Alerta de seguridad informática	8FFR20-00285-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 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 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 dos portales fraudulentos asociados a dos IPs que suplantan 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 COMPROMISO

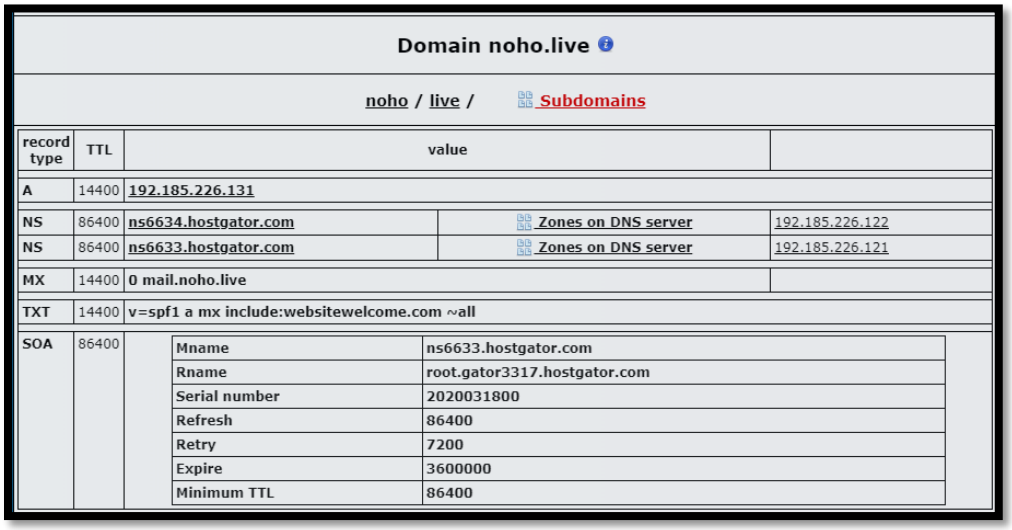
URL

noho[.]live/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html
acceso[.]bacoestado[.]life
acceso[.]bacoestado[.]life/inicio

IP

192[.]185[.]226[.]131
142[.]93[.]213[.]241

DOMINIOS DONDE SE ALOJA URL



Domain noho.live

noho / live / Subdomains

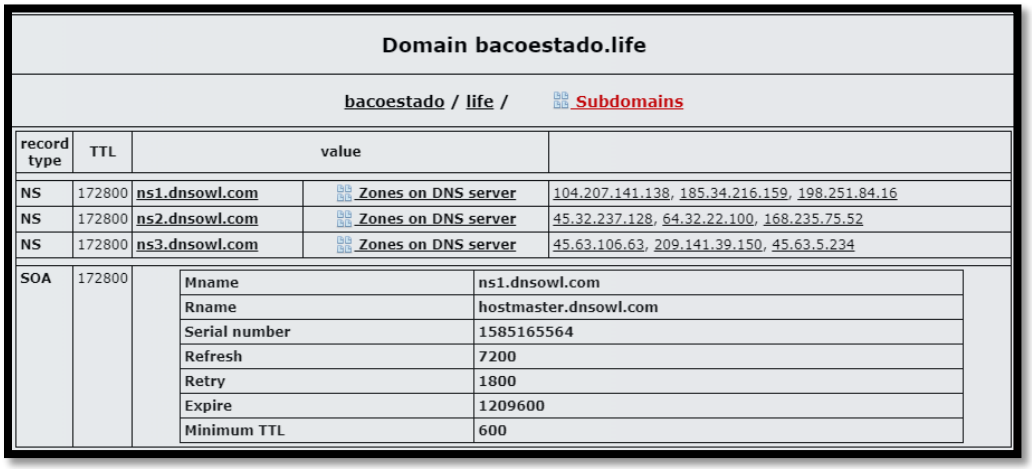
record type	TTL	value		
A	14400	192.185.226.131		
NS	86400	ns6634.hostgator.com	Zones on DNS server	192.185.226.122
NS	86400	ns6633.hostgator.com	Zones on DNS server	192.185.226.121
MX	14400	0 mail.noho.live		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		

SOA	86400	Mname	ns6633.hostgator.com
		Rname	root.gator3317.hostgator.com
		Serial number	2020031800
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

