Alerta de seguridad informática	**8FFR-00034-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**31 de Agosto de 2019**
Última revisión	**31 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 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 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 llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portal fraudulentos asociados a una IP que suplantan el sitio web oficial del bancoestado.cl, los que podrían servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s
http[://]spart4[.]com/dr9/imagenes/comun2008/banca-en-linea-personas[.]html

IP
192[.]185[.]76[.]253

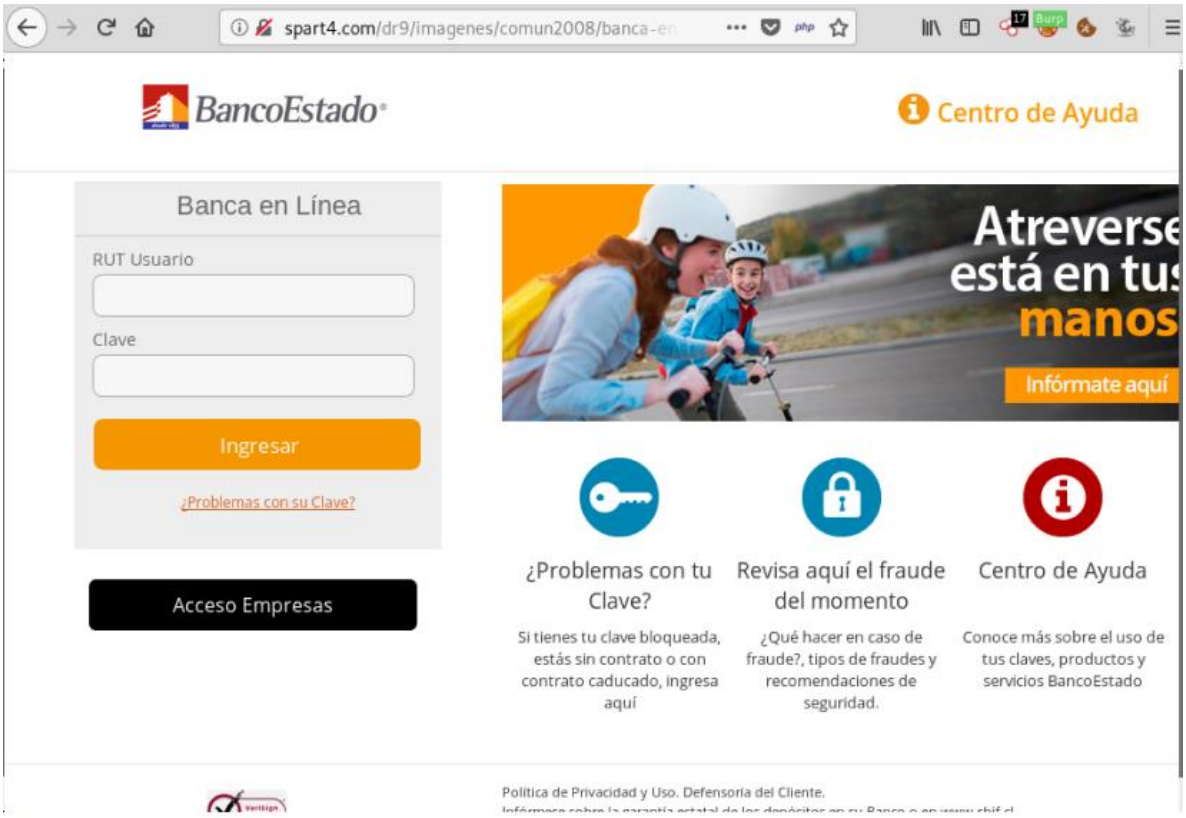
Localización

Texas, Estados Unidos

Whois

```
soc@kali:~$ whois -h whois.namesilo.com spart4.com
Domain Name: spart4.com
Registry Domain ID: 2427972648_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-08-29T07:00:00Z
Creation Date: 2019-08-29T07:00:00Z
Registrar Registration Expiration Date: 2020-08-29T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller: QHOSTER.COM
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: junior peralta
Registrant Organization:
Registrant Street: Argomedo Ndeg 1698
Registrant City: lima
Registrant State/Province: lima
Registrant Postal Code: 0051
Registrant Country: PE
Registrant Phone: +51.935952482
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: juniorperalta347@gmail.com
Registry Admin ID:
Admin Name: junior peralta
Admin Organization:
Admin Street: Argomedo Ndeg 1698
Admin City: lima
Admin State/Province: lima
Admin Postal Code: 0051
Admin Country: PE
Admin Phone: +51.935952482
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: juniorperalta347@gmail.com
Registry Tech ID:
Tech Name: junior peralta
Tech Organization:
Tech Street: Argomedo Ndeg 1698
Tech City: lima
Tech State/Province: lima
Tech Postal Code: 0051
Tech Country: PE
Tech Phone: +51.935952482
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: juniorperalta347@gmail.com
Name Server: NS1295.WEBSITEWELCOME.COM
Name Server: NS1296.WEBSITEWELCOME.COM
DNSSEC: unsigned
```

Imagen


spart4.com/dr9/imagenes/comun2008/banca-en
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Atreverse está en tus manos
Infórmate aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en 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: 2019.08.30
22:14:31 -04'00'