Alerta de seguridad informática	8FPH21-00421-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de julio de 2021
Última revisión	28 de julio 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 de Gobierno), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene de Cencosud Scotiabank.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.
El mensaje del correo argumenta falsamente que “por la seguridad del cliente se vieron en la obligación de bloquear la tarjeta de crédito”, por lo que en un plazo de 24 horas después de haber recibido el mensaje puede acceder a activar su tarjeta Cencosud Scotiabank. Allí, las personas son dirigidas a un sitio falso, donde se exponen al robo de credenciales.

Observación

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

Indicadores de compromiso

URL de redirección:
https://bit[.]ly/3zbcUjL?l=www.tarjetacencosud.cl

URL sitio falso:
http://www.tarjetacencosud.cl.intra[.]az/

Asunto:
Fwd:Tarjeta Cencosud Scotiabank Bloqueada.

SMTP Sender:
cprapid[.]com

SMTP Host
[185.13.231.14]

Otros antecedentes

Certificado Digital

Fecha Valido	:	18-07-2021
Fecha Término	:	16-10-2021
Emitido	:	R3

Datos Alojamiento

IP	:	[185.22.155.185]
Número de sistema autónomo (AS)	:	51659
Etiqueta del sistema autónomo	:	LLC Baxet
País	:	RU
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	intra[.]az
Creado	:	NO APLICA
Expira	:	NO APLICA
Información del registrador	:	Intra MMC
ID IANA	:	NO APLICA
Correo electrónico	:	NO APLICA
Servidores de nombres	:	ns5.sayt.az ns6.sayt.az

Imagen del mensaje

martes 27-07-2021 11:41

Cencosud Scotiabank <estado_cuenta@tarjetacencosud.cl>

Fwd:Tarjeta Cencosud Scotiabank Bloqueada.

Para .cl

FALSO CSIRT

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Publica. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre Ã©ste). Ante sospechas o dudas, reporte a la mesa de ayuda.

cencosud Scotiabank

TE QUIERO VER FELIZ

Estimado(a): .cl

Cencosud Scotiabank,queremos informarle que en el marco de los ultimos pasos del proceso de integraciÃ³n de Banca en Linea.

Se encontro algunos errores en su cuenta al momento de unificar nuestros sistemas internos y canales digitales,que por su seguridad nos vemos en la obligacion de Bloquear su Tarjeta de Credito por un plazo de 24 horas despues de haber recibido este mensaje.

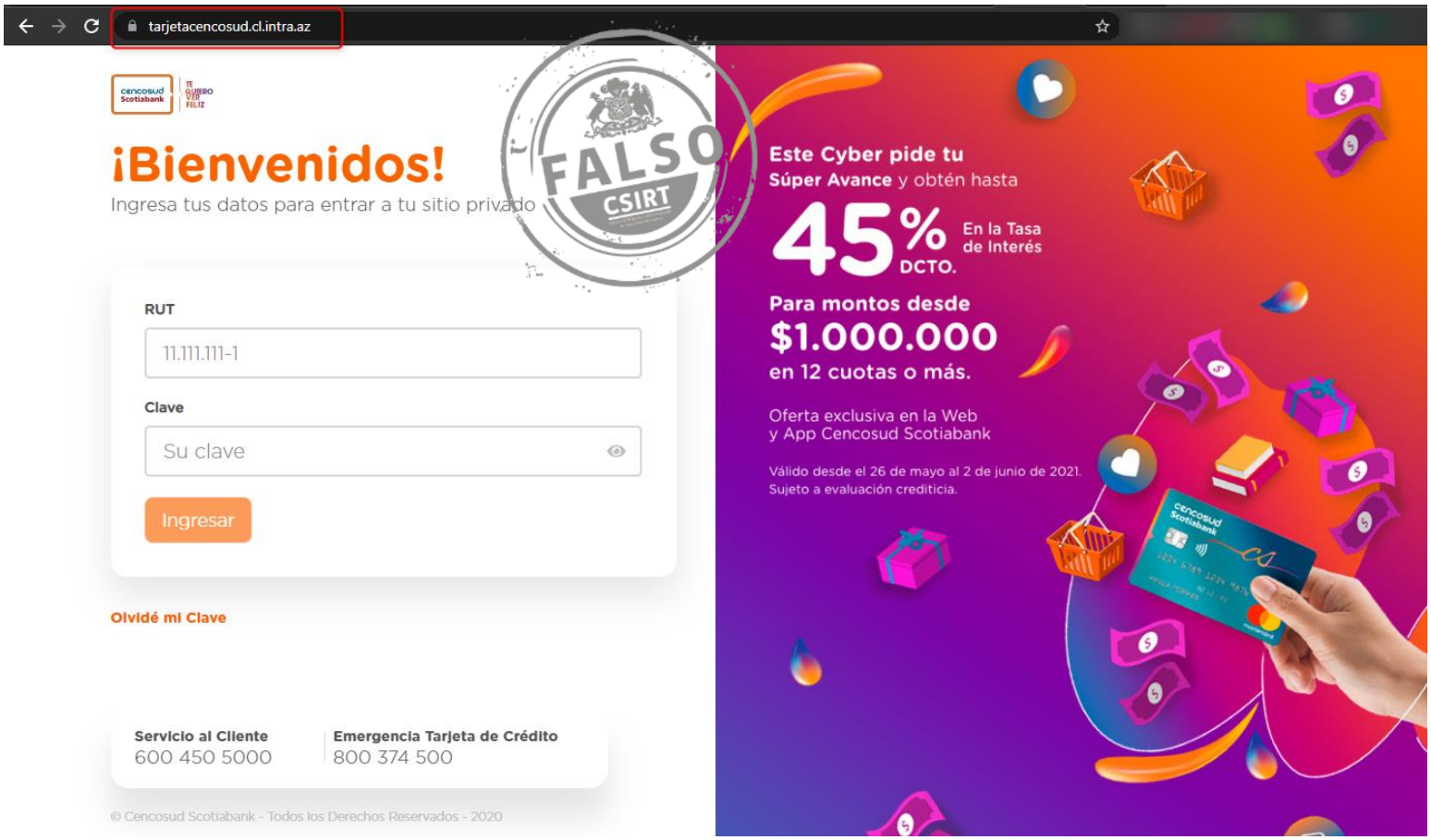
Activar suTarjeta Cencosud Scotiabank: aqui

www.tarjetacencosud.cl

Emergencias de Tarjeta de Credito

800 374 500

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: 2021.07.29 14:03:37 -04'00'