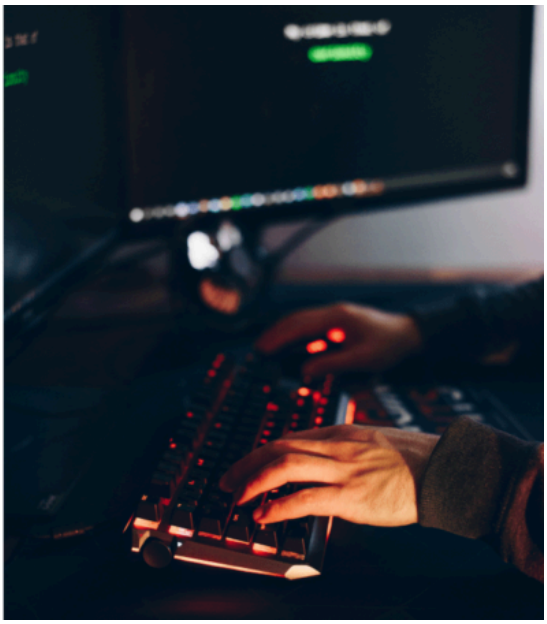
MÉXICO

# Conoce a Red WinterDog, un hacker que se hace pasar por el SAT y se roba tu información bancaria

El Ciudadano · 31 de julio de 2023

Un cibercriminal identificado como Red WinterDog está detrás de alrededor de 10 mil ataques a contribuyentes del Servicio de Administración Tributaria (SAT) en México.

Especialistas de TELMEX-Scitum, empresa mexicana de ciberseguridad, detectaron dos malwares, a través de los cuales, el hacker roba la información de los mexicanos.

Las dos campañas de troyanos que operan con extensiones maliciosas en el país se denominan como “BlackDog” y “Black Belen“. Ambas, se distribuyen a partir de correos electrónicos, mensajes de texto y páginas apócrifas.

“Red WinterDog” es el nombre que SCILabs de TELMEX-Scitum le asignó al cibercriminal que opera aproximadamente desde junio de 2022. Según la compañía mexicana, su objetivo es robar información de los contribuyentes del SAT como del Registro Nacional de Población (Renapo).

“Su objetivo es robar información bancaria y personal de las víctimas, así como cuentas de correo electrónico empresariales de usuarios en México”**.SCILabs de TELMEX-Scitum**

# ALERTA
## DE SEGURIDAD

# RED Winterdog

**Malware en navegadores de internet**

**Red WinterDog** es el nombre que **SCILabs** de **SCITUM-Telmex** asignó al cibercriminal detrás de las campañas **BlackDog** y **BlackBelen**, el cual opera desde mediados del 2022

Su objetivo es robar información bancaria y personal de las víctimas, así como cuentas de correo electrónico empresariales de usuarios en México

**BlackBelen** se distribuye po medio de campañas de phishing utilizando pretextos relacionados al SAT, RENAP Google Drive. Utiliza **malvertising** (publicidad maliciosa) en buscadores co Bing y DuckDuck Go, tambié hace uso de las tiendas oficiales de Microsoft Edge y Google Chrome

**BlackDog** se distribuye por medio de correos electrónicos de phishing con pretextos relacionados a supuestas transferencias bancarias y, complementos del SAT y la CURP

El atacante hace uso de extensiones maliciosas diseñadas principalmente para los navegadores Google Chrome y Microsoft Edge


Con base en la telemetría de **SCILabs** de **SCITUM-Telmex**, el malware distribuido por **Red WinterDog** cuenta con más de 10,000 equipos infectados en México

## Métodos de infección

La victima ingresa a un sitio apócrifo a través del buscador o recibe un correo relacionado al SAT, la CURP o Google Drive

Instala una extensión maliciosa por medio de las tiendas de aplicaciones o ejecuta un archivo de JavaScript obtenido por medio de correos electrónicos de phishing

La extensión o el archivo de JavaScript se instala en el navegador y roba información del usuario

## RECOMENDACIONES

- **Evitar abrir correos electrónicos sospechosos**
- **Evitar descargar archivos de fuentes no legitimas**
- **Antes de instalar extensiones en tu navegador, consúltalo con el área correspondiente**


SCILabs identificó, en junio de 2022, al cibercriminal Red WinterDog a partir del análisis de correos electrónicos, URLs y direcciones IP infectadas en Latinoamérica. Seis meses después, los especialistas encontraron otro malware llamado Black Belen, diseñado por el mismo hacker.

---

**Fuente:** El Ciudadano