Alerta de seguridad informática	8FFR20-00264-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 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.

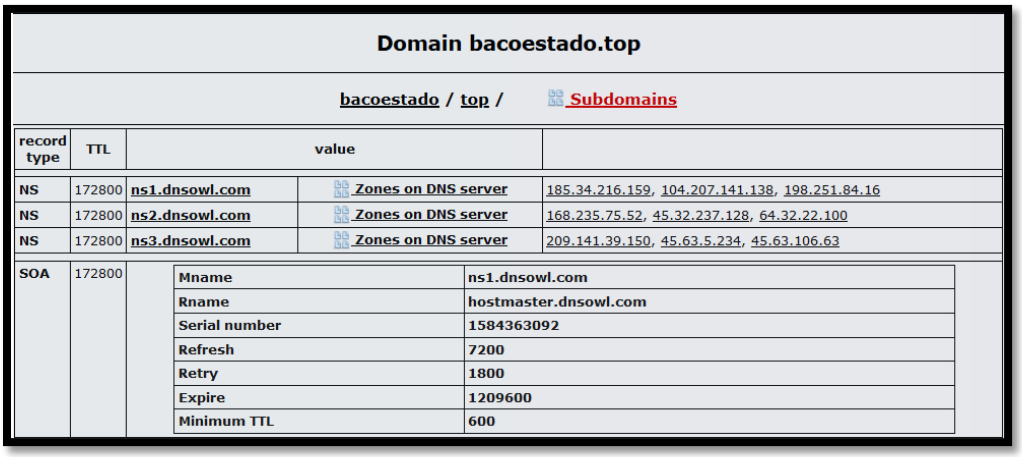
Indicadores de Compromisos

URL´s

acceso[.]bacoestado[.]top

acceso[.]bacoestado[.]club

bencoestadooenlinea[.]hdkhdcf[.]com

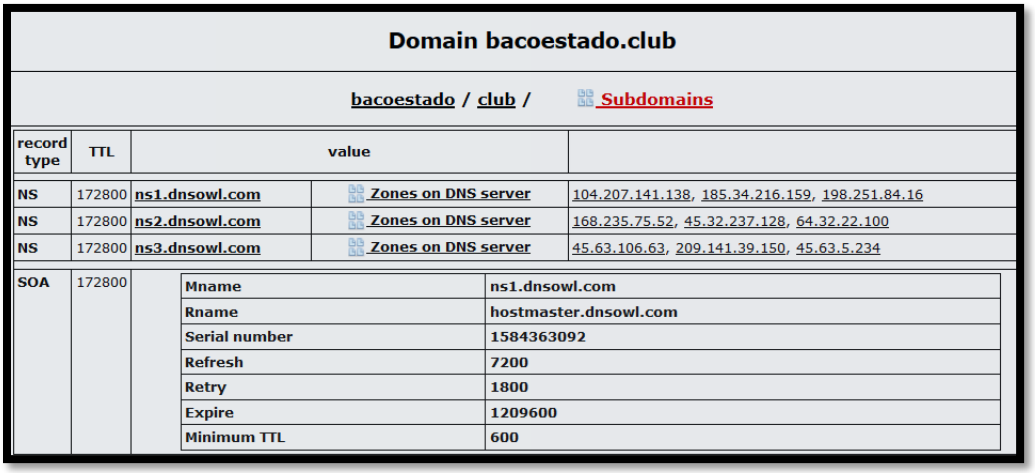


Domain bacoestado.top

bacoestado / top / Subdomains

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

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584363092
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

