Alerta de Seguridad Informática (8FPH-00044-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 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 Estado.

El correo trata de persuadir a los clientes del Banco indicándoles que se realizó un proceso de actualización en sus servidores, sin embargo su cuenta se encuentra bloqueada temporalmente y para restablecerla debe hacer clic en un enlace (imagen) para así activar su cuenta inmediatamente.

El mensaje estable que solo se puede realizar este procedimiento con el hipervínculo señalado en el correo, de esta forma los criminales tratan de persuadir a al usuario a realizar clic en el hipervínculo de la imagen, solicitando las credenciales de acceso. Este enlace redirige a la víctima a un sitio falso semejante al de Banco Estado.

> “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[:]//helloiloa[.]gq/MicroEmpresas/beneficios/
- http[:]//3dprintsibiu[.]ro/js/Team/imagenes/comun2008/banca-en-linea-personas[.]html

Smtp Host

- pr0mart[.]net [170.239.86.133]
- Vicky[.]net [170.239.86.154]

Sender

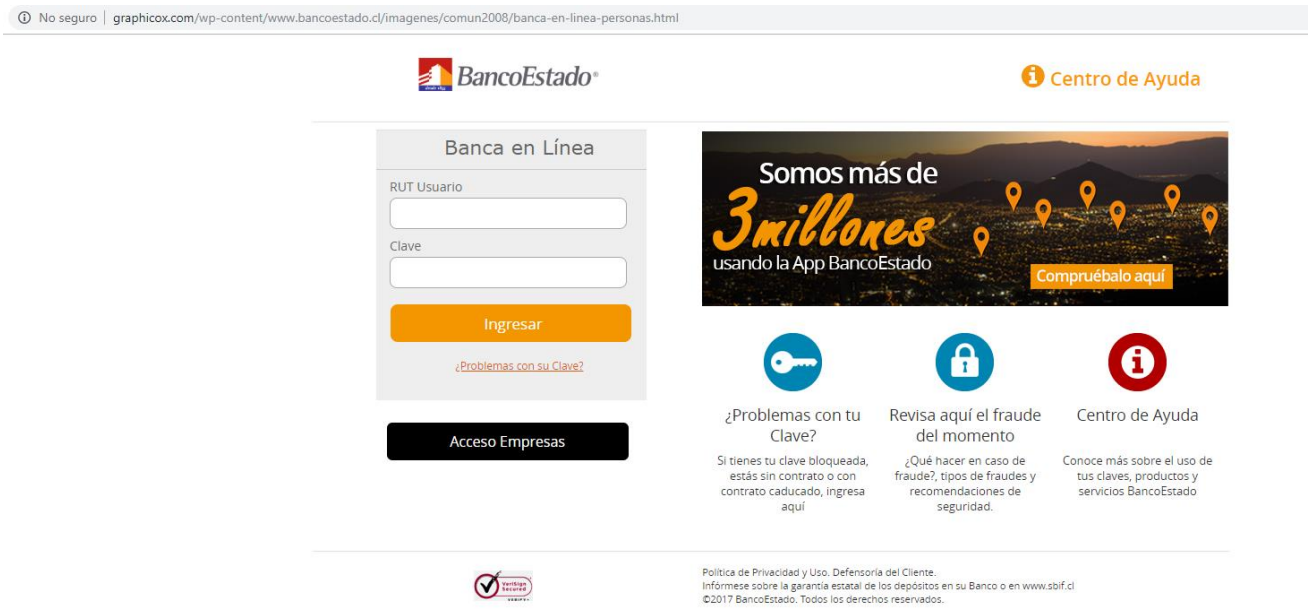
- apache@pr0mart[.]net
- apache@vicky[.]net

Subject:

- Fwd:Cuenta Bloqueada.

Imagen Phishing correo

Imagen Sitio Web



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
- 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: 2019.07.17
19:24:07 -04'00'