Alerta de seguridad informática	8FPH22-00607-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 de septiembre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

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: *"Le informamos que se ha detectado un intento de ingreso desde un dispositivo desconocido a su banca, por lo que hemos restringido el acceso a su banca temporalmente."*

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

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromiso

URL redirección:

https://lati[.]link/dc1m?=app
https://ajgeotech[.]cl/index/?app=app

URL sitio falso:

https://harahoritelecomllp[.]com/1664541464/portada/personas/home.asp

Asunto	Correo de Salida	SMTP Host
Santander - Alerta de Dispositivo.	louiswong@skyfortune.com	[173.249.151.122]

Otros antecedentes

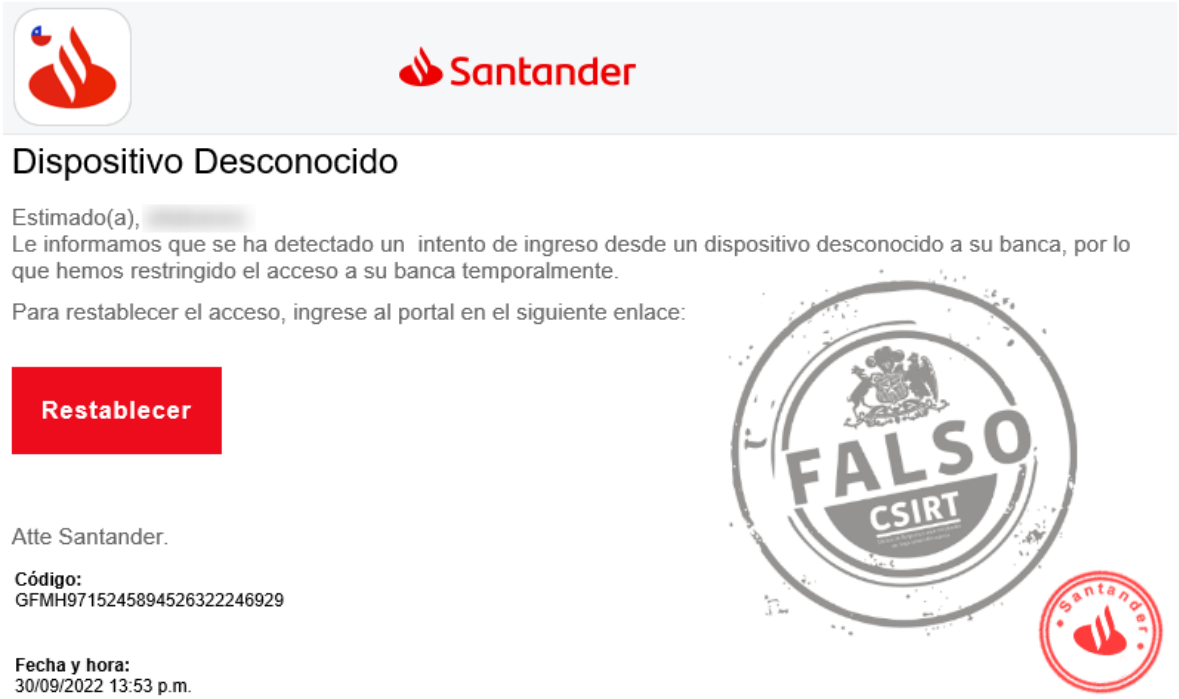
Certificado Digital

Fecha Valido	30 Aug 2022
Fecha Término	28 Nov 2022
Emitido	Let's Encrypt R3

Datos Alojamiento y Dominio

IP	[184.168.96.149]
Número de sistema autónomo (AS) IP	26496
Emitido Etiqueta del sistema autónomo IP	AS-26496-GO-DADDY-COM-LLC
Registrador IP	APNIC
País IP	SG
Dominio	harahoritelecomllp.com
Registrador Dominio	https://namecheap.com

Imagen del mensaje



Santander

Dispositivo Desconocido

Estimado(a),
Le informamos que se ha detectado un intento de ingreso desde un dispositivo desconocido a su banca, por lo que hemos restringido el acceso a su banca temporalmente.

Para restablecer el acceso, ingrese al portal en el siguiente enlace:

Restablecer

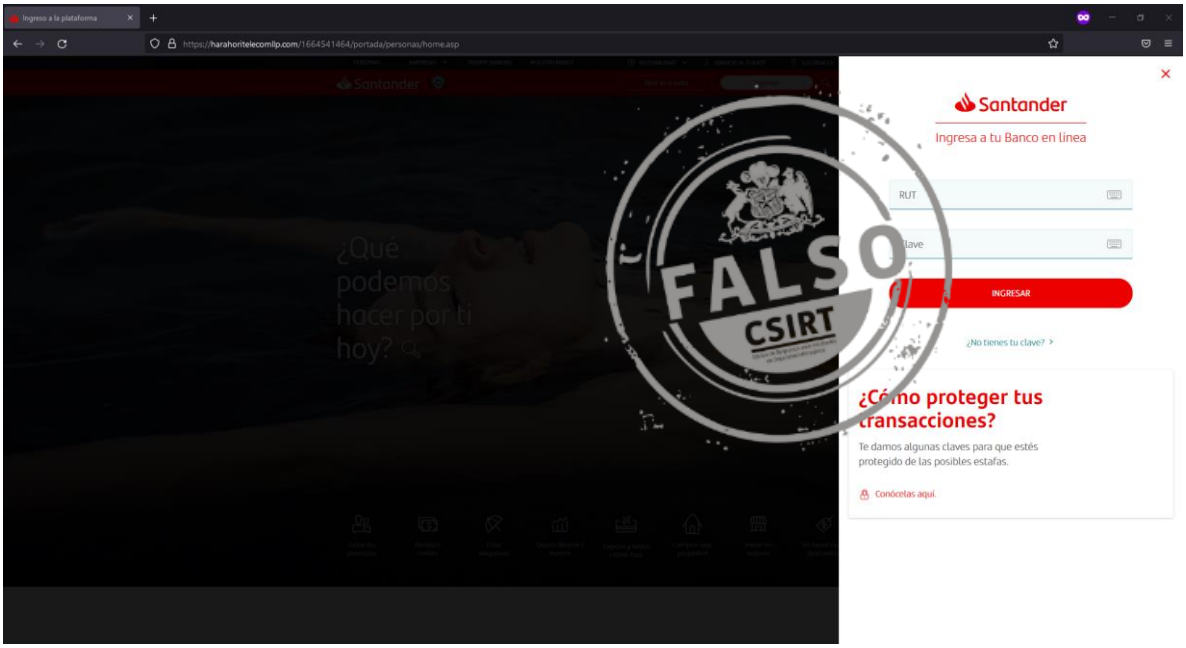
Atte Santander.

Código:
GFMH971524589452632224692 9

Fecha y hora:
30/09/2022 13:53 p.m.

Infórmese sobre la garantía estatal de los depósitos en su banco o en www.cmfchile.cl
2022 Santander. Todos los Derechos Reservados.

Imagen del sitio



Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.03 15:49:02 -03'00'