Alerta de Seguridad Informática (8FPH-00039-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 25 de Junio de 2019 | Última revisión 25 de Junio 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 Estado. El correo trata de persuadir a los clientes del Banco para que vuelvan a activar su cuenta, de lo contraria podría quedar bloqueada. Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

Indicadores de compromisos

Url's:

http[:]//www.tennis-russia[.]ru/en/public/personas_bancoestado

https[:]//metroo[:]ir/id/home/imagenes/comun2008/banca-en-linea-personas.html

Smtp Host

seleccion.com [190.114.254.208]

Sender

apache@seleccion[.]com

From (Falso):

BancoEstado <bancoestado@plusconsulting[.]cl>

Subject:

✓ Alerta Cuenta Inhabilitada - (Activar Urgente)

Imagen Phishing correo

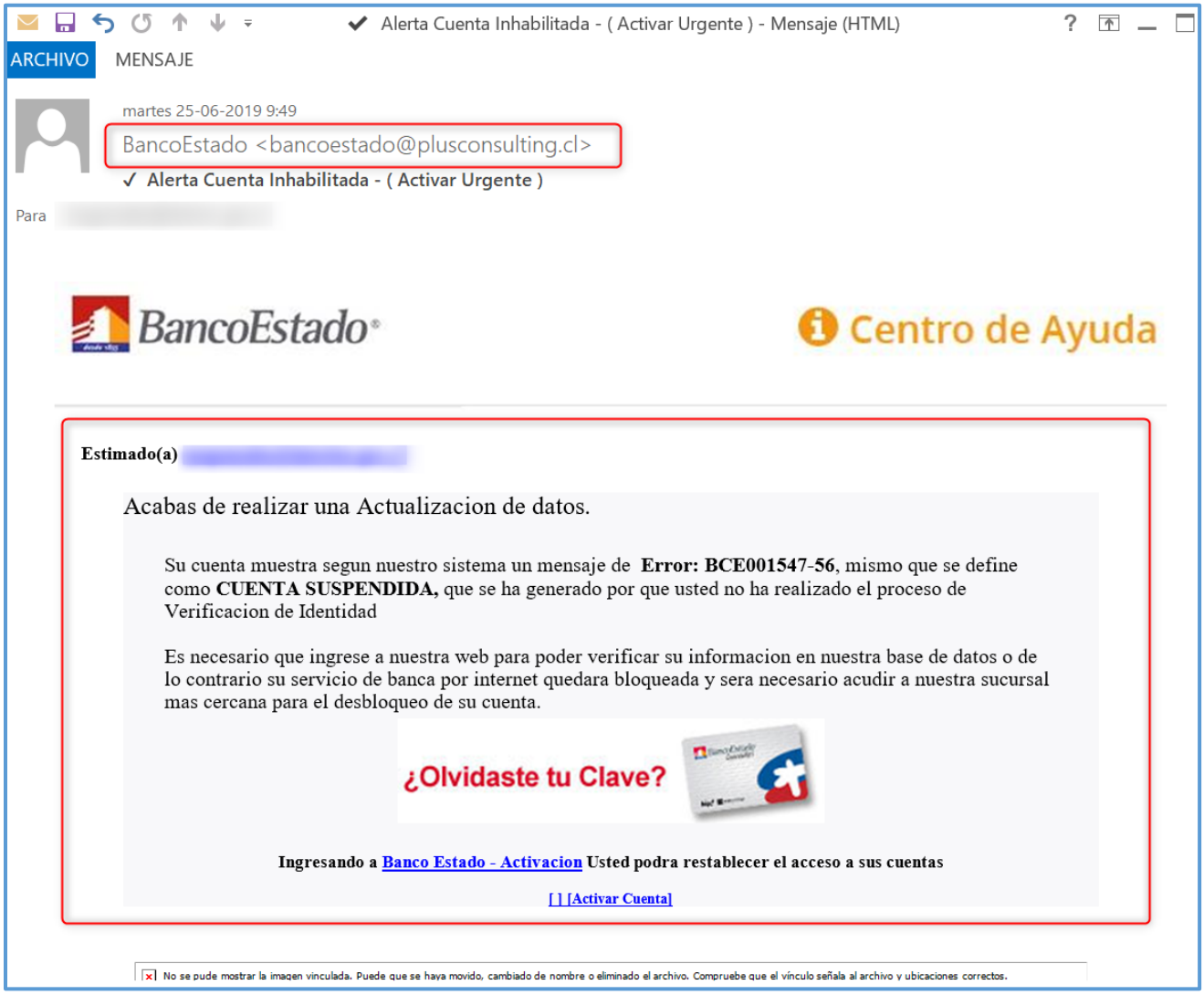
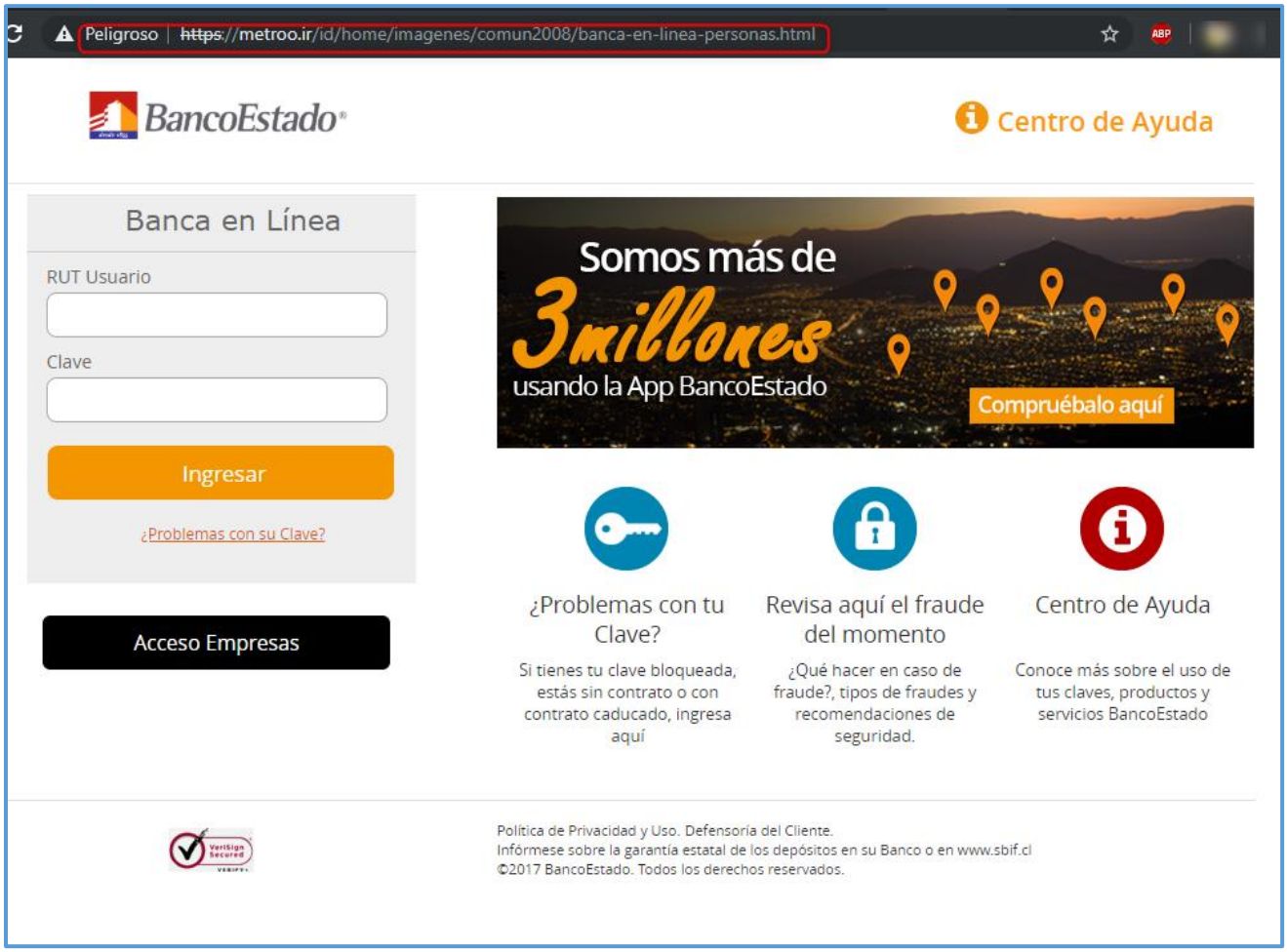


Imagen Sitio Phishing



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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

Contactos

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