Alerta de seguridad informática	8FPH21-00376-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Febrero de 2021
Última revisión	19 de Febrero de 2021

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 correo electrónico, que supuestamente proviene del Banco Santander.

El atacante busca persuadir a las personas para utilizar un enlace adjunto.

El mensaje del correo indica que su SuperClave fue bloqueada y para activarla debe seleccionar el enlace adjunto. Al hacerlo, es dirigido a un sitio falso, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls sitio falso:
https://samtanderpersona-cl.beingbamboo[.]com/b04cb2898fcbb657c1c3c2b6af207eeb/index.asp

Asunto
Activa tus Alertas de seguridad

Smtp Sender:
apache@98a78d673378[.]com

Smtp Host:
[92.223.65.202]

Otros antecedentes

Certificado Digital

Fecha Válida	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

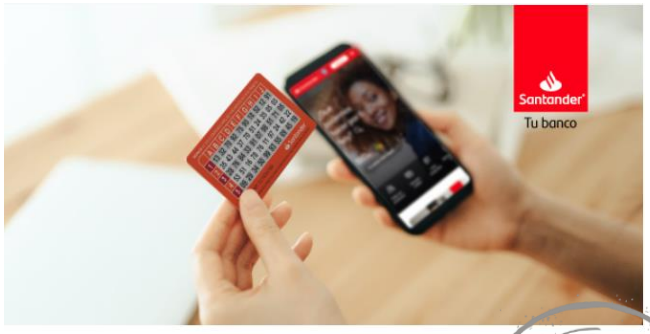
Datos Alojamiento

IP	:	68.65.123.231
Número de sistema autónomo (AS)	:	22612
Etiqueta del sistema autónomo	:	NAMECHEAP-NET
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	samtanderpersona-cl.beingbamboo[.]com
Creado	:	03-07-2020
Expira	:	03-07-2021
Información del registrador	:	GoDaddy.com, LLC
ID IANA	:	146
Correo electrónico	:	abuse@register.it
Servidores de nombres	:	dns1.namecheaphosting.com dns1.namecheaphosting.com

Imagen del mensaje



Tu SuperClave se encuentra Bloqueada,

Estima :

La SuperClave es una tarjeta de coordenadas que debes llevar contigo cada vez que quieras hacer un movimiento de fondos desde tus productos.

FALSO
CSIRT

Por motivos de seguridad tu SuperClave fue bloqueada. Para activar sus operaciones de manera segura, debe reactivarlo siguiendo estos pasos:

Restablecer

Has recibido este correo porque figura como el E-mail de tu cuenta Scotiabank. Para modificarlo contactate con tu ejecutiva o visita una de nuestras sucursales.

- El sistema te pedira una combinacion de solo 3 coordenadas que podras obtener de tu SuperClave y con ella estaras autorizando la transaccion.
- La combinacion de numeros se te solicitara de forma aleatoria cada vez que realices una transaccion.
- Tu numero secreto jamas se repite.

2020. S.A.C.I Santander Chile,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: 2021.02.19 15:06:28 -03'00'