Alerta de seguridad cibernética	8FPH23-00875-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de agosto de 2023
Última revisión	14 de agosto de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente:

"Por medio del presente,expresar nuestro saludo y tambien queremos informarte acerca de la cuenta que mantienes con nosotros.Hemos identificado que su cuenta no ha sido actualizada y verificada durante mucho tiempo,esto va en contra de nuestras politicas de seguridad."

De abrir el enlace, la persona es dirigida a un sitio falso semejante a los de Banco Santander, donde se expone al robo de su usuario y contraseña (credenciales).

Indicadores de compromiso

Antes de evaluar la aplicación de acciones, tenga presente las advertencias de gestión de los IoC. Los IoC de este informe pueden ser obtenidos directamente desde nuestro repositorio.

URL del sitio falso
http://banco-santander-cl.ctisupplies[.]co.ke/1692019109/portada/personas/home.asp

URL de redirección
http://wordpress.zuliatec[.]com.ve/bancosantander/cuenta-dhqq/

IP del sitio falso
209.205.218.2

Asuntos del correo electrónico
Fwd_🔒!Falta 1 dias!🕵,su cuenta necesita actualizacion de datos Seguridad👆💳Urgente.

Correos de salida
forinc@server2.fishbonesecurity.com

IP	Comentario
208.76.80.220	SMTP

Imágenes Relacionadas

Imagen 1: Correo electrónico

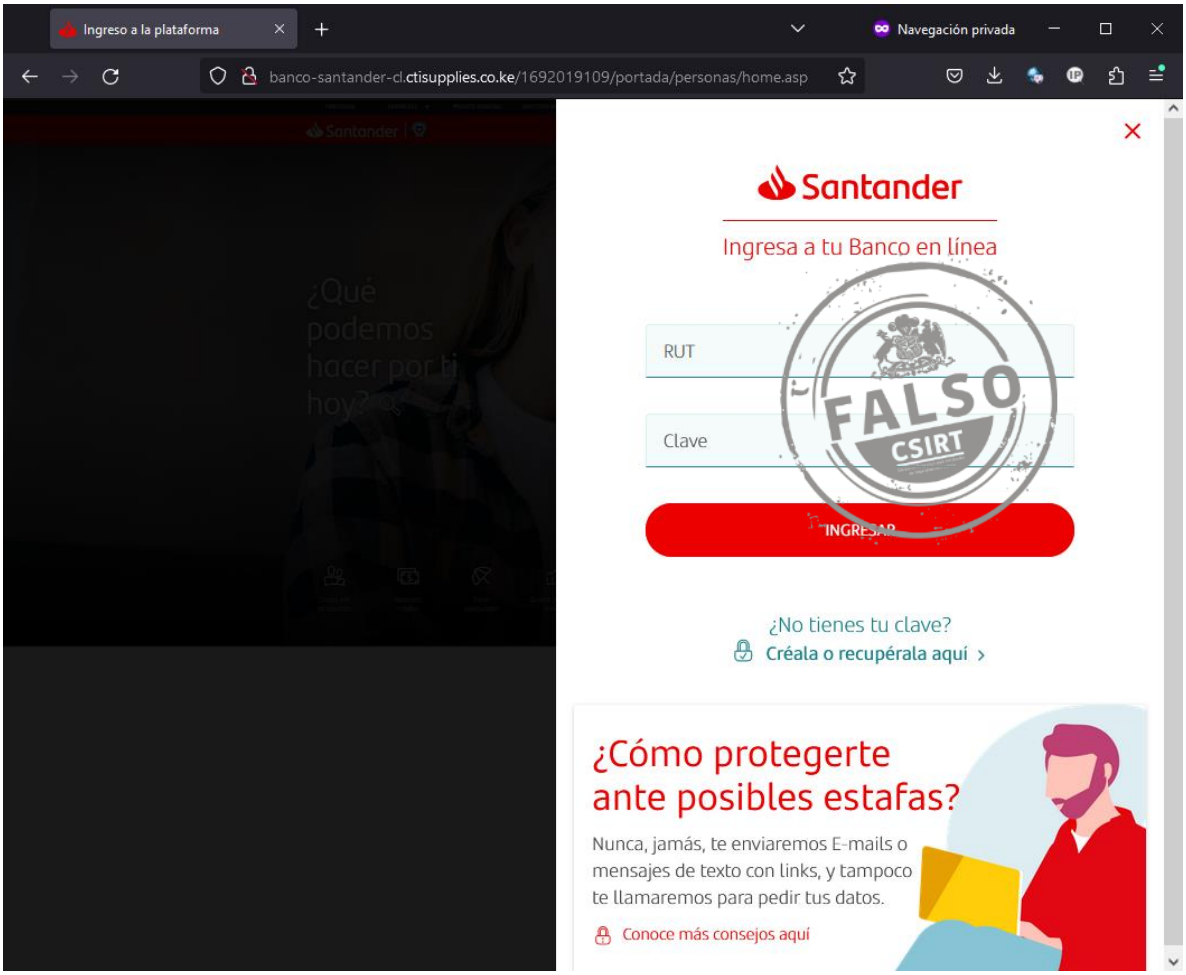

Imagen 2: Sitio fraudulento

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.14 11:04:44 -04'00'