Alerta de seguridad informática	**8FPH-00057-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**20 de Agosto de 2019**
Última revisión	**20 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), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Estado, notificándoles en el correo que su cuenta ha sido bloqueada temporalmente ya que se han realizado actualizaciones en servidores de procesos bancarios y esgrimiendo que la cuenta no se encontraría registrada debidamente en la banca por internet, el atacante solicita al usuario que ingrese al enlace a través de la imagen indicada en el correo. Si el usuario ingresa al enlace este se expone a que el atacante robe sus credenciales desde un sitio semejante al del Banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

http[:]//contadores[.]site/readme/Simuladores/
http[:]//www[.]infallthings[.]com/impt/imágenes/comun2008/banca-en-linea-personas[.]html

Smtp Host

[45.236.129.99]

From: (Original)

apache@trikitrack.net

From: (Falso):

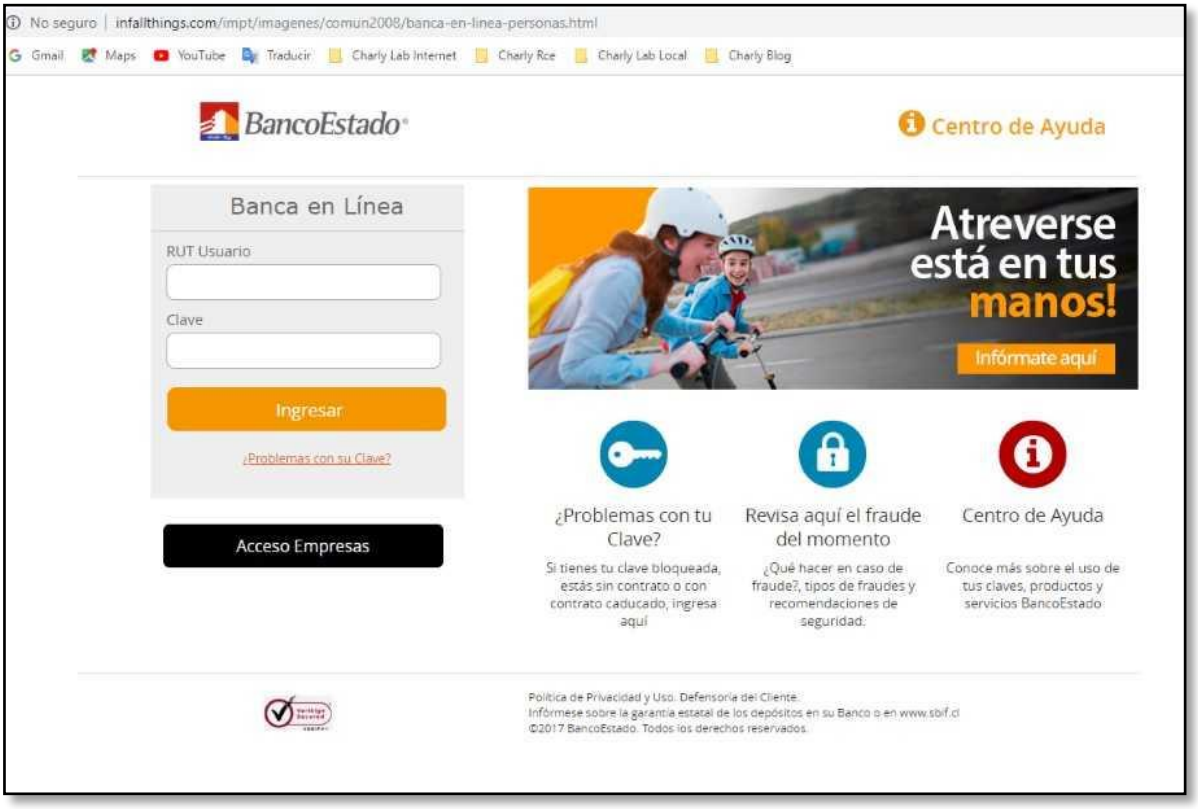
bancoestado@plusconsulting.cl

Subject:

Aviso Importante: Cuenta Bloqueada

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: 2019.08.20
17:07:30 -04'00'