Alerta de seguridad informática	**8FPH-00056-000**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**18 de Agosto de 2019**
Última revisión	**18 de Agosto 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), con la colaboración de usuarios de redes sociales[1], ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco BCI, notificándoles en el correo que su cuenta ha sido suspendida temporalmente ya que su correo electrónico no se encuentra registrado debidamente en la banca por internet. Por lo antes mencionado el atacante solicita ingresar al enlace indicado en el correo. Al hacerlo, el usuario ingresa se expone a que el atacante robe sus credenciales desde un sitio semejante al del Banco.

[1] CSIRT destaca la colaboración de Felipe Ovalle Salinas

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

http[:]//www.cnct.org[.]ar/foros/-/https:/www.bci.cl/Cliente/?
https[:]//www.empresas03[.]com/elegir[.]php
https[:]//www.empresas03[.]com/psn/acs[.]php
https[:]//www.empresas03[.]com/emp/acs[.]php

Smtp Host

[145.239.31.48]
[139.99.219.89]
[139.99.216.39]
[51.79.142.36]
[51.79.140.38]
[51.79.143.79]

From:

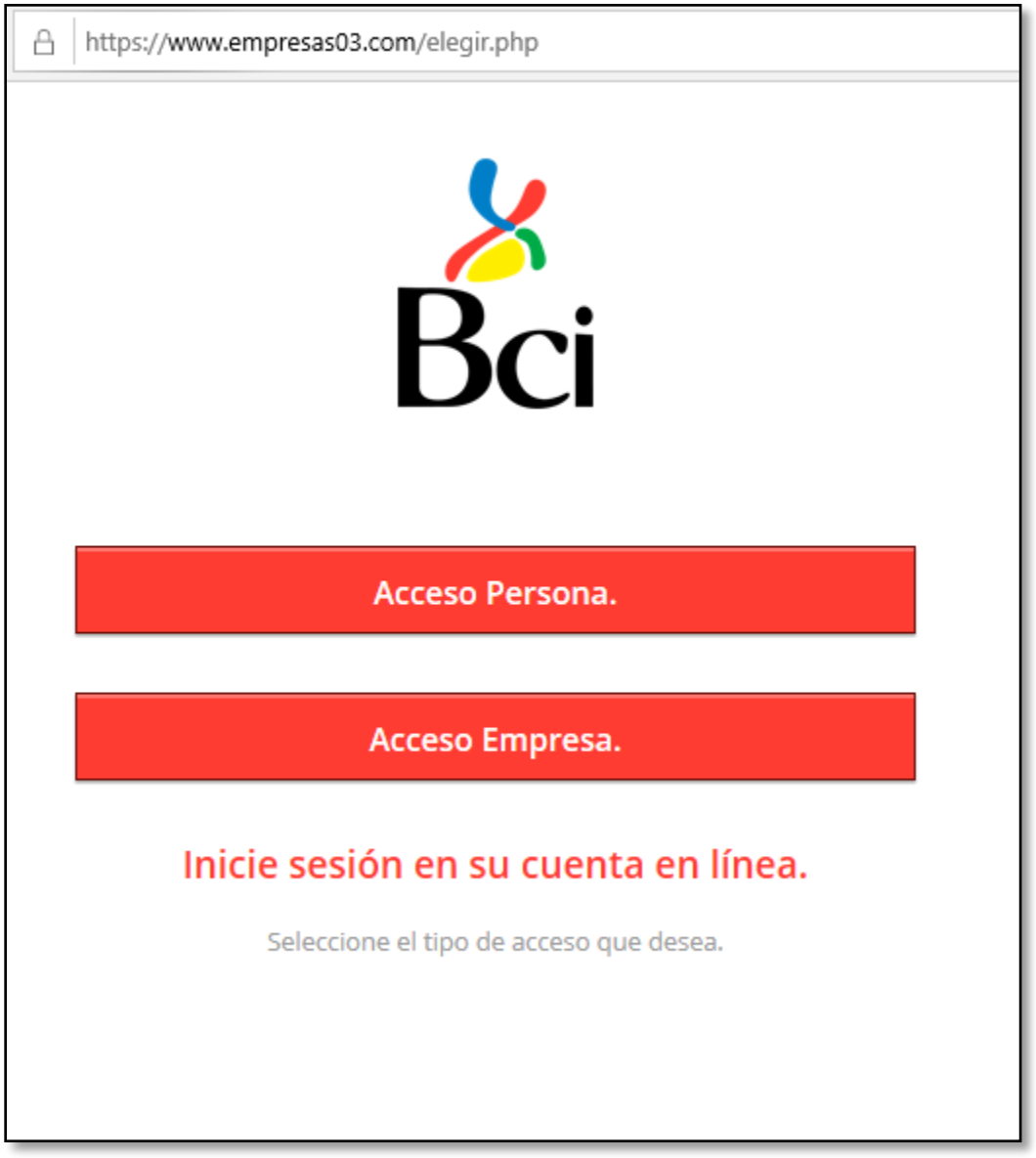
apache@k5[.]eurobueno[.]pictures
apache@j2[.]eurobueno[.]pictures
apache@j3[.]eurobueno[.]pictures
apache@j4[.]eurobueno[.]pictures
apache@j5[.]eurobueno[.]pictures
apache@j6[.]eurobueno[.]pictures
apache@j9[.]eurobueno[.]pictures
apache@h10[.]eurobueno[.]pictures

