Alerta de seguridad informática	8FPH23-00867-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de agosto de 2023
Última revisión	03 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 del Banco Santander, donde se expone al robo de su usuario y contraseña (credenciales).

IoC Correo Electrónico

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. De forma preventiva, sugerimos aplicar las siguientes recomendaciones de ciberseguridad.

URL redirección:

https://bit[.]ly/3OE47RK?l=www.santander.cl
https://www.nationaltreasures.co[.]nz/bancosantander/cuenta-daiu/

URL sitio falso:

https://banco.santander-cl.infenso[.]hr/1691069564/portada/personas/home.asp

Dirección IP del sitio falso:

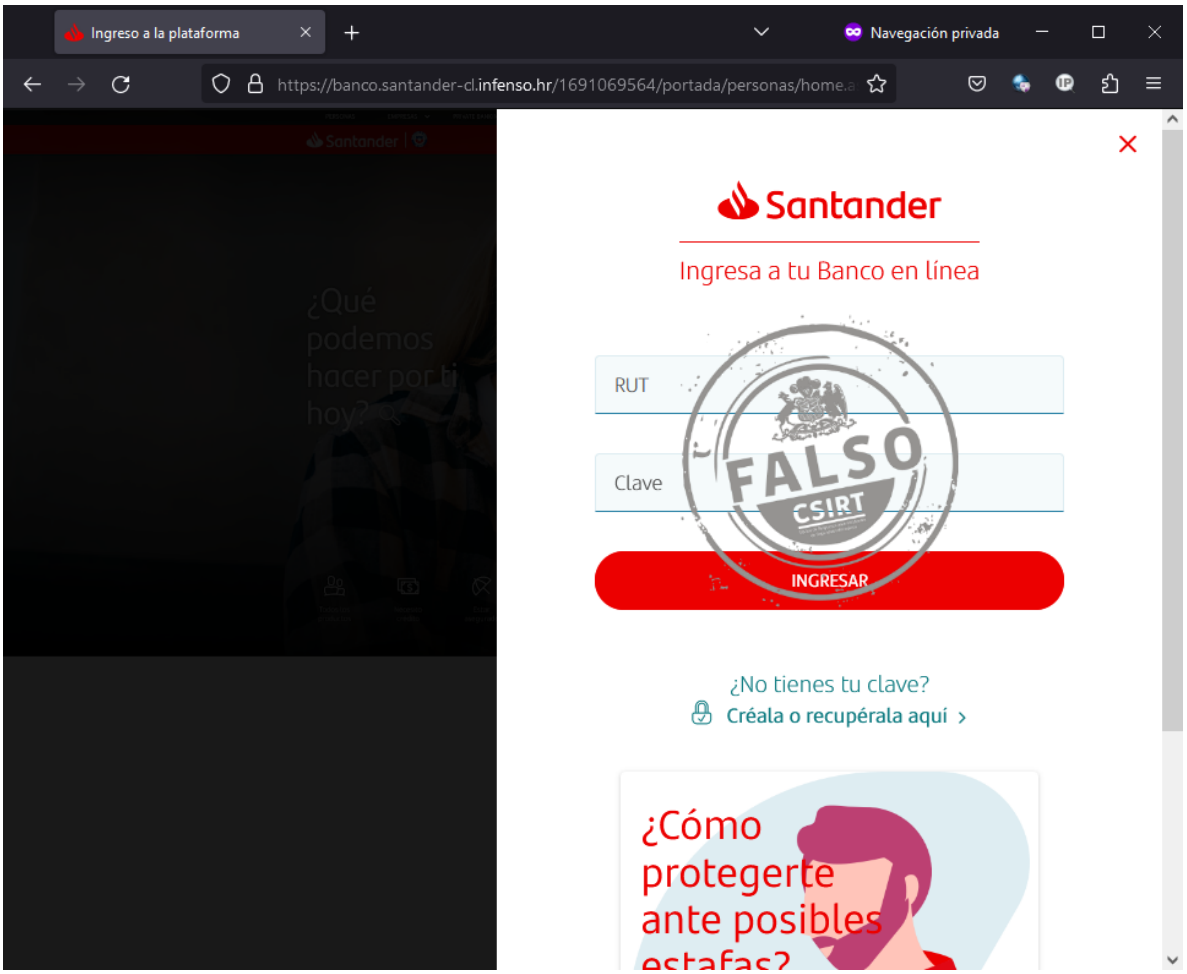
[185.58.73.179]

Datos del remitente:

Asunto	Correo de Salida	SMTP Host
Fwd_ 🔓 !AVISO IMPORTANTE!,su cuenta necesita actualizacion de datos Seguridad 👍 💳	ebuys6154@host.talkitter.com	[216.158.228.91]

Imagen del mensaje

Imagen del sitio



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.03 11:08:54 -04'00'