Alerta de seguridad cibernética	8FPH20-00270-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Julio de 2020
Última revisión	17 de Julio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. 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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del Banco Santander.

El atacante intenta persuadir a la víctima para utilizar un enlace en el cuerpo del correo

El mensaje del correo indica la cuenta fue bloqueada y se debe ingresar al sitio para volver a activarla.

Al seleccionar el botón para ingresar al Banco Santander, la persona es dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirecciones:
hxxp://bit[.]ly/30n7hPw?l=www.santander[.]cl
Urls sitio falso:
hxxp://www[.]invatamimpreuna[.]ro/www[.]santander[.]cl/pagina/login[.]asp

Sender
tk13467[@]dichthuatdongduong[.]com

Smtp Host
[103.74.122.232]

Asunto
Fwd:Cuenta - Bloqueada.

Otros antecedentes

URL Body SHA-256

12d3d59ab3a5801b44935de5a1966febcd53ee084cff4cb981f8408782667645

Datos Alojamiento

IP	:	188.215.250.94
Número de sistema autónomo (AS)	:	AS 5588
Etiqueta del sistema autónomo	:	T-Mobile Czech Republic a.s.
País	:	Rumanía
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	invatamimpreuna[.]ro
Creado	:	2017-08-03
Expira	:	2022-08-02
Información del registrador	:	Rospot SRL
Servidores de nombres	:	ns1.webdesignagency.ro ns2.webdesignagency.ro

Imagen del mensaje

De: Santander☐ <noreply@publimailer.com>
Para:
CC:
Asunto: Fwd:Cuenta - Bloqueada.

Santander

Estimado(a) :

Santander,comunica a nuestros clientes que como responsabilidad de informar sobre las nuevas medidas de seguridad de nuestro banco.

Le informamos que realizamos los **monitoreos de las actividad de nuestras cuentas,**segun la nueva ley Nï¿½ 20.009,nos hemos puesto en contacto con usted para informarle que su cuenta ha sido **bloqueada,**para verificar la actividad de su cuenta y evitar el proceso de baja acceda a nuestro portal.

Activa tu cuenta . Aqui

Si tienes consultas o deseas mas informacion:

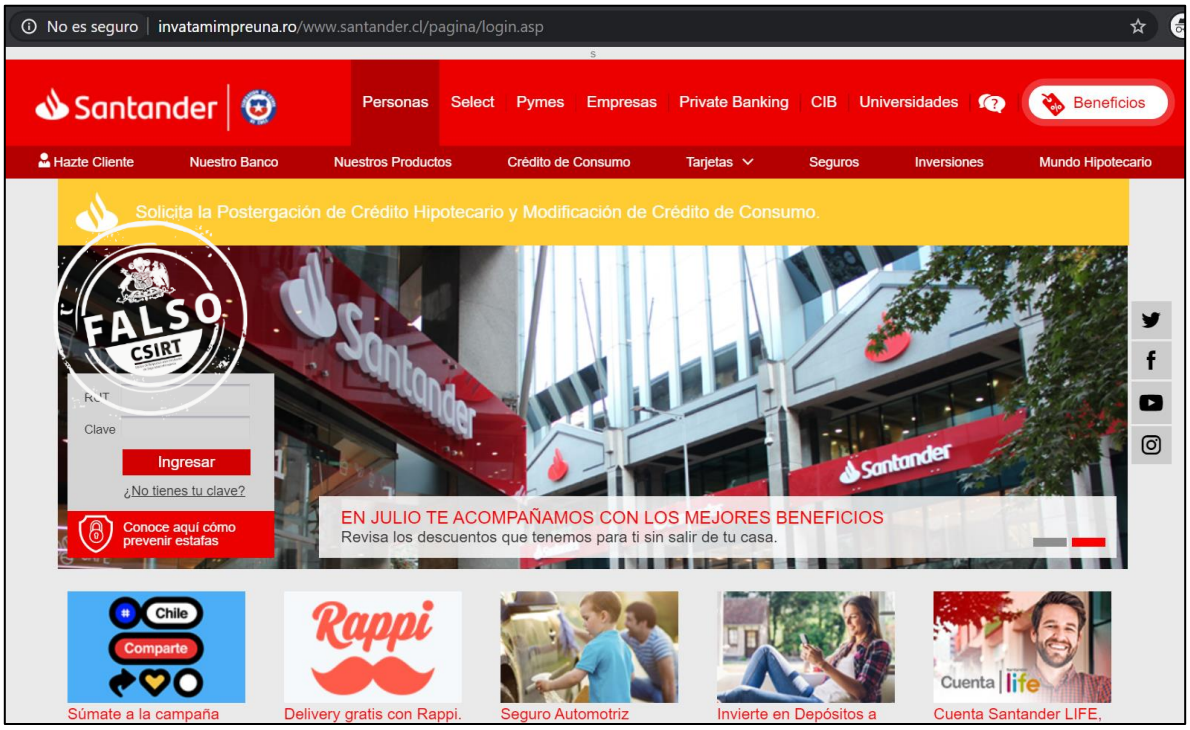
ingresa aquï¿½

https://www.santander.cl/seguros/fraude

Atentamente, Santander

Si no deseas continuar recibiendo correos de BancoEstado, por favor haz **click aqui**

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