Alerta de seguridad informática	8FPH21-00360-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2021
Última revisión	25 de enero 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 smishing que supuestamente proviene del Banco Santander.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del mensaje.

El mensaje indica que por motivos de seguridad se ha bloqueado su tarjeta.

Al seleccionar el enlace para realizar la activación, 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 Redirección:
https[:]//santader-sms[.]app/?sms=santander

Urls sitio falso:
https[:]//bancosantan-der[.]live/1611601036/personas/index.asp

Mensaje
Santander: Por seguridad bloqueamos tu Tarjeta de Crédito. Verificar tu cuenta para activar acceso: https[:]//santader-sms[.]app/?sms=Santander.

Otros antecedentes

Certificado Digital

Fecha Válida	:	24-01-2021
Fecha Término	:	25-01-2022
Emitido	:	Sectigo RSA Domain Validation Secure Server CA

Datos Alojamiento

IP	:	198.54.115.246
Número de sistema autónomo (AS)	:	22612
Etiqueta del sistema autónomo	:	Namecheap, Inc.
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	bancosantan-der[.]live
Creado	:	25-01-2021
Expira	:	25-01-2022
Información del registrador	:	WhoisGuard, Inc.
ID IANA	:	1068
Correo electrónico	:	abuse@namecheap.com
Servidores de nombres	:	dns1.namecheaphosting.com dns2.namecheaphosting.com

Imagen del mensaje

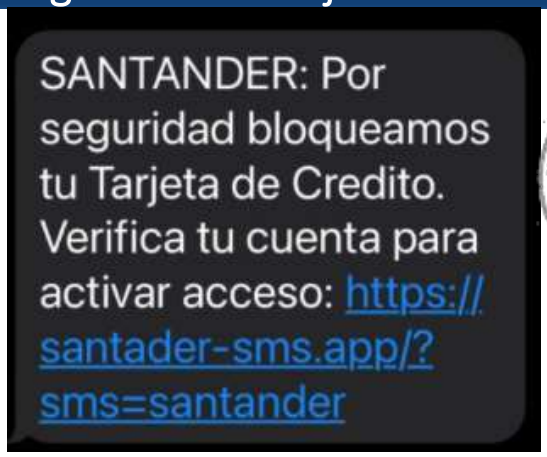
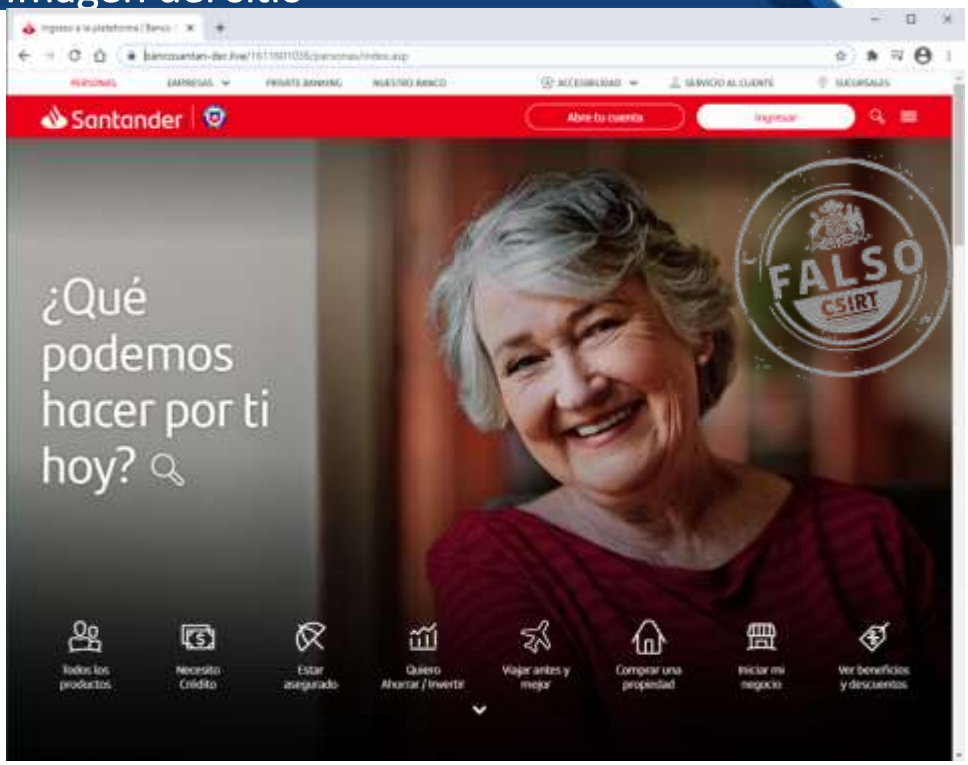


Imagen del sitio



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: 2021.01.25 16:46:24 -03'00'