Domain acceso.bacoestado.life

acceso / bacoestado / life / Subdomains

record type	TTL	value	
A	3600	142.93.213.241	



Domain bacoestado.life

bacoestado / life / Subdomains

record type	TTL	value		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 185.34.216.159, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 64.32.22.100, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1585165564
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2598483229	2020-03-19	2020-03-18	2020-06-16	autodiscover.noho.live cpanel.noho.live mail.noho.live noho.live webdisk.noho.live webmail.noho.live www.noho.live	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2606207505	2020-03-21	2020-03-20	2020-06-18	acceso.bacoestado.life	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2606207453	2020-03-21	2020-03-20	2020-06-18	acceso.bacoestado.life	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain noho.live is located on IP address << 192.185.226.131 >>

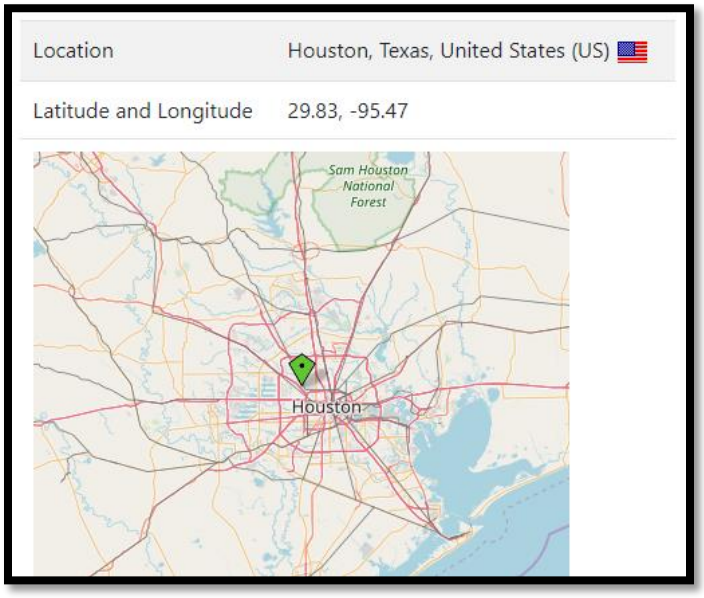
Block start	192.185.0.0
End of block	192.185.255.255
Block size	65536 Domains in block
Block name	HGBLOCK-10
AS number	46606
Parent block	192.0.0.0 - 192.255.255.255
Organization	WEBSITEWELCOME.COM

Domain acceso.bacoestado.life is located on IP address << 142.93.213.241 >>

Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.

