Alerta de seguridad informática	**8FFR-00010-002**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Medio**
TLP	**Blanco**
Fecha de lanzamiento original	**31 de Julio de 2019**
Última revisión	**07 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 actualizado la información sobre la activación de portales fraudulentos que suplantan el sitio web oficial del **BANCOESTADO.CL** que se informó el 31 de julio pasado, y que tenían como objetivo obtener las credenciales de potenciales víctimas. Algunos de los sitios incluso cuentan con certificados que les permiten tener el candado para brindar la sensación de seguridad a los usuarios que puedan ser víctimas del fraude.

Lo anterior constituye una falsificación de la marca institucional con fines de fraude hacia los usuarios y/o clientes de la entidad afectada.

CSIRT quiere informar que los dominios informados en su oportunidad fueron neutralizados antes de que pudieran ser utilizados por los atacantes.

Indicadores de Compromisos

URL´s

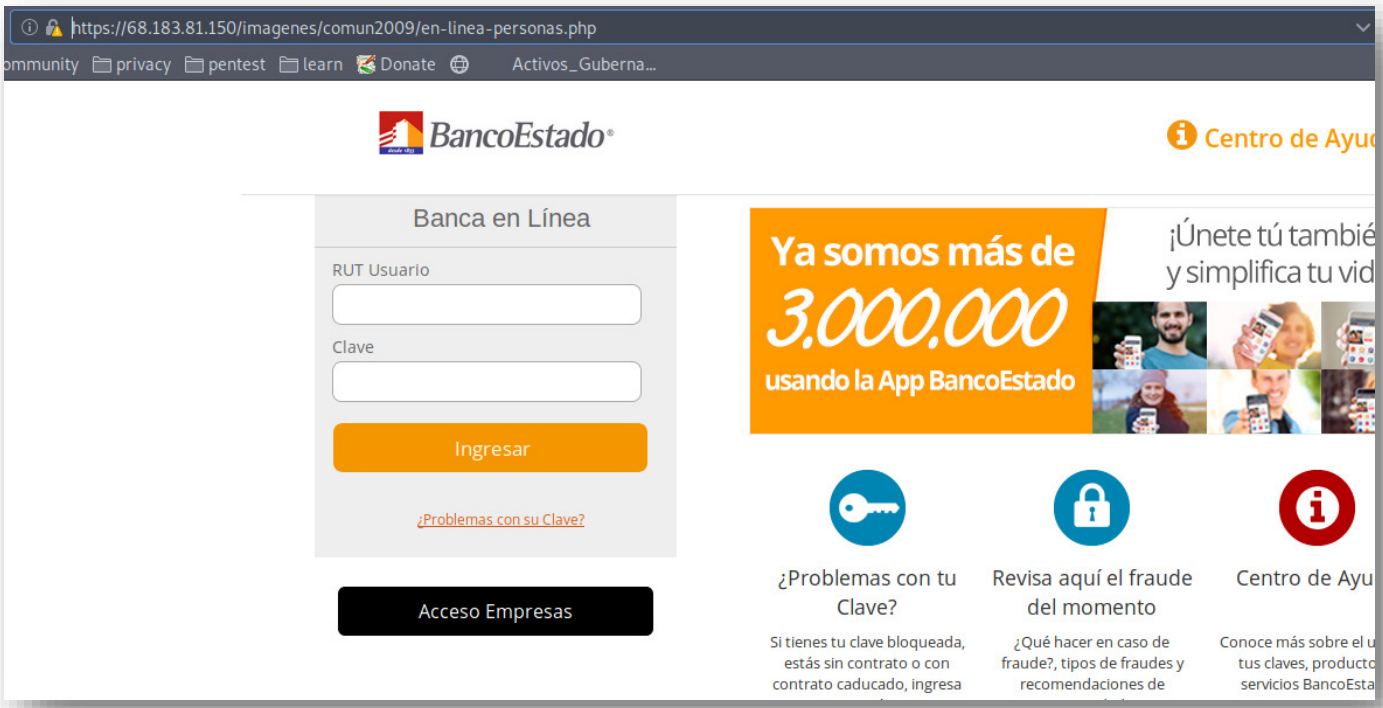
http[:]//bncostado-cl[.]xyz
https[:]//bncostado[.]xyz/imagenes/comun2009/en-linea-personas[.]php
bncostado[.]xyz
bncostado-cl[.]xyz
http[:]//bncostado-cl[.]xyz/imagenes/comun2009/en-linea-personas[.]php
http[:]// bancoestad-cl[.]xyz[.]
http[:]// bancostado-cl[.]xyz[.]
http[:]// bankestado-cl[.]xyz[.]
http[:]// bncostado-cl[.]xyz[.]
http[:]// bncostado[.]xyz[.]
http[:]// bancoestado-cl[.]link
http[:]// Bancoestado[.]online
http[:]// Bncoestado[.]top
http://bancoestado[.]don-seguridad[.]com/login[.]html
http://decksoldier[.]com/info/www[.]bancoestado[.]cl/imagenes/comun2008/nuevo_paglg_pers2[.]html http://estadodecitius[.]pt/IlOysTgNjFrGtHtEAwVo/indexx[.]php
http://lenintextile[.]com/onedrive/www[.]bancoestado[.]cl/imagenes/comun2008/nuevo_paglg_pers2[.]html http://perinadesign[.]com[.]br/wp-includes/www[.]bancoestado[.]cl/imagenes/comun2008/nuevo_paglg_pers2[.]html
https://demositeslive[.]com/-/https://www[.]bancoestado[.]cl/?cliente=renata[.]sachez@sgurlepei[.]com
https://ww2[.]bancoestado[.]cl-q[.]pw/bancenlinea/index[.]php
https://www[.]bancoestado[.]cl-j[.]pw/bancanlinea http://chiropas[.]com/estado
http://evmade[.]com/docs/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html http://gamebattleground[.]net/wp-admin/bestado
https://bancoestado[.]e-estudios[.]cl https://bancoestado[.]e-estudios[.]cl/login
http://www[.]bancoestado[.]cl[.]imagenes[.]comun2008[.]banca_en_linea_persona[.]dfgum[.]club/wps
http://www[.]bancoestado[.]cl[.]imagenes[.]comun2008[.]banca_en_linea_personas[.]zary[.]club/wpf
http://www[.]bancoestado[.]cl[.]imagenes[.]comun2008[.]banca_en_linea_personas[.]zarys[.]club/wpf
http://www[.]bancoestado[.]cl[.]imagenes[.]comun2008[.]banca_en_linea_personas[.]zarys[.]xyz/wpf http://www[.]carpetworldlondon[.]com/fonts/personas_bancoestado[.]cl