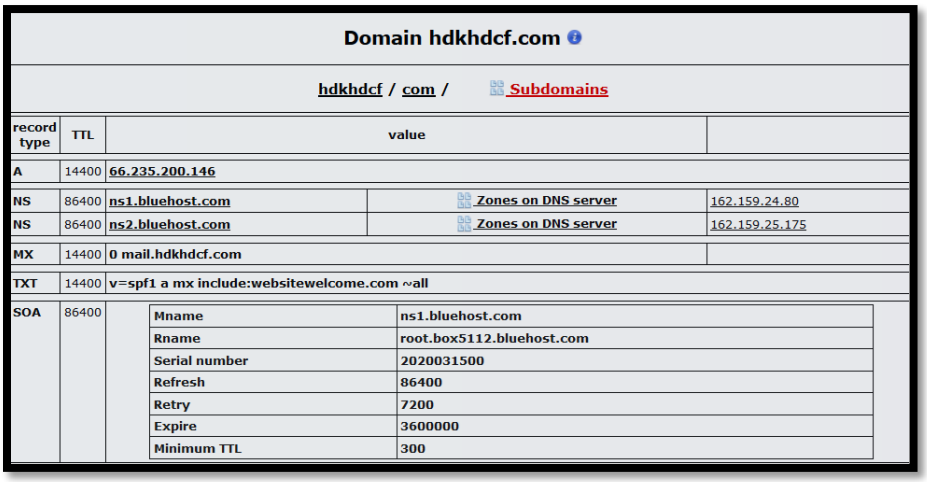


Domain bacoestado.club

bacoestado / club / 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	168.235.75.52, 45.32.237.128, 64.32.22.100
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	1584363092
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



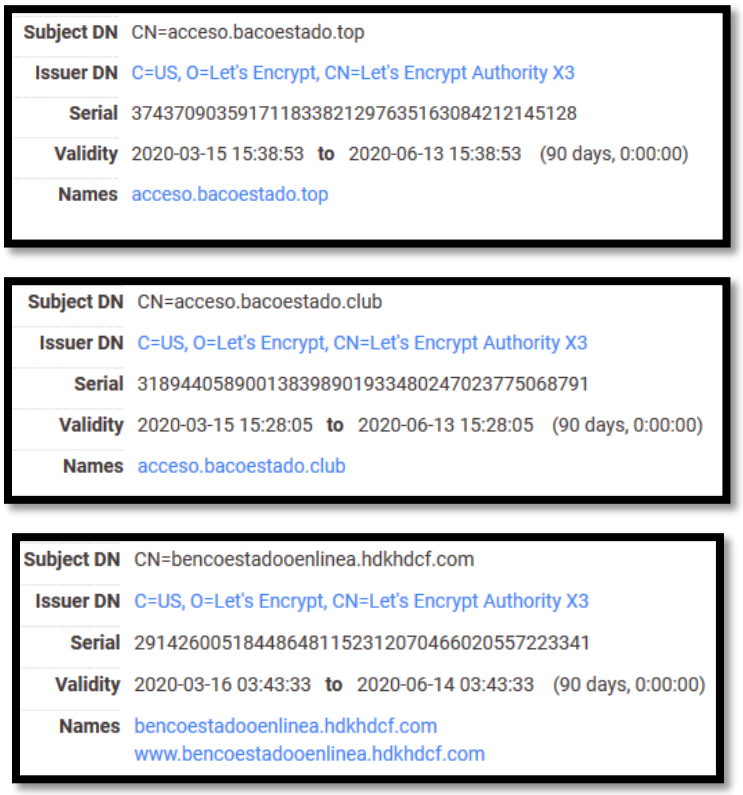
Domain hdkhdcf.com

hdkhdcf / com / Subdomains

record type	TTL	value		
A	14400	66.235.200.146		
NS	86400	ns1.bluehost.com	Zones on DNS server	162.159.24.80
NS	86400	ns2.bluehost.com	Zones on DNS server	162.159.25.175
MX	14400	0 mail.hdkhdcf.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname	ns1.bluehost.com	
		Rname	root.box5112.bluehost.com	
		Serial number	2020031500	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	300	

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

Certificados



Subject DN CN=acceso.bacoestado.top
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 374370903591711833821297635163084212145128
Validity 2020-03-15 15:38:53 **to** 2020-06-13 15:38:53 (90 days, 0:00:00)
Names acceso.bacoestado.top

Subject DN CN=acceso.bacoestado.club
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 318944058900138398901933480247023775068791
Validity 2020-03-15 15:28:05 **to** 2020-06-13 15:28:05 (90 days, 0:00:00)
Names acceso.bacoestado.club

