Alerta de seguridad informática	**8FFR-00013-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**09 de Agosto de 2019**
Última revisión	**09 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 fraude no involucran a directamente a las entidades ni al sistema bancario, sino que son técnica de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, 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 llamado a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado una serie de dominios que se sospecha podrían ser utilizados para suplantar el sitio web oficial del **bancoestado.cl** con el objetivo de perjudicar a usuarios, clientes y al banco aludido.

El CSIRT informó oportunamente a la entidad bancaria con el objetivo de desechar cualquier tipo de relación de propiedad u otra con el sitio sospechoso, así como para coordinar una respuesta adecuada para contener el incidente.

Actualmente los sitios señalados están inactivos, pero pueden ser activados en cualquier momento con los fines antes señalados.

Indicadores de Compromisos

Dominios

bancestado[.]icu
bancestado[.]org
bancoestado-cl[.]top
bancoestadocl[.]com
bancoestadonline[.]com
bancoestados[.]com
elbancoestado-cl[.]com
bancoestados-cl[.]com
bancoestadovdz[.]com
bancoestado[.]com

Recomendaciones

- Evitar acceder a las páginas asociadas a los dominios anteriormente indicados, e informar a los usuarios sobre la existencia de los sitios, para que no ser víctimas del fraude.
- Ser precavidos frente a páginas fraudulentas, provienen de los dominios Informados.
- Bloquear en los proxy o sistemas de control de contenido
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.09 18:30:19 -04'00'