LOCALIZACIÓN

Houston, Texas, Estados Unidos



New York City, New York, Estados Unidos

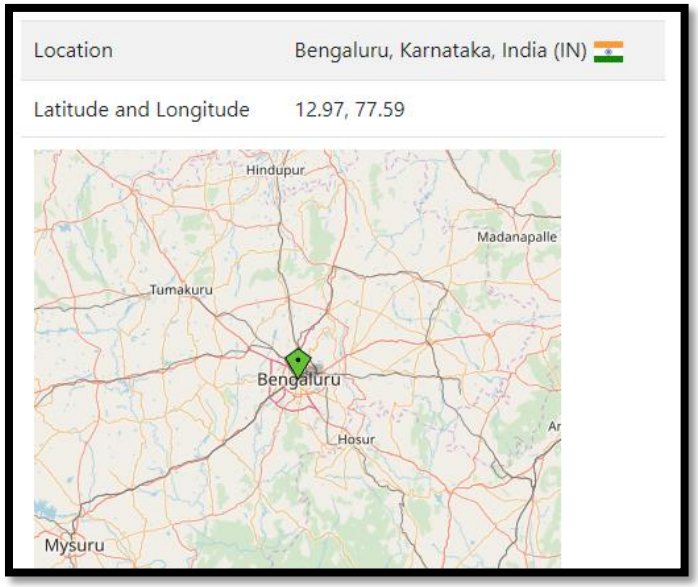
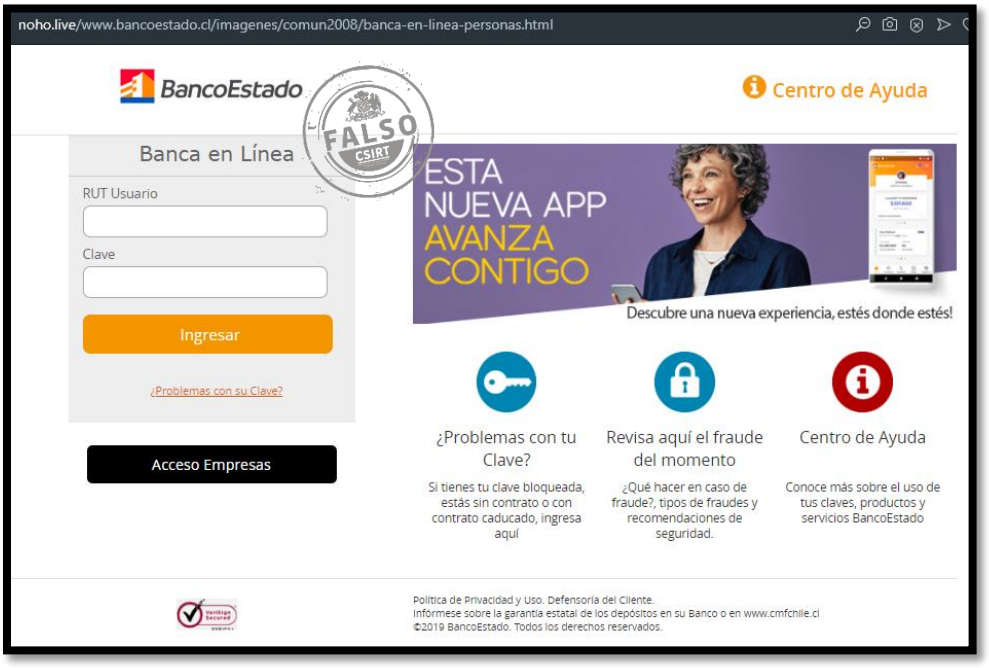
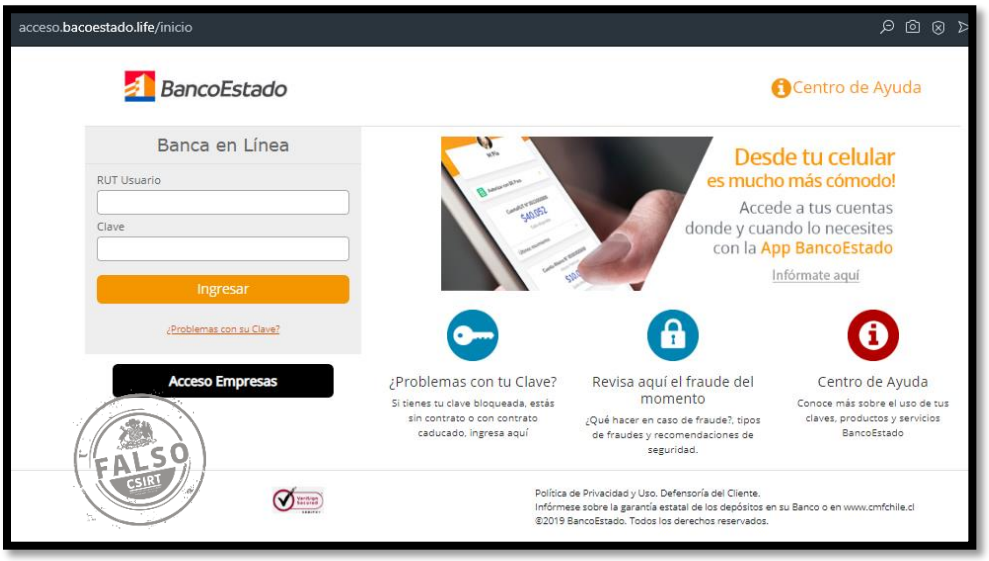


IMAGEN DEL SITIO





WHOIS

```
Domain Name: NOHO.LIVE
Registry Domain ID: 72178513d4e94f6c92bfd57a09204bdc-DONUTS
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2019-07-14T19:02:19Z
Creation Date: 2016-05-30T19:02:19Z
Registrar Registration Expiration Date: 2020-05-30T19:02:19Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/noho.live
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/noho.live
Registry Tech ID: Not Available From Registry
Tech Name: Whois Agent
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/noho.live
Name Server: ns6633.hostgator.com
Name Server: ns6634.hostgator.com
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.7203101849
```

```
Domain Name: bacoestado.life
Registry Domain ID: 3f5e6124213c4c3b9da825c951e5675a-DONUTS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-21T07:00:00Z
Creation Date: 2020-03-20T07:00:00Z
Registrar Registration Expiration Date: 2021-03-20T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
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-20f6c80909b136e12c1f4cc6ff62014c@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-20f6c80909b136e12c1f4cc6ff62014c@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-20f6c80909b136e12c1f4cc6ff62014c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

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: 2020.03.26 09:49:11 -03'00'