Subject DN CN=bencoestadooenlinea.hdkhdcf.com
Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial 291426005184486481152312070466020557223341
Validity 2020-03-16 03:43:33 **to** 2020-06-14 03:43:33 (90 days, 0:00:00)
Names bencoestadooenlinea.hdkhdcf.com
www.bencoestadooenlinea.hdkhdcf.com

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

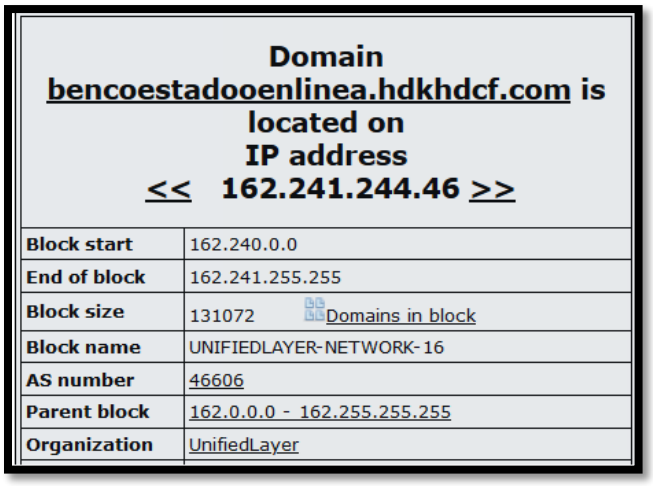
IP
208[.]123[.]119[.]175
159[.]89[.]123[.]83
162[.]241[.]244[.]46

Domain acceso.bacoestado.top is located on IP address << 46.101.240.41 >>

Block start	46.101.128.0
End of block	46.101.255.255
Block size	32768 Domains in block
Block name	EU-DIGITALOCEAN-DE1
AS number	14061
Parent block	46.101.0.0 - 46.101.255.255
Organization	Digital Ocean, Inc.

Domain acceso.bacoestado.club is located on IP address << 159.89.123.83 >>

Block start	159.89.0.0
End of block	159.89.255.255
Block size	65536 Domains in block
Block name	FCCL
AS number	14061
Parent block	159.0.0.0 - 159.255.255.255
Organization	FletcherChallengeCanadaLimited

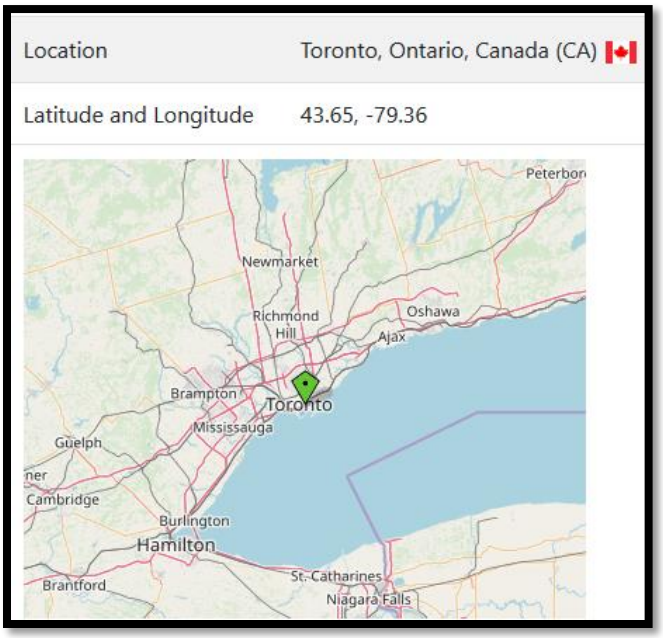


Domain bencoestadooenlinea.hdkhdcf.com is located on IP address << 162.241.244.46 >>

Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer

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

Localización
Frankfurt am Main, Hessen, Alemania
Toronto, Ontario, Canada
Provo, Utah, Estados Unidos


Location
Toronto, Ontario, Canada (CA)
Latitude and Longitude
43.65, -79.36
Peterbor
Newmarket
Richmond Hill
Oshawa
Ajax
Brampton
Toronto
Mississauga
Guelph
Cambridge
Burlington
Hamilton
Brantford
St. Catharines
Niagara Falls

