Alerta de seguridad informática	8FPH20-00327-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre 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 busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica que el estado de la SuperClave del cliente requiere una reactivación para lo cual sumistra un enlace.

Al seleccionar el enlace para activar la clave, el usuario 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[:]//santander.personascl[.]site/1605527542/index.asp

Smtp Host
[69.167.167.190]

Sender:
heroisticbcg@host.heroisticbcg[.]com

Asunto
Estado de tu SuperClave requiere Activacion

Otros antecedentes

URL Body SHA-256

dd6a55eeceaf20ef631862bec76f8ca6f3ce42a81a6517ab7072c9c1d5ac9f53

Certificado Digital

Fecha Valido	:	18/10/2020
Fecha Término	:	16/01/2021
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	34.82.143.57
úmero de sistema autónomo (AS)	:	15169
Etiqueta del sistema autónomo	:	Google LLC
País	:	EU
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	personascl[.]site
Creado	:	18-10-2020
Expira	:	18-10-2021
Información del registrador	:	Name.com LLC
ID IANA	:	625
Correo electrónico	:	sure.baboyan.asedl.am
Servidores de nombres	:	ns1hwy.name.com ns2cvx.name.com ns3jwx.name.com ns4lny.name.com

Imagen del mensaje

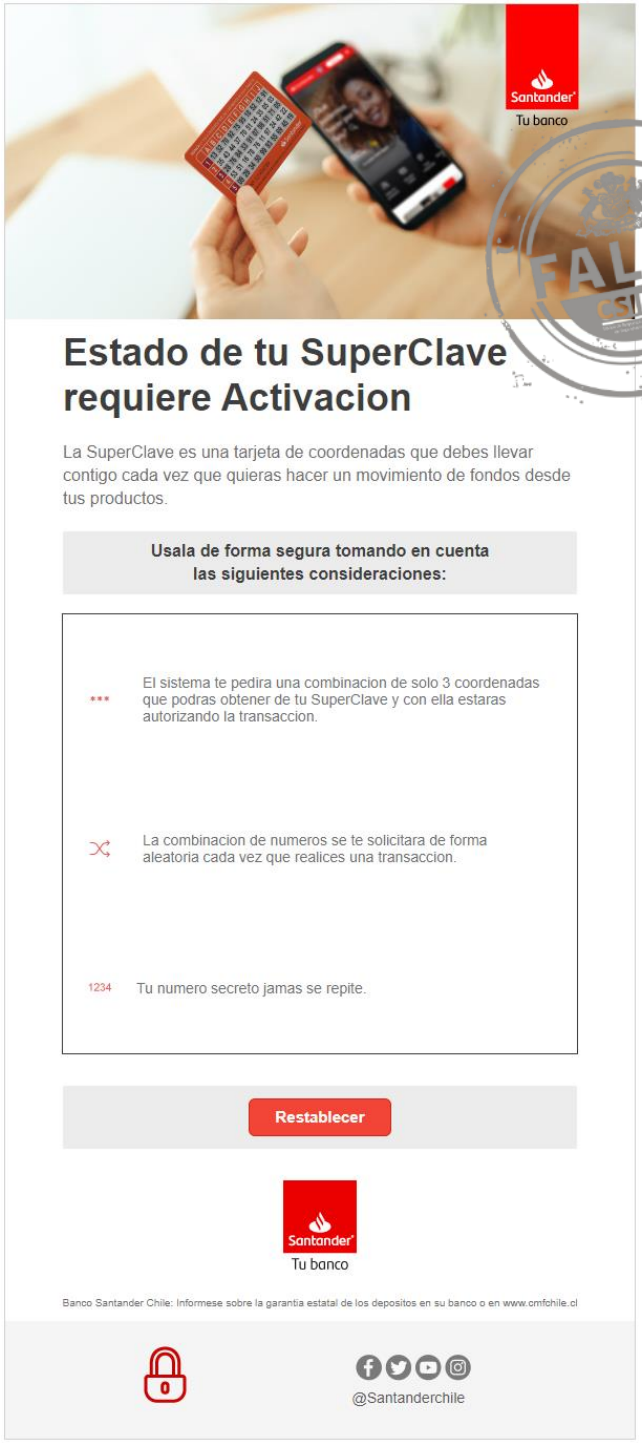
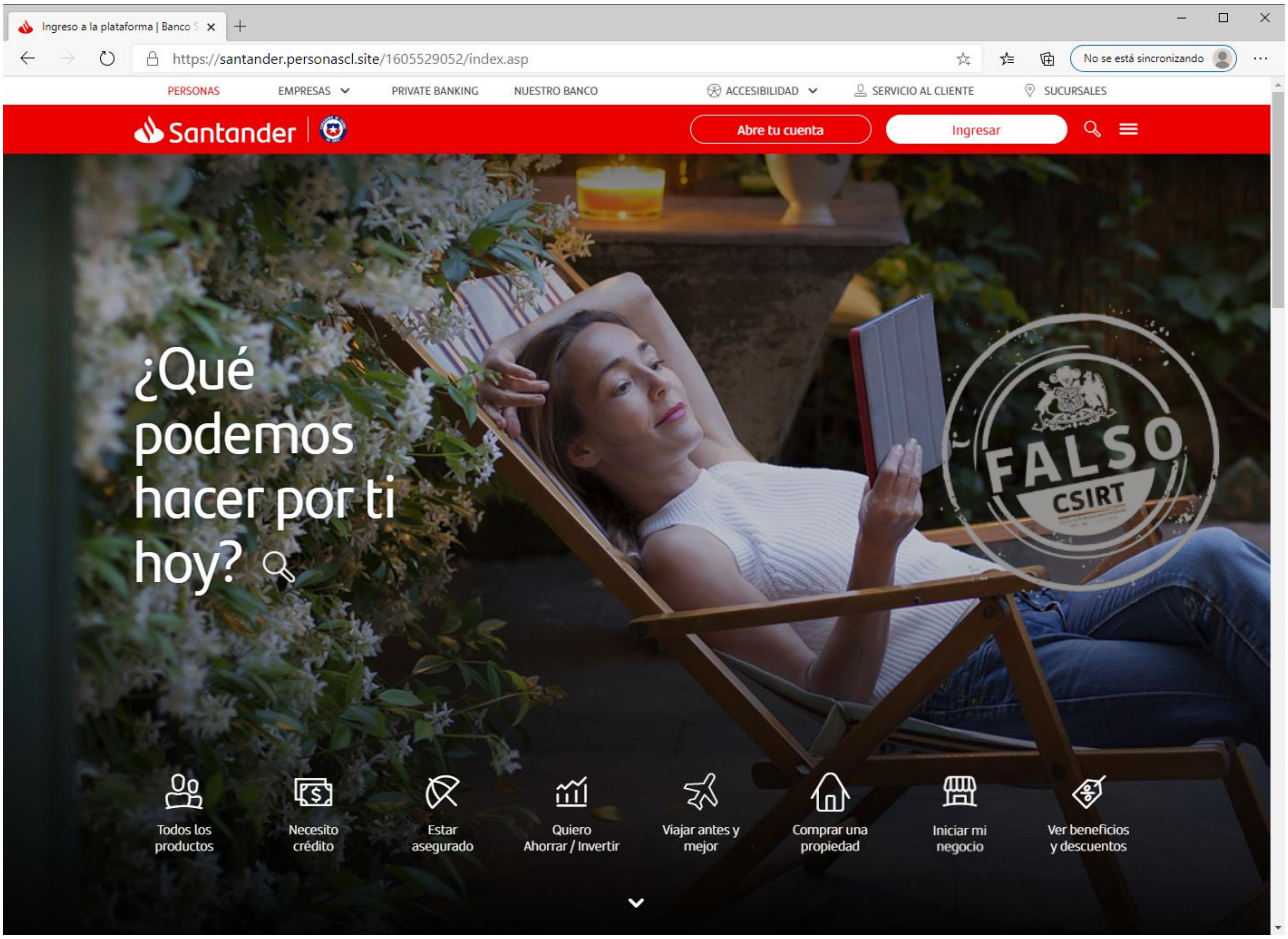


Imagen del sitio



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: 2020.11.16 10:30:28 -03'00'