

Alerta de seguridad informática	8FPH-00061-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Septiembre de 2019
Última revisión	10 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 afectada 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 persuadir a los usuarios del Banco Estado para que realicen una actualización utilizando un enlace dentro del cuerpo del correo. El mensaje señala que se realizó una actualización de las cuentas, pero que ya estarían operativos. Producto de la actualización, los criminales advierten a la potencial víctima sobre la detección de un error en su cuenta, razón por la que se procedió al bloqueo de la misma de forma temporal. Los estafadores señalan que la única forma de desbloquear la cuenta es ingresando al enlace malicioso oculto en el enlace. A través de ingeniería social, el atacante incita a sus víctimas para ingresar al enlace, exponiéndolos al robo de sus credenciales desde un sitio semejando al del Banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

[http://gothamglassworks\[.\]com/dr9/imagenes/comun2008/banca-en-linea-personas.html](http://gothamglassworks[.]com/dr9/imagenes/comun2008/banca-en-linea-personas.html)

[http://axnpop\[.\]site/readme/Simuladores/](http://axnpop[.]site/readme/Simuladores/)

Smtip Host

hwsrv-561036.hostwinddns[.]com [104.168.243.238]

hwsrv-561039.hostwinddns[.]com [104.168.243.220]

Sender:

apache@hwsrv-561036.hostwinddns[.]com

apache@hwsrv-561039.hostwinddns[.]com

Subject:

✓ Fw: Cuenta Bloqueado

Imagen Phishing Correo



BancoEstado | CON TODOS PARA TODOS
CORREDORES DE SEGUROS

Con esta dupla no hay días fríos



Estimado(a)

Banco de Estado, le comunica que nuestros servidores de procesos bancarios han sido actualizados y ya estan operativos.

Sin embargo debido que su cuenta no se encuentra registrada correctamente, nos vemos en la obligacion de **Bloquearla Temporalmente**.

Puede Restablecer su cuenta haciendo clic sobre la imagen, con esta accion su cuenta quedara restaurada de forma permanente. solo podra hacerlo por medio de este e-mail.

Para activar su cuenta ingrese Aqui. 

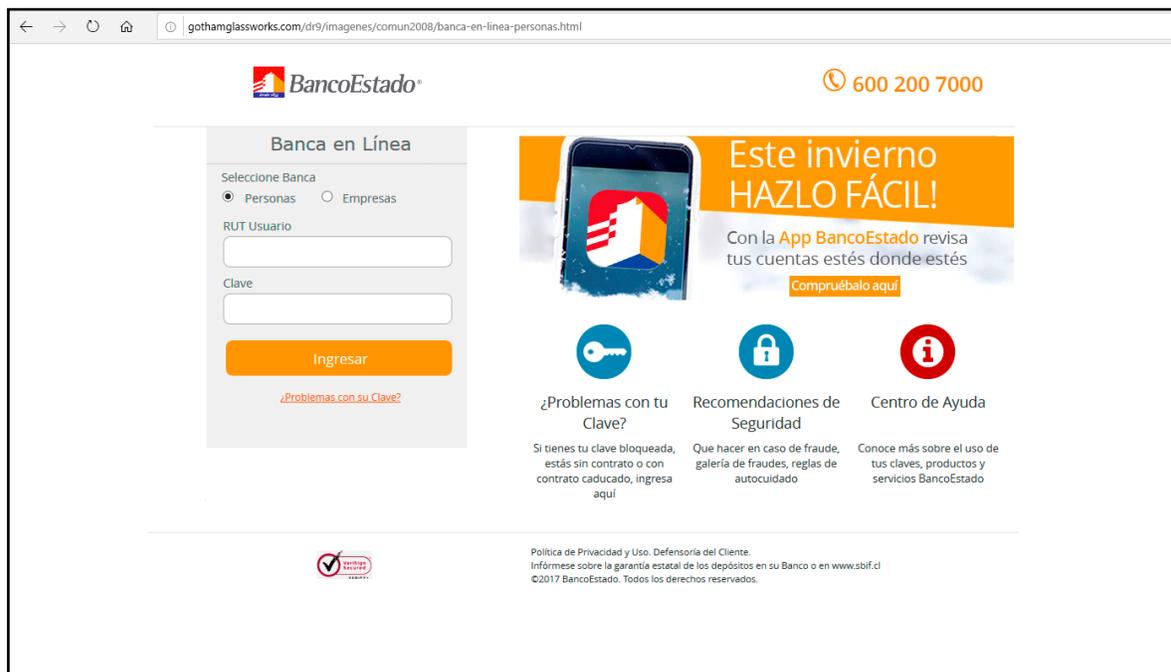
https://www.bancoestado.cl/Seguridad/Activacion_Cuenta

www.bancoestado.cl



600 200 6000
bancoestado.cl

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