

Alerta de seguridad informática	8FFR-00014-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Agosto de 2019
Última revisión	10 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 loC 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 loC 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 identificado la activación de un portal fraudulento que suplanta el sitio web oficial del **bancoestado.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's

https[:]//viveropaztrana-urban[.]net

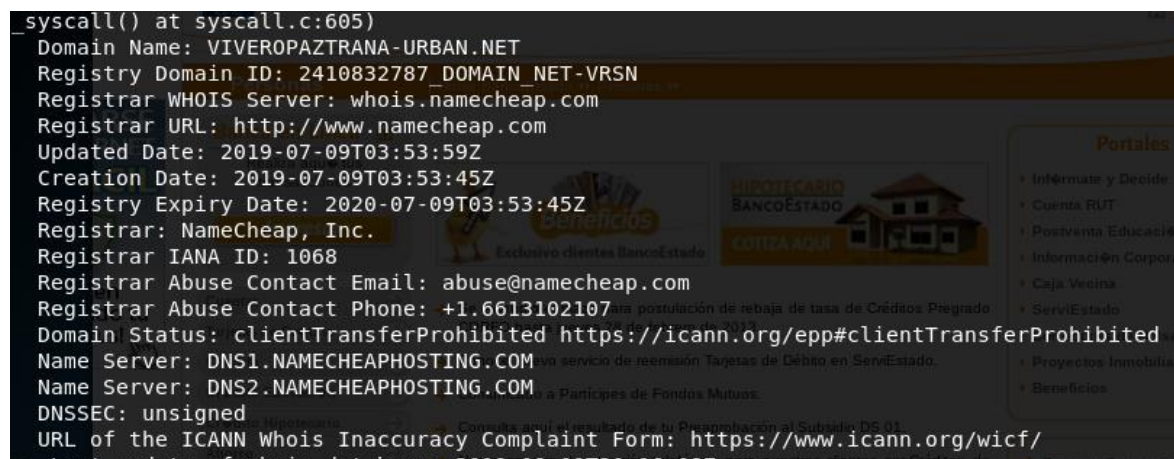
### IP

198.187.29.150

### Localización

United States, Atlanta, Georgia

```
syscall() at syscall.c:605)
Domain Name: VIVEROPAZTRANA-URBAN.NET
Registry Domain ID: 2410832787_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2019-07-09T03:53:59Z
Creation Date: 2019-07-09T03:53:45Z
Registry Expiry Date: 2020-07-09T03:53:45Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.NAMECHEAPHOSTING.COM
Name Server: DNS2.NAMECHEAPHOSTING.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
Last update of whois database: 2019-08-09T20:16:00Z
```



## Ejemplo de Imagen del sitio



BancoEstado Personas

https://viveropaztrana-urban.net/83617C429A994E009BA0BDFB9916156/C8A...

Simuladores Tarifas Red de Atención Emergencias  
Mapa del Sitio

602 202 7077  
Contacto  
Inicio

Personas | Home BancoEstado >> Personas >>

**Banca en Línea**  
Realiza aquí tus transacciones  
**Ingresar**

**Beneficios**  
Exclusivo clientes BancoEstado

**HIPOTECARIO BANCOESTADO**  
COTIZA AQUÍ

**Portales**

- ▶ Infórmate y Decide
- ▶ Cuenta RUT
- ▶ Postventa Educación
- ▶ Información Corporativa
- ▶ Caja Vecina
- ▶ ServiEstado
- ▶ Corredores de Bolsa
- ▶ Proyectos Inmobiliarios
- ▶ Beneficios

→ Bases y Concursos

→ Boletas y Facturas

→ Pagos de Servicios

→ Servicios **24 HORAS**

Cuentas →  
Tarjetas de Crédito →  
Crédito →  
Crédito Educación →  
Crédito Hipotecario →  
Ahorro →  
Inversiones →  
Seguros →  
Pagos Electrónicos →  
Envío de Dinero →  
Propiedades →

→ Se extendió el plazo para postulación de rebaja de tasa de Créditos Pregrado CORFO hasta jueves 28 de febrero de 2013.

→ Conoce nuevo servicio de reemisión Tarjetas de Débito en ServiEstado.

→ Comunicado a Partícipes de Fondos Mutuos.

→ Consulta aquí el resultado de tu Preaprobación al Subsidio DS 01.

→ Nuevo servicio de atención telefónica para nuestros clientes con Créditos de Educación, 600 264 2020. Horario de atención: lunes a viernes de 9:00 a 18:00 hrs. Para otras consultas llamar al 602 202 7077.

→ Ahora puedes reestructurar tu crédito hipotecario moroso y bajar tu dividendo.

¿PASE RNET? ¡CIL!  
¿cómo lo usas!

## 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