

Alerta de seguridad informática	8FFR20-00270-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Marzo de 2020
Última revisión	18 de Marzo de 2020

## 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 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's

acceso[.]bacoestado[.]cloud  
 acceso[.]bacoestado[.]cloud/inicio

Domain acceso.bacoestado.cloud			
acceso / bacoestado / cloud / <a href="#">Subdomains</a>			
record type	TTL	value	
A	3600	159.65.77.246	

Domain bacoestado.cloud																	
bacoestado / cloud / <a href="#">Subdomains</a>																	
record type	TTL	value															
NS	172800	ns1.dnsowl.com	<a href="#">Zones on DNS server</a> 198.251.84.16, 104.207.141.138, 185.34.216.159														
NS	172800	ns2.dnsowl.com	<a href="#">Zones on DNS server</a> 168.235.75.52, 64.32.22.100, 45.32.237.128														
NS	172800	ns3.dnsowl.com	<a href="#">Zones on DNS server</a> 209.141.39.150, 45.63.106.63, 45.63.5.234														
SOA	172800	<table border="1"> <tr><td>Mname</td><td>ns1.dnsowl.com</td></tr> <tr><td>Rname</td><td>hostmaster.dnsowl.com</td></tr> <tr><td>Serial number</td><td>1584475580</td></tr> <tr><td>Refresh</td><td>7200</td></tr> <tr><td>Retry</td><td>1800</td></tr> <tr><td>Expire</td><td>1209600</td></tr> <tr><td>Minimum TTL</td><td>600</td></tr> </table>		Mname	ns1.dnsowl.com	Rname	hostmaster.dnsowl.com	Serial number	1584475580	Refresh	7200	Retry	1800	Expire	1209600	Minimum TTL	600
Mname	ns1.dnsowl.com																
Rname	hostmaster.dnsowl.com																
Serial number	1584475580																
Refresh	7200																
Retry	1800																
Expire	1209600																
Minimum TTL	600																

Ilustración 1 Dominio donde se Aloja Url del Banco Estado Falso y DNS que utiliza

## Certificados

<b>Subject DN</b>	CN=acceso.bacoestado.cloud
<b>Issuer DN</b>	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
<b>Serial</b>	313590105184286387352924070282868500319392
<b>Validity</b>	2020-03-17 10:11:44 to 2020-06-15 10:11:44 (90 days, 0:00:00)
<b>Names</b>	acceso.bacoestado.cloud

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP


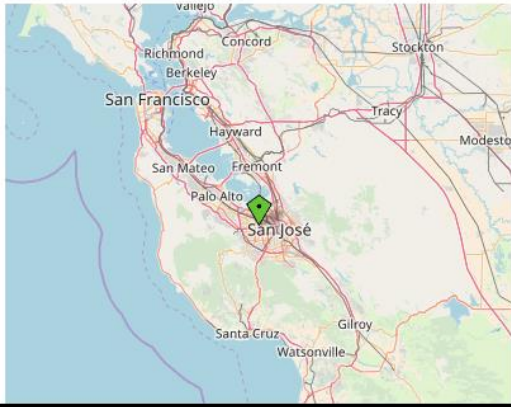
159[.]65[.].77[.]246

Domain <u>acceso.bacoestado.cloud</u> is located on IP address << 159.65.77.246 >>	
Block start	159.65.0.0
End of block	159.65.255.255
Block size	65536 <a href="#">Domains in block</a>
Block name	PHS-NET
AS number	<u>14061</u>
Parent block	<u>159.0.0.0 - 159.255.255.255</u>
Organization	<u>PresbyterianHealthcareSys.</u>

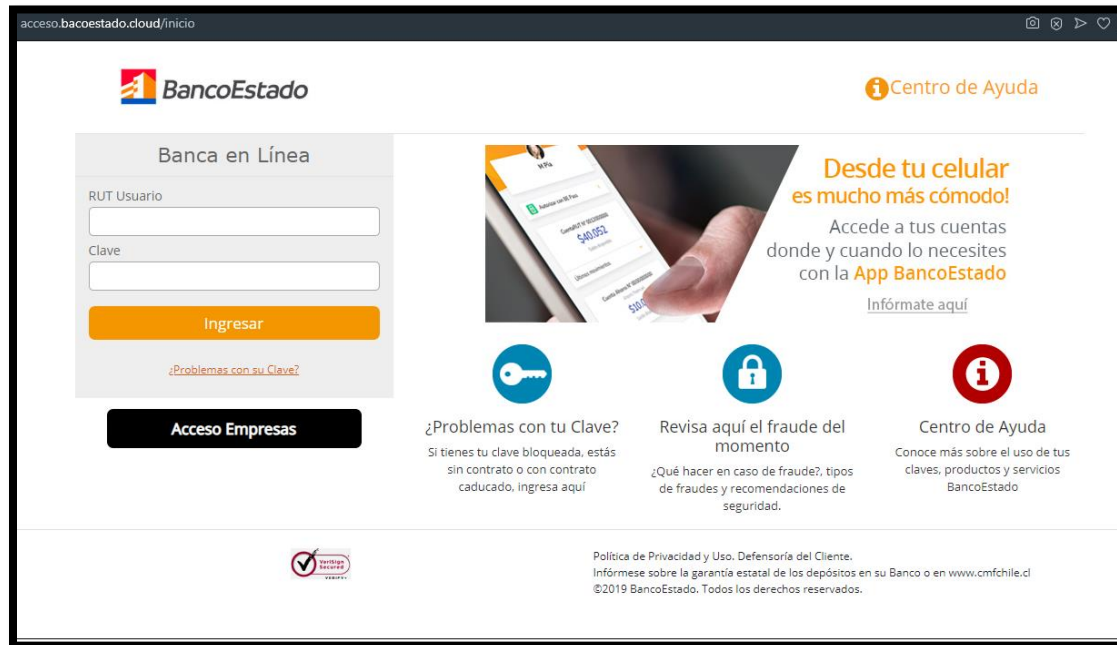
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

### Localización

Santa Clara, California, Estados Unidos

Location	Santa Clara, California, United States (US) 
Latitude and Longitude	37.34, -121.98
	

## Imagen del sitio



## Whois

```
Domain Name: bacoestado.cloud
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-17T07:00:00Z
Creation Date: 2020-03-17T07:00:00Z
Registrar Registration Expiration Date: 2021-03-17T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-5e274feel77a5bc303217cla0c02efff@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-5e274feel77a5bc303217cla0c02efff@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-5e274feel77a5bc303217cla0c02efff@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.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.