Alerta de Seguridad Informática (8FPH-00049-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Chile. El correo informa a las víctimas que deben revisar si tienen un aumento de cupo en su tarjeta y/o línea de crédito, la cual tiene una vigencia hasta el 31 de julio del 2019. Para verificar la vigencia de la supuesta oferta, se invita al usuario a seleccionar el enlace indicado en el correo, direccionando al afectado a un sitio semejante al del banco para que entregue sus credenciales bancarias.

> “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”

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- https[:]//stcfood[.]dz/wp-content/plugins/cmb2/js/chile/LOA/index[.]php
- https[:]//tokyobbqtown[.]vn/wp-content/upgrade/frxrcgxgvgthvth/bancochile[.]cl/R1/index[.]php
- https[:]//kwhonolulu[.]com/app/uploads/2017/06/hhjh/LOA/index[.]php
- https[:]//www[.]tritonrt[.]eu/wp-content/upgrade/sercivio/LOA/index[.]php
- http[:]//rationalpolitics[.]online/wp-content/languages/themes/mdklcklvkldlkv/LOA/index[.]php
- https[:]//spyinstructor[.]com/cgi-bin/kkmmvmodfkpgvr/LOA/index[.]php
- https[:]//www[.]bizbon[.]com/wp-content/uploads/2014/10/aumentocupo/LOA/index[.]php
- https[:]//aridostlari[.]com/wp-content/uploads/2019/02/tygyyb/LOA/index[.]php
- https[:]//spaseniyestrizhey[.]com[.]ua/wp-includes/fonts/flflfrfr/LOA/index[.]php
- https[:]//www-login-avance-de-linea-credito-cl[.]cf/www[.]bancoedwards[.]cl
- https[:]//www-servicios-cupo-cl[.]cf/ww3[.]bancochile[.]cl/Login[.]htm
- https[:]//www-servicio-de-avance-cl[.]cf/www[.]bancoedwards[.]cl/Login[.]htm
- https[:]//www-login-portal-personas-cl[.]cf/ww3[.]bancochile[.]cl/Login[.]htm
- https[:]//www-servicio-de-avance-cl[.]cf/www[.]bancoedwards[.]cl/Login[.]htm
- http[:]//i64[.]tinypic[.]com/25pqzk6[.]png
- http[:]//i64[.]tinypic[.]com/ivcwzt[.]png
- http[:]//i63[.]tinypic[.]com/23rlqvo[.]png
- http[:]//i63[.]tinypic[.]com/2z53vvr[.]jpg
- http[:]//i64[.]tinypic[.]com/25pqzk6[.]png
- 91[.]209[.]70[.]21

Smtp Host

- 212[.]68[.]46[.]234
- vmi191044[.]contaboserver[.]net

From:

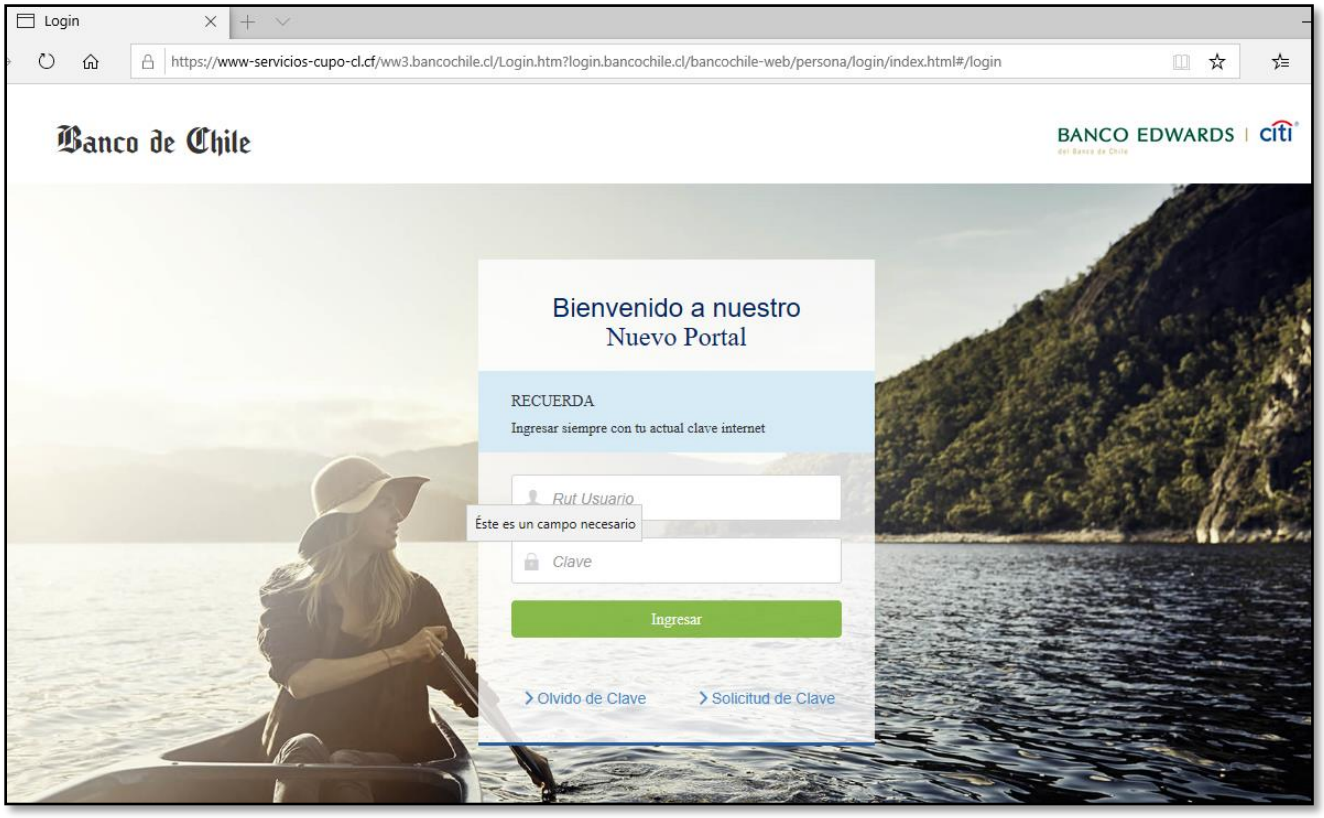
- web-bounce+www.eagle-executives.com@adept.co[.]za
- nobody@linux.acilkitap[.]com
- admin@atad[.]vn
- apache@cp.cashhost[.]net

Subject:

- Obten tu avance de manera rapida y segura para lo que necesites

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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.24 18:31:47 -04'00'