| | |
|---|---|
| **Alerta de seguridad informática** | **8FFR-00056-001** |
| **Clase de alerta** | **Fraude** |
| **Tipo de incidente** | **Falsificación de Registros o Identidad** |
| **Nivel de riesgo** | **Alto** |
| **TLP** | **Blanco** |
| **Fecha de lanzamiento original** | **11 de Septiembre de 2019** |
| **Última revisión** | **11 de Septiembre 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial del **banco Estado.cl,** el que podría 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.

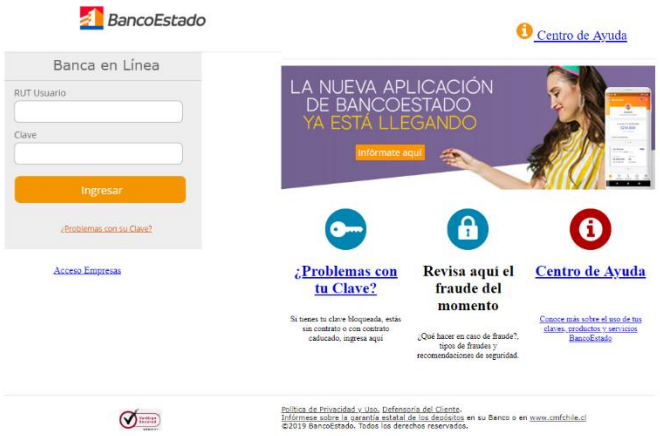
**Indicadores de Compromisos**

**URL de redirección:**
https://bncestad0[.]000webhostapp[.]com/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

**IP´s**
153[.]92[.]0[.]100

**Localización**
Ashburn, Virginia  United States

**Ejemplo de Imagen del sitio**



**Whois**

```
soc@kali:~$ whois 000webhostapp.com
   Domain Name: 000WEBHOSTAPP.COM
   Registry Domain ID: 2027404438_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.hostinger.com
   Registrar URL: http://www.hostinger.com
   Updated Date: 2017-04-05T08:04:14Z
   Creation Date: 2016-05-11T13:34:12Z
   Registry Expiry Date: 2022-05-11T13:34:12Z
   Registrar: Hostinger, UAB
   Registrar IANA ID: 1636
   Registrar Abuse Contact Email: abuse@hostinger.com
   Registrar Abuse Contact Phone: +37064503378
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: DNS1.000WEBHOST.COM
   Name Server: DNS2.000WEBHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-09-10T03:06:45Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

**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, hacia la URL maliciosa
- 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: 2019.09.11 13:58:25 -03'00'