

Alerta de seguridad informática	8FFR20-00273-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Marzo de 2020
Última revisión	19 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 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 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 de **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

bacnestado[.]ddns[.]net

Domain bacnestado.ddns.net ⓘ			
<a href="#">bacnestado</a> / <a href="#">ddns</a> / <a href="#">net</a> / <a href="#">Subdomains</a>			
record type	TTL	value	
A	60	208.123.119.175	

Domain ddns.net ⓘ																	
<a href="#">ddns</a> / <a href="#">net</a> / <a href="#">Subdomains</a>																	
record type	TTL	value															
A	60	8.23.224.108															
NS	86400	<a href="#">nf1.no-ip.com</a>	<a href="#">Zones on DNS server</a> 194.62.182.53														
NS	86400	<a href="#">nf2.no-ip.com</a>	<a href="#">Zones on DNS server</a> 45.54.64.53														
NS	86400	<a href="#">nf3.no-ip.com</a>	<a href="#">Zones on DNS server</a> 204.16.253.53														
NS	86400	<a href="#">nf4.no-ip.com</a>	<a href="#">Zones on DNS server</a> 194.62.183.53														
NS	86400	<a href="#">nf5.no-ip.com</a>	<a href="#">Zones on DNS server</a> 204.16.253.53														
MX	1800	5 mail.ddns.net															
SOA	86400	<table border="1"> <tr><td>Mname</td><td>nf1.no-ip.com</td></tr> <tr><td>Rname</td><td>hostmaster.no-ip.com</td></tr> <tr><td>Serial number</td><td>2299643093</td></tr> <tr><td>Refresh</td><td>10800</td></tr> <tr><td>Retry</td><td>1800</td></tr> <tr><td>Expire</td><td>604800</td></tr> <tr><td>Minimum TTL</td><td>1800</td></tr> </table>		Mname	nf1.no-ip.com	Rname	hostmaster.no-ip.com	Serial number	2299643093	Refresh	10800	Retry	1800	Expire	604800	Minimum TTL	1800
Mname	nf1.no-ip.com																
Rname	hostmaster.no-ip.com																
Serial number	2299643093																
Refresh	10800																
Retry	1800																
Expire	604800																
Minimum TTL	1800																

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

## Certificados

Certificates	cert.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
	<a href="#">2597415313</a>	2020-03-18	2020-03-18	2020-06-16	bacnestado.ddns.net	C=US,O=Let's Encrypt,CN=Let's Encrypt Authority X3

Ilustración 1 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP  
208[.]123[.]119[.]175



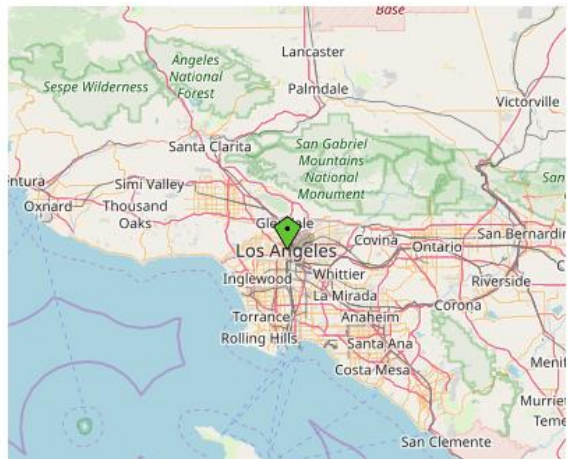
<b>Domain <u>bacnestado.ddns.net</u> is located on IP address &lt;&lt; 208.123.119.175 &gt;&gt;</b>	
<b>Block start</b>	208.123.119.0
<b>End of block</b>	208.123.119.255
<b>Block size</b>	256  <a href="#">Domains in block</a>
<b>Block name</b>	ATISTAR
<b>AS number</b>	<a href="#">395092</a>
<b>Parent block</b>	<a href="#">208.123.112.0 - 208.123.119.255</a>
<b>Organization</b>	<a href="#">ATISTAR INTERNET SERVICES LLC</a>

Ilustración 1 Ip de Origen donde se aloja Sitio Falso del Banco Estado

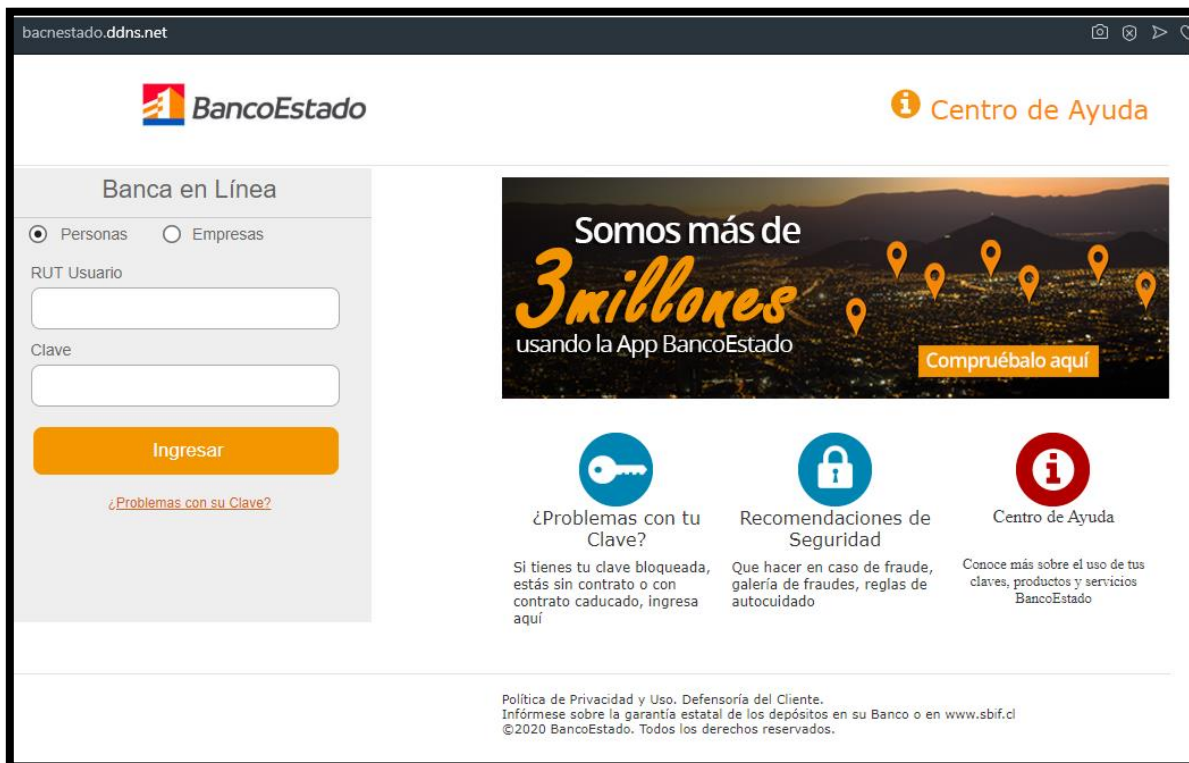
### Localización

Los Angeles, California, Estados Unidos

Location	Los Angeles, California, United States (US) 
Latitude and Longitude	34.05, -118.24



## Imagen del sitio



## Whois

```
Domain Name: ddns.net
Registry Domain ID: 73816572_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2020-02-07T16:50:29Z
Creation Date: 2001-06-28T16:04:59Z
Registrar Registration Expiration Date: 2022-06-28T16:04:59Z
Registrar: TLDS LLC, d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.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.