Alerta de seguridad informática	**8FPH-00059-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**09 de Septiembre de 2019**
Última revisión	**09 de Septiembre de 2019**

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 identificado una campaña de phishing a través de un correo electrónico dirigido a los usuarios del Banco de Chile. El mensaje del correo hace referencia a un eventual aumento de cupo en la línea de crédito y/o tarjeta de crédito, cuya vigencia es solo por el mes de Septiembre. A través de ingeniería social, los criminales intentan persuadir a los usuarios para ingresar al hipervínculo asociado a la oferta. Si las personas ingresan al enlace, se exponen a que el atacante robe sus credenciales desde un sitio que imita al original del Banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

https://thegoodhumanfactory.com/wp-content/plugins/contact-form-7/includes/js/aumento/LOA/index.php

https://oferta-avance-de-tarjeta.gq/www.bancoedwards.cl/Login.htm

Smtp Host

[95.183.6.207]

From:

boobadigital@il3lv8152.activetraildns.net

Subject:

Vigencia 01 al 30 de Septiembre de 2019. Otorgamiento de aumento de cupo de Línea de Crédito y/o Tarjeta de Crédito

Imagen Phishing Correo

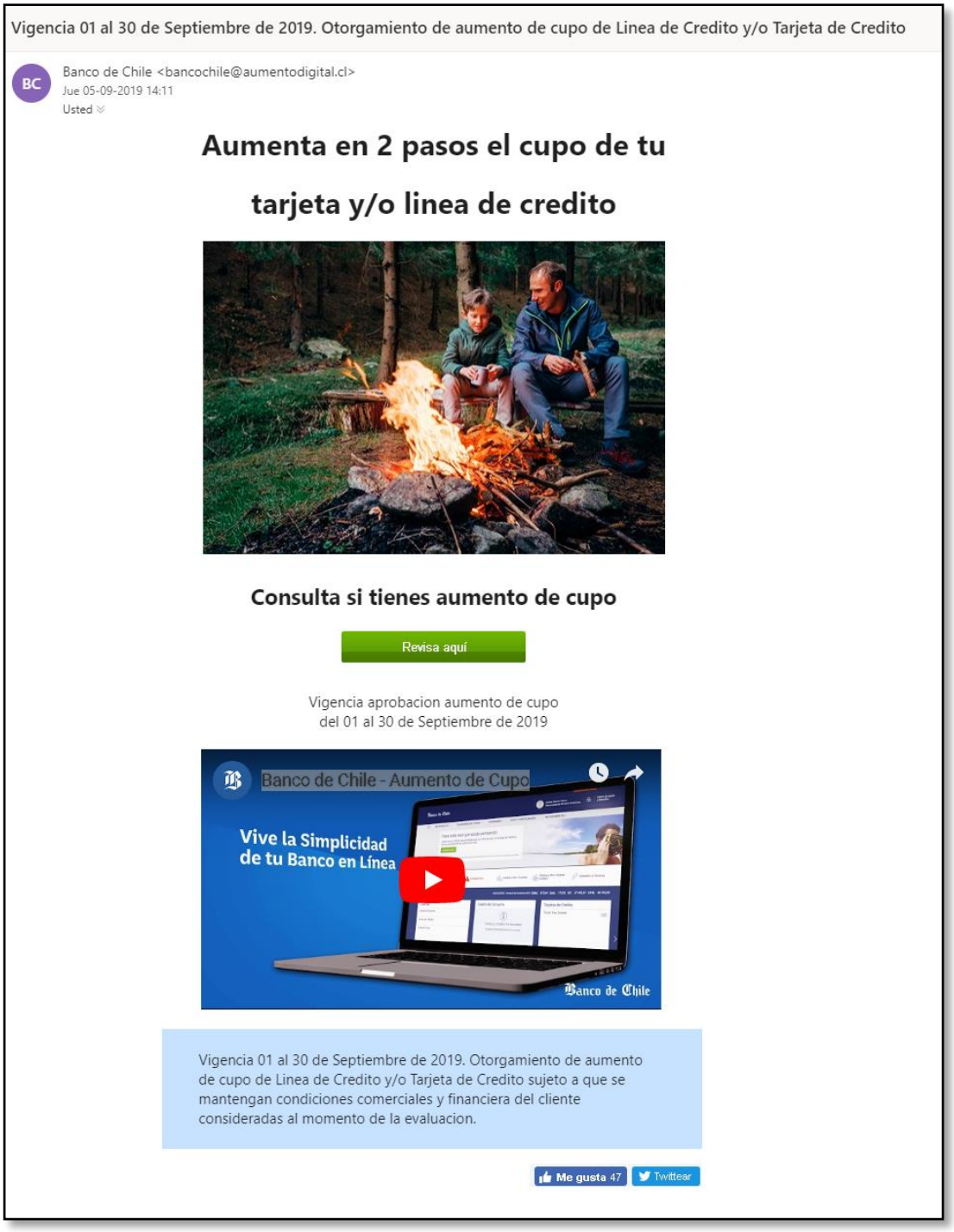
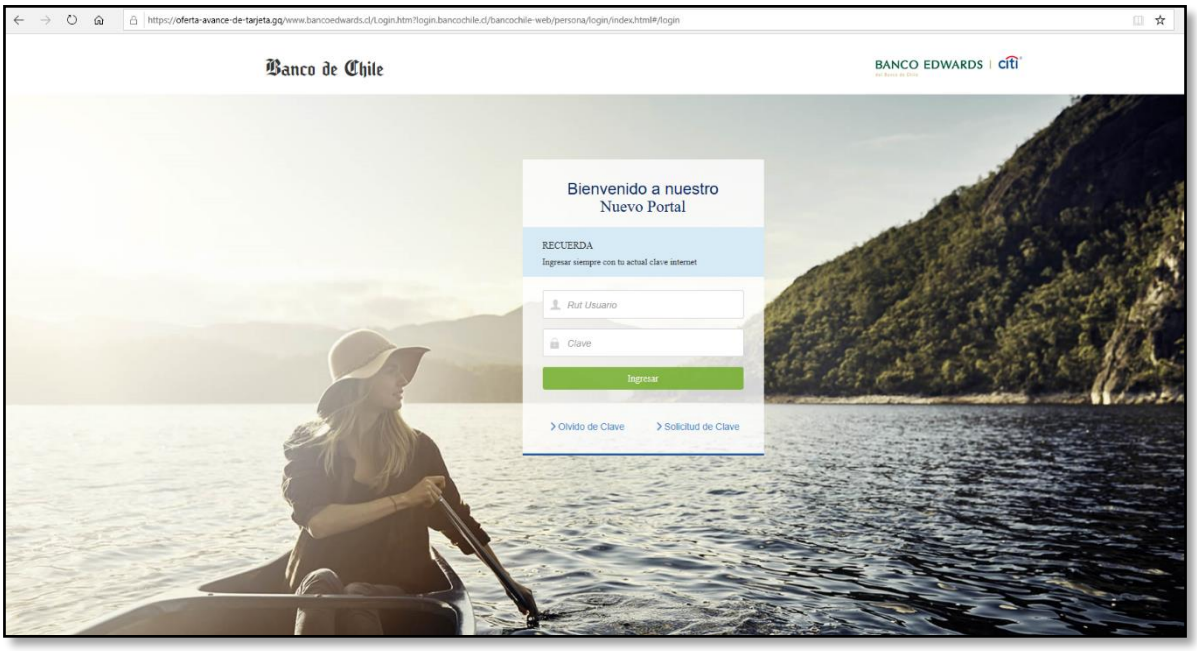


Imagen Sitio Web



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 que sean los oficiales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.09 14:53:11 -03'00'