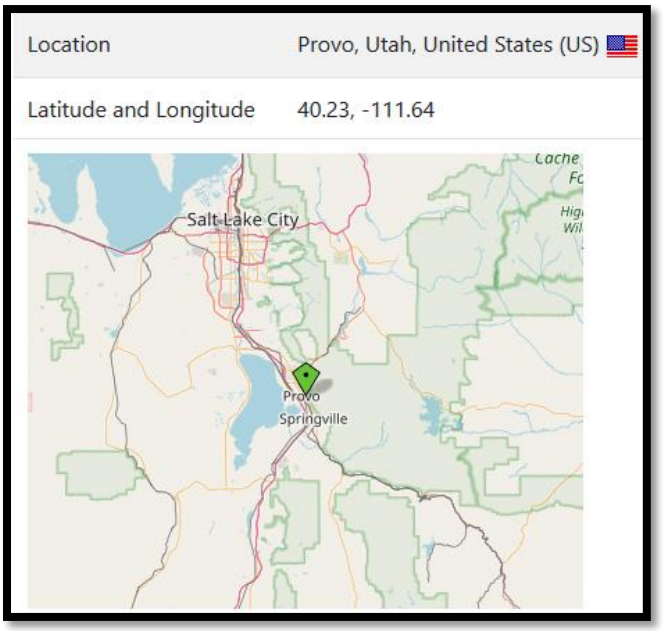
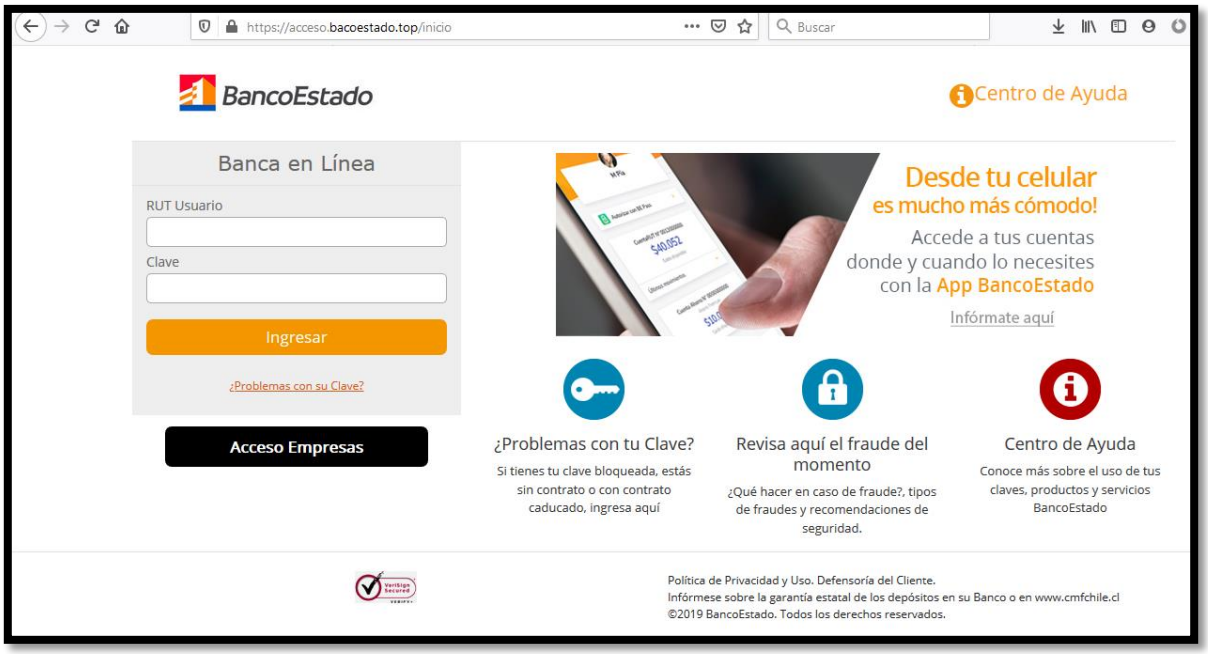
