| | |
|---|---|
| Alerta de seguridad informática | 8FPH20-00116-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Febrero de 2019 |
| Última revisión | 20 de Febrero 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 cuyo mensaje intenta engañar a los usuarios del Banco Edwards del Banco de Chile.

El atacante utiliza un mensaje indicando que revise si tiene un aumento de cupo en su tarjeta y/o línea de crédito. Esta promoción tiene una duración desde el 01 hasta el 29 de Febrero de 2020. Los estafadores disponibilizan un enlace que al seleccionarlo, la víctima es direccionada a un sitio semejante al del Banco de Chile.

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

## Indicadores de compromisos

### Url's:
https[:]//d8[.]gotoproject[.]net/bancochile[.]php
http[:]//smartykids[.]by/email/chile/validacion/8d5e957f297893487bd98fa830fa6413/Login[.]htm

### Sender
apache@chikumashobo.co.jp

### Smtp Host
[210.152.127.66]

### Subject:
Revisa si tienes un aumento en 2 pasos el cupo de tu tarjeta o línea de crédito

### Imagen Phishing Correo

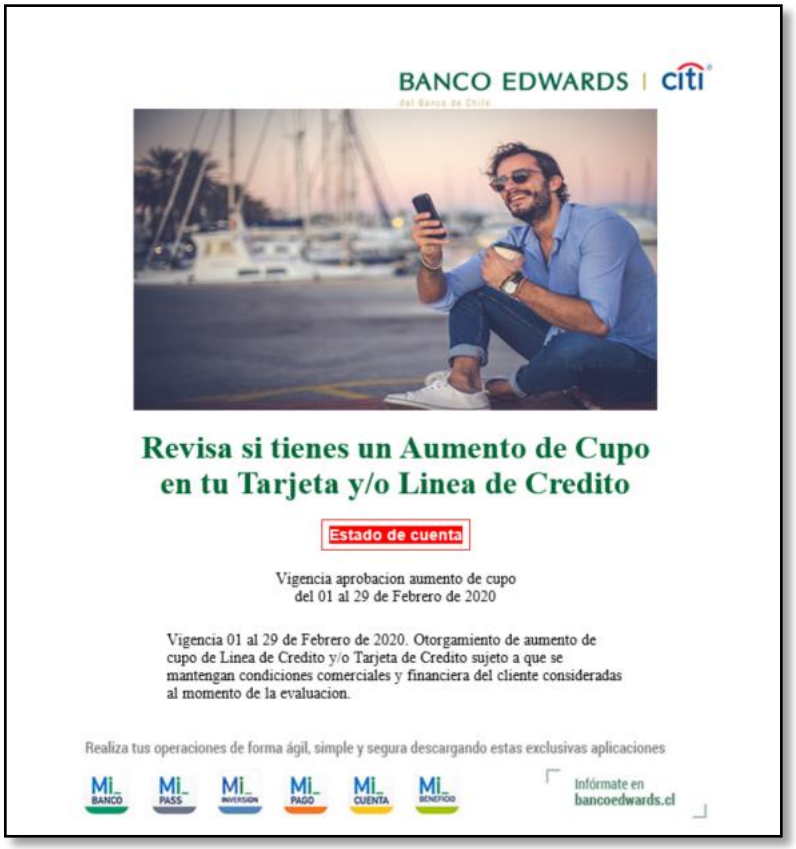
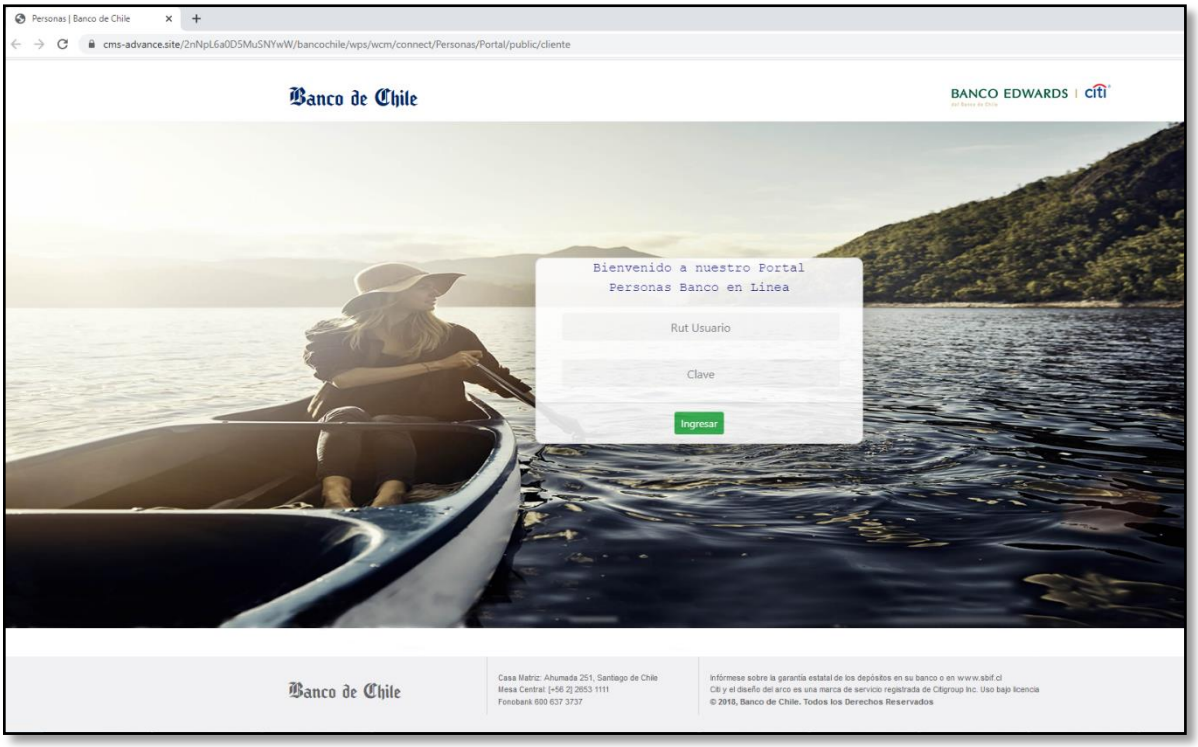


Imagen Sitio Web




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: 2020.02.20 10:05:19 -03'00'