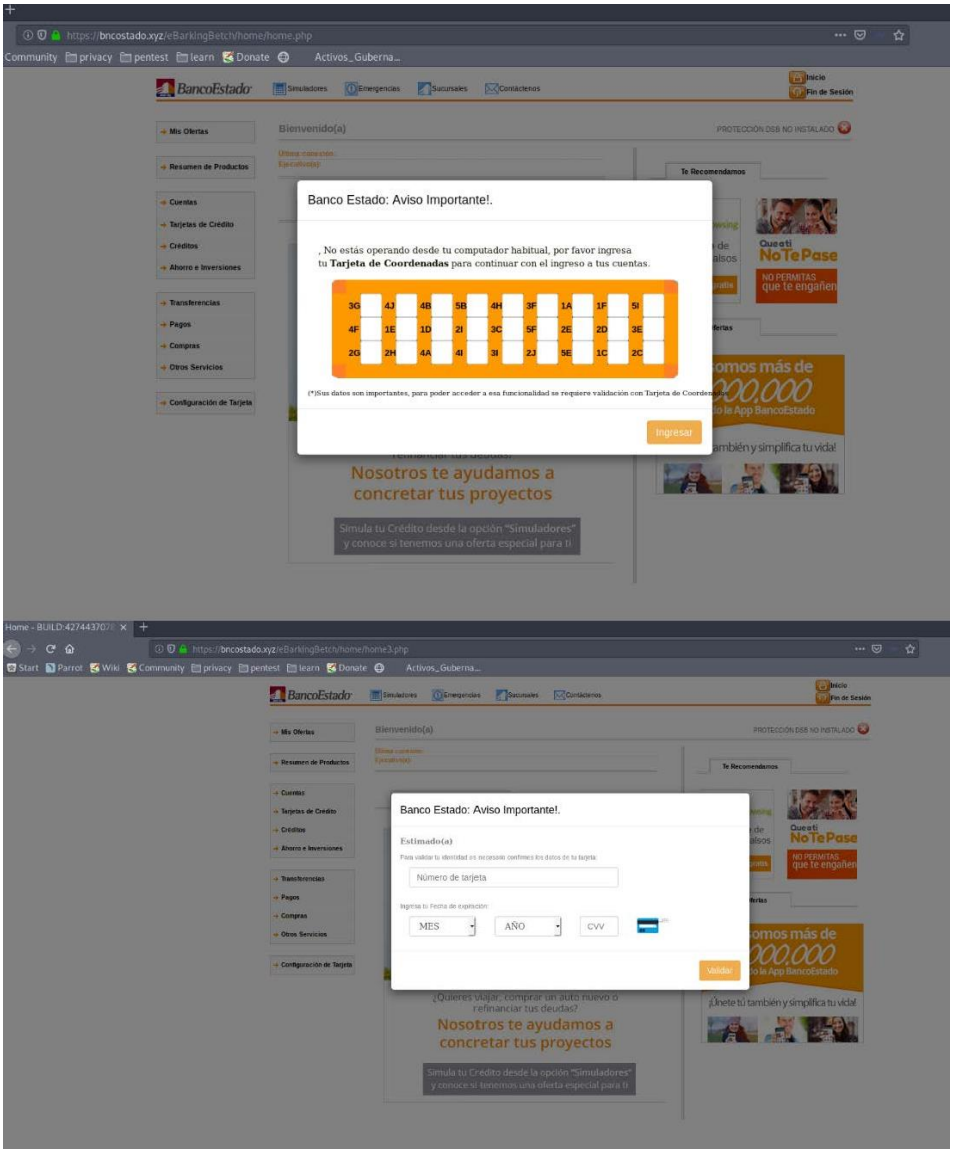
IP's
68.183.81.150
139.59.66.85

Localización en red

AS14061 DigitalOcean, LLC, geolocalizado en la India.
AS19817 DSL Extreme, geolocalizada en los EE.UU.

Imagen de los sitios




Banco Estado: Aviso Importante!.
, No estás operando desde tu computador habitual, por favor ingresa tu Tarjeta de Coordenadas para continuar con el ingreso a tus cuentas.
Ingresar
Nosotros te ayudamos a concretar tus proyectos
Banco Estado: Aviso Importante!.
Estimado(a)
Número de tarjeta
MES
AÑO
CVV
Validar
Nosotros te ayudamos a concretar tus proyectos

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre la existencia del sitio, para que no ser víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- 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: 2019.08.07
19:59:12 -04'00'