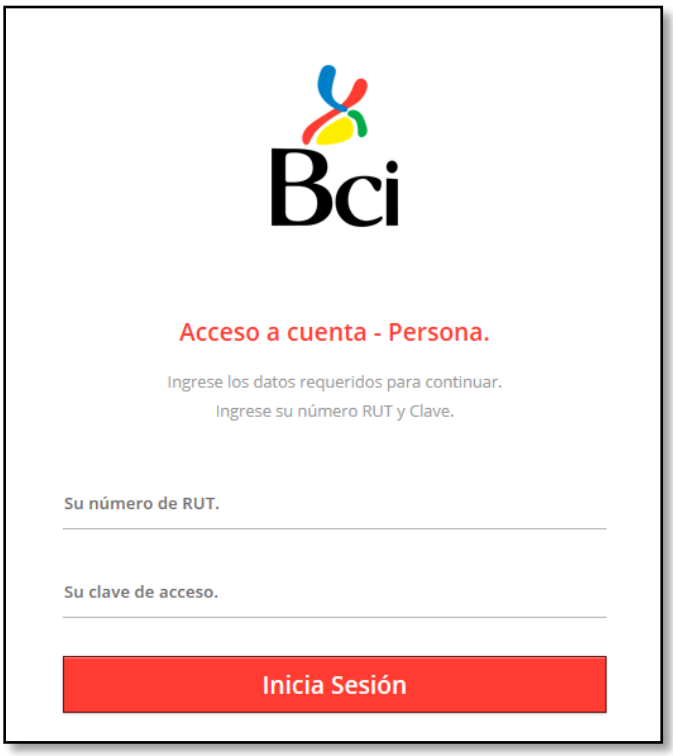
Subject:

Infoemail BCI - Importante - Servicio de Transferencias Bloqueado - (n°)

Imagen Phishing Correo

Imagen Sitio Web




Bci
Acceso a cuenta - Persona.
Ingrese los datos requeridos para continuar.
Ingrese su número RUT y Clave.
Su número de RUT.
Su clave de acceso.
Inicia Sesión


Bci
Acceso a cuenta - Empresa.
Ingrese los datos requeridos para continuar.
Ingrese su número RUT y Clave.
RUT.
Su clave de acceso.
Inicia Sesión

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: 2019.08.18 15:47:22 -04'00'