Alerta de seguridad cibernética	8FPH20-00151-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril 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 falso que aparente provenir de Cencosud.

El mensaje del correo le indica a la víctima que posee un avance el cual puede simular ingresando al enlace que se encuentra en el cuerpo del correo. Si una persona selecciona el enlace será dirigido a un sitio que simula ser el de la tarjeta Cencosud, donde se expone al robo de sus credenciales asociadas a la tarjeta de crédito.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls Redirecciones:
https[:]//music[.]bunyorosqoop[.]com/tarjeta-cencosud[.]php

Urls sitio falso:
https[:]//tarjetacencosud-cl[.]gq/js/tarjeta/nuevo/www[.]tarjetacencosud[.]cl/Tarjeta/Simular-avance[.]html

Smtp Host
210[.]152[.]127[.]66
163[.]44[.]196[.]73

Sender
apache[@]chikumashobo[.]co[.]jp
pume[@]memtreat[.]com

Asunto
Super Avance.

IMAGEN DEL MENSAJE

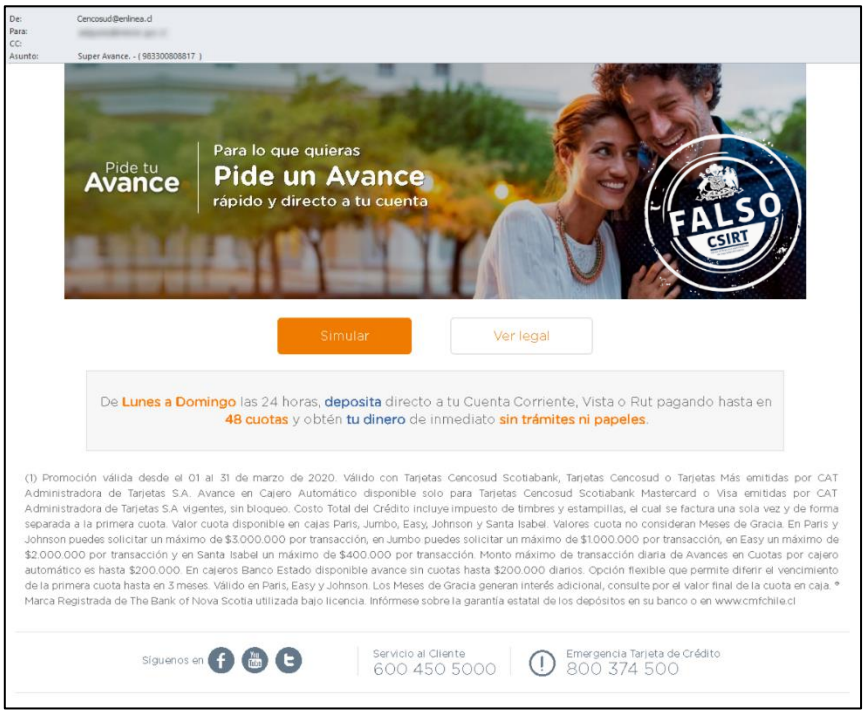
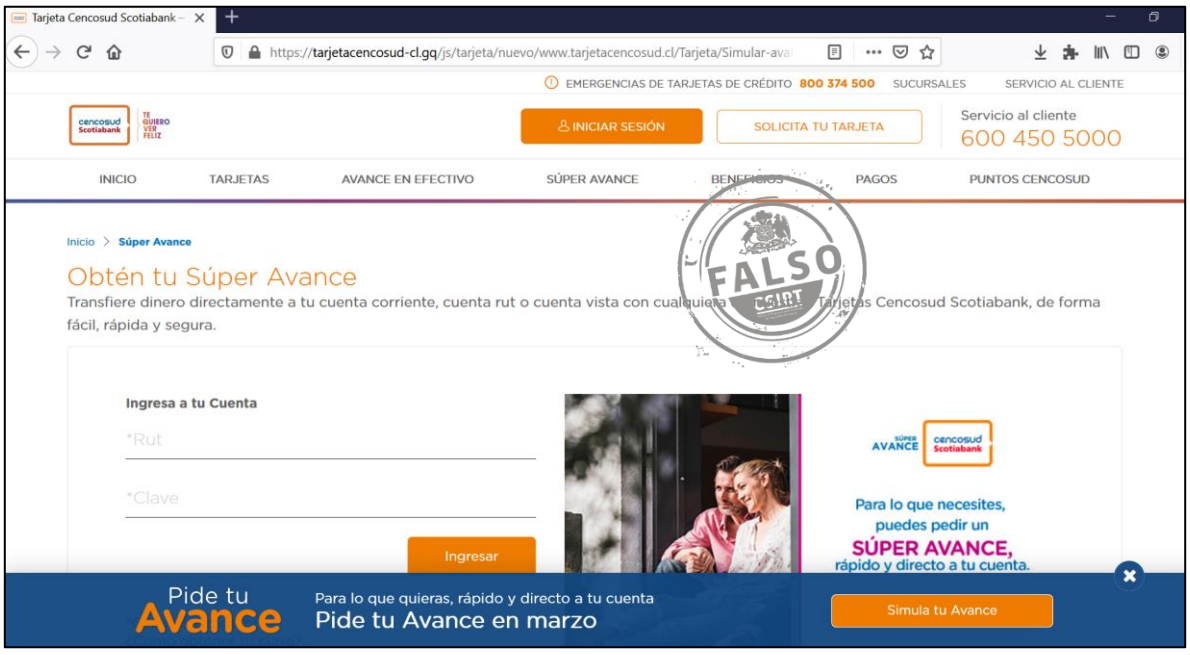
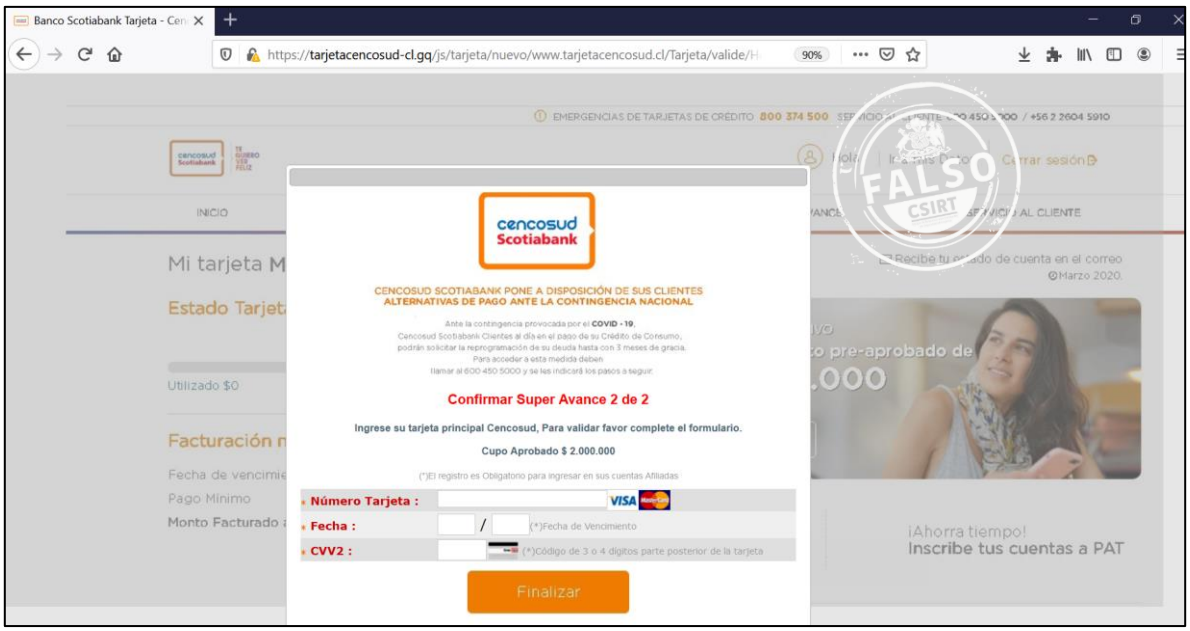


IMAGEN DEL SITIO





RECOMENDACIONES

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- 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: 2020.04.01 16:06:04 -03'00'