

Alerta de seguridad informática	8FFR-00055-001
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 investigaciones propias del equipo CSIRT. La información contenida en los informes o comunicados está afectada 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 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**. 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:

http[:]and[0]ip[.]site/sql/imagenes/comun2008/banca-en-linea-personas[.]html
https[:]bnc0stadocl[.]000webhostapp[.]com

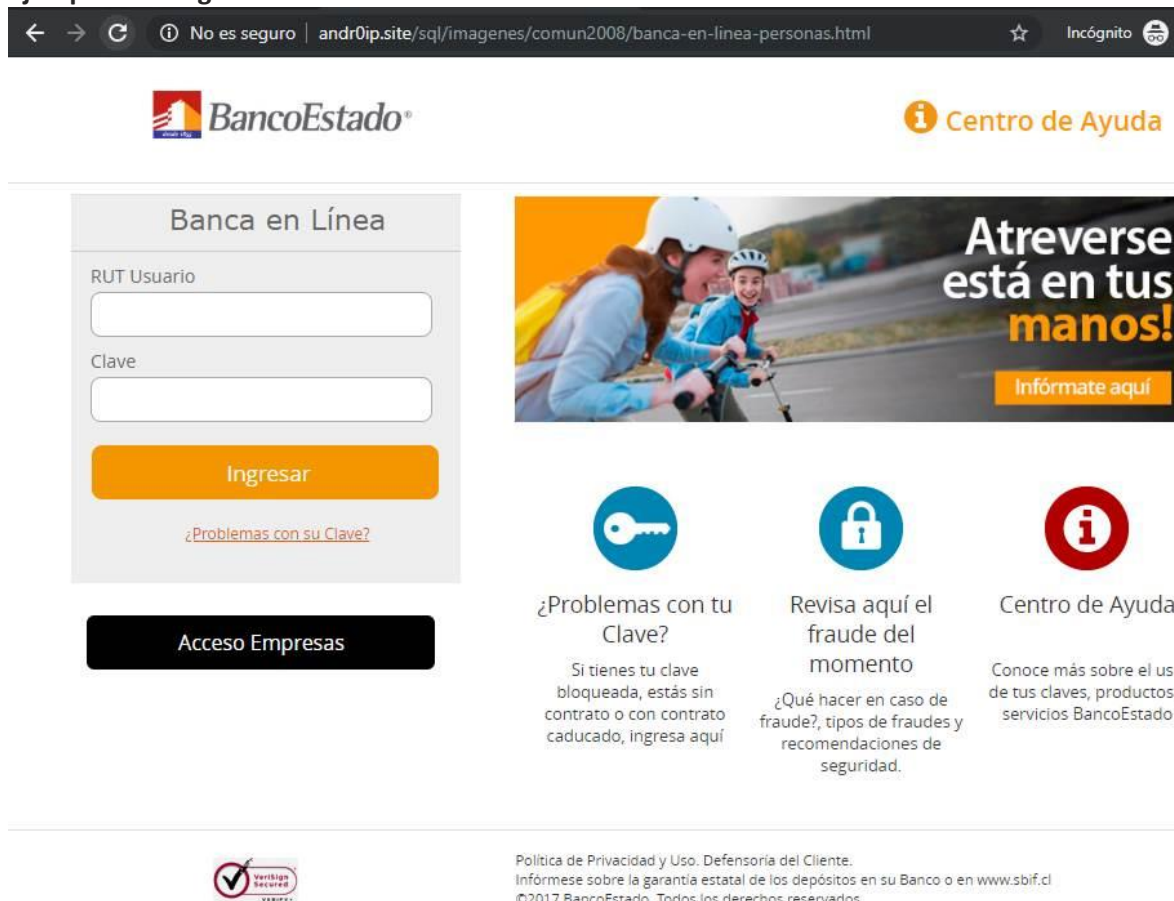
IP's

158[.]106[.]136[.]179
198[.]58[.]118[.]167

Localización

Dallas, Texas, Estados Unidos

Ejemplo de Imagen del sitio



The screenshot shows the BancoEstado website interface. At the top, there is a navigation bar with the BancoEstado logo and a 'Centro de Ayuda' link. The main content area features a 'Banca en Línea' login form with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is an 'Acceso Empresas' button. To the right, there is a large banner with the text 'Atreverse está en tus manos!' and a 'Infórmate aquí' button. Below the banner are three circular icons: a key, a padlock, and an information icon. Each icon has a corresponding text block: '¿Problemas con tu Clave?' (with subtext about blocked or expired keys), 'Revisa aquí el fraude del momento' (with subtext about fraud types and security recommendations), and 'Centro de Ayuda' (with subtext about using keys and products). At the bottom, there is a 'Verisign Internet' logo and a footer with 'Política de Privacidad y Uso. Defensoría del Cliente. Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl ©2017 BancoEstado. Todos los derechos reservados.'

Whois

```
soc@kali:~$ whois -h whois.cdmon.com androip.site
Domain Name: ANDROIP.SITE
Registry Domain ID:
Registrar WHOIS Server: whois.cdmon.com
Registrar URL: https://www.cdmon.com
Updated Date: 2019-09-09T19:50:05Z
Creation Date: 2019-09-09T17:50:05Z
Registrar Registration Expiration Date: 2020-09-09T23:59:59Z
Registrar: IODENCEHISPAHARD, S.L
Registrar IANA ID: 1403
Registrar Abuse Contact Email: abuse@cdmon.com
Registrar Abuse Contact Phone: +34.935677577
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransfer
Prohibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: lima
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: PE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: http://www.whoiscontactsprotection.com/
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: http://www.whoiscontactsprotection.com/
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: http://www.whoiscontactsprotection.com/
Name Server: cp1.privatesystems.net
Name Server: cp2.privatesystems.net
Name Server: cp3.privatesystems.net
Name Server: cp4.privatesystems.net
DNSSEC: unsigned
```

```
soc@kali:~$ whois -h whois.hostinger.com OOWEBHOSTAPP.COM
Domain Name: OOWEBHOSTAPP.COM
Registry Domain ID: 2071431105_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2018-11-10T02:31:41Z
Creation Date: 2016-11-03T21:55:38Z
Registrar Registration Expiration Date: 2019-11-03T21:55:38Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8022274003
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact@privacyprotect.org
Registry Admin ID: Not Available From Registry
Admin Name: Domain Admin
Admin Organization: Privacy Protect, LLC (PrivacyProtect.org)
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8022274003
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact@privacyprotect.org
Registry Tech ID: Not Available From Registry
Tech Name: Domain Admin
Tech Organization: Privacy Protect, LLC (PrivacyProtect.org)
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8022274003
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact@privacyprotect.org
Name Server: ns1.mytrafficmanagement.com
Name Server: ns2.mytrafficmanagement.com
DNSSEC: Unsigned
```

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