Alerta de seguridad cibernética	8FPH20-00315-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Octubre de 2020
Última revisión	15 de Octubre 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 Smishing que se está difundiendo a través de mensajes de texto vía celular que supuestamente proviene del Banco Santander.

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

El mensaje del correo indica que por motivos de seguridad se ha producido el bloqueo de la tarjeta de crédito y solicita verificar la cuenta a través del enlace.

Al seleccionar el enlace para ver el estado de la cuenta, la víctima es dirigida a un sitio falso, donde se expone al robo de sus credenciales.

CSIRT agradece la colaboración de Joshua Ríos, quien nos informó sobre este incidente. Para reportar un incidente, puedes completar el formulario de reporte en el sitio www.csirt.gob.cl o llamar las 24 horas al teléfono +(562) 2486 3850.

Observación

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

Indicadores de compromiso

URL redirección:
Hxxps[:]//santaander-appvil[.]ovh/?sms=santander

URL sitio falso:
hxxps[:]//santaander-appmvil[.]ovh/1602728744/personas/index[.]asp

Asunto
Santander: Por motivos de seguridad hemos bloqueado tu Tarjeta de Crédito. Verificar tu cuenta para activar el acceso

Otros antecedentes

Body SHA-256

0b46016421693a6c940dc8b3470e0ec38374196ff388e4735673a7e107fb6ba4

Certificado Digital

Fecha Válido	2020-03-26
Fecha Término	2021-03-26
Emitido	Sectigo RSA Domain Validation Secure Server CA

Datos Alojamiento

IP	51[.]161[.]122[.]78
Número de Sistema Autónomo (AS)	16276
Etiqueta del Sistema Autónomo	OVH SAS
País	CA
Registrador	ARIN

Datos del Dominio

Nombre de Dominio	SantaAnder-AppMvll[.]ovh
Estado del Dominio	addPeriod, clientDeleteProhibited, clientTransferProhibited
Creado	2020-10-10
Expira	2021-10-10
Información del Registrador	OVH
ID IANA	433
Correo Electrónico	abuse@ovh[.]net
Name Server	DNS10.OVH.CA NS10.OVH.CA

Imagen del mensaje

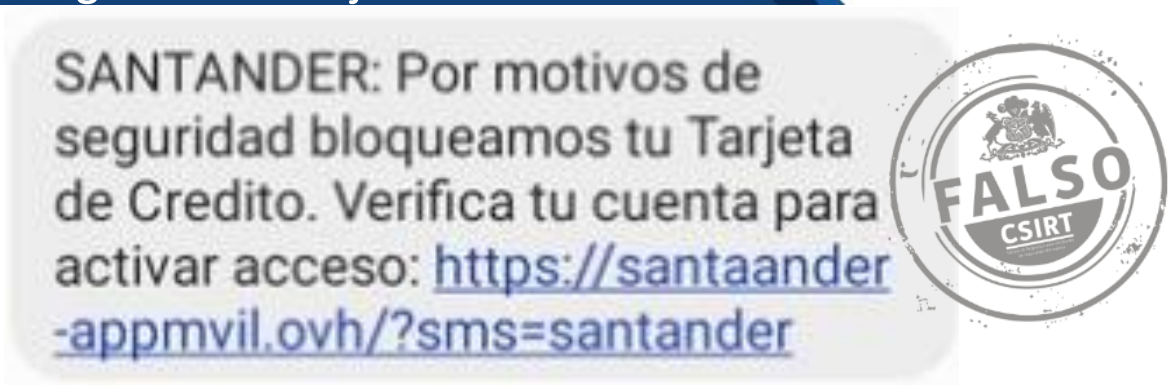
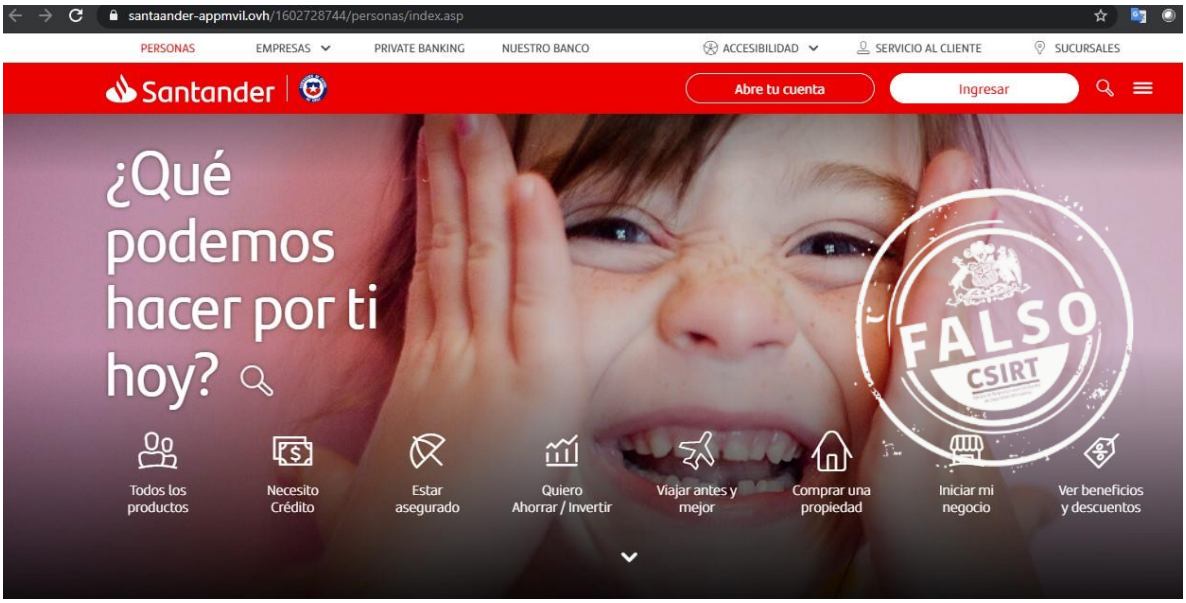


Imagen del sitio



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.