Alerta de seguridad cibernética	8FPH20-00165-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 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), ha detectado dominios de suplantación de Banco Chile, Banco Scotiabank y Cencosud, que intentan engañar a los clientes utilizando técnicas de phishing.

Los delincuentes intentan convencer a sus víctimas a través de correos electrónicos u otros medios, para que accedan a los sitios suplantados, con la finalidad de que los clientes entreguen sus credenciales de acceso a sus cuentas.

La Ip [144.91.76.213], que intenta suplantar a la identidad Bancaria Scotiabank utilizando el dominio “online-cl.live”, tiene la particularidad que al escribir cualquier subdominio utilizando caracteres alfa numéricos y un punto, es direccionado al sitio falso.

La IP [178.159.36.139], que intenta suplantar la identidad del Banco de Chile y Cencosud, desde el 18 de marzo del 2020, está diariamente creando dominios falsos hasta. A la fecha de esta publicación, se han registrado 182 dominios. En todos los casos se ha utilizado la palabra covid-19 en el dominio, concepto asociado a la actual pandemia.

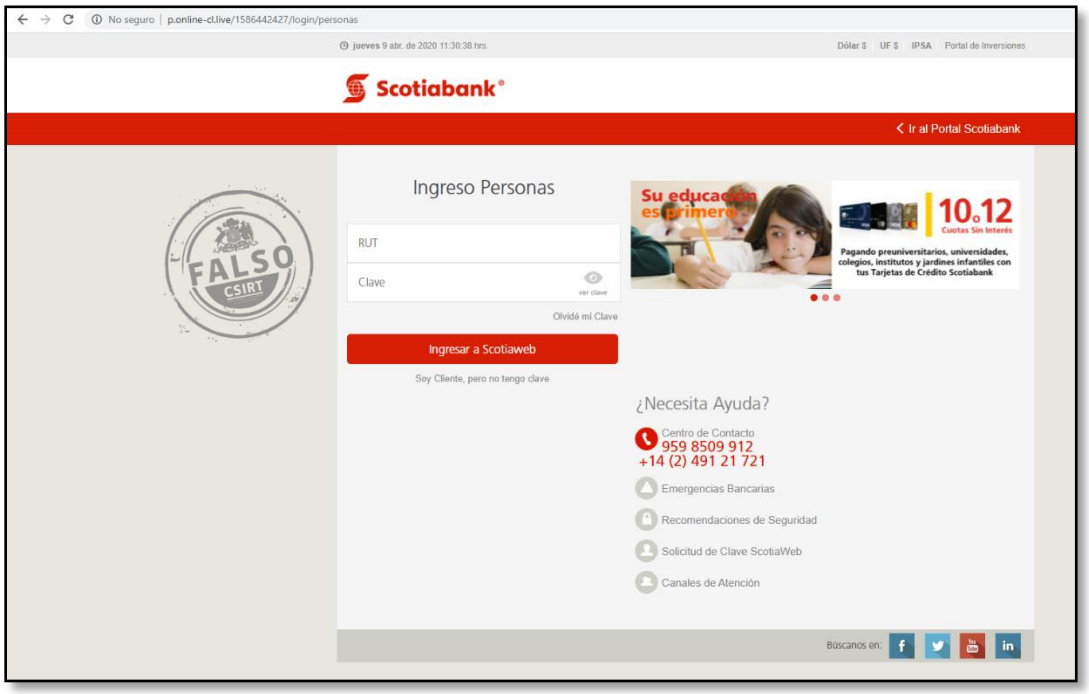
OBSERVACIÓN

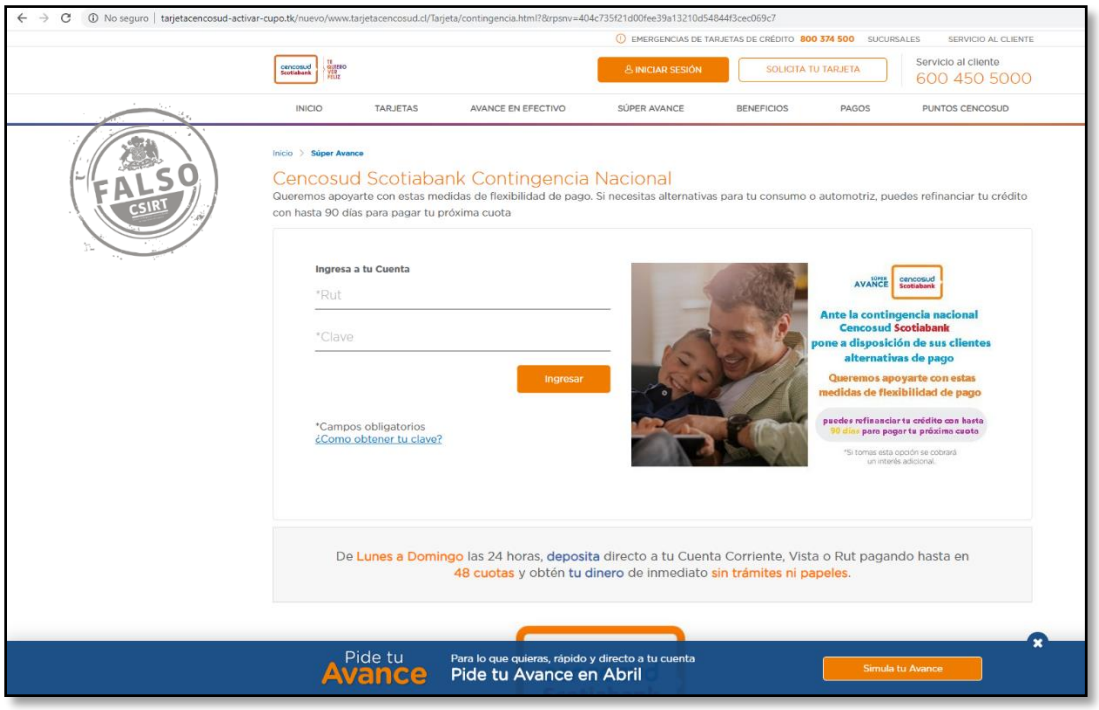
Solicitamos tener en consideración las señales de compromiso en su conjunto.

INDICADORES DE COMPROMISO

IP Servidores
[144.91.76.213]
[178.159.36.139]

IMAGEN DEL SITIO





RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen
- Prestar atención en los detalles de los mensajes o redes sociales
- Desconfiar de promociones que no se encuentren en los canales oficiales
- Siempre visitar los canales de comunicaciones oficiales
- 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: 2020.04.09 15:16:10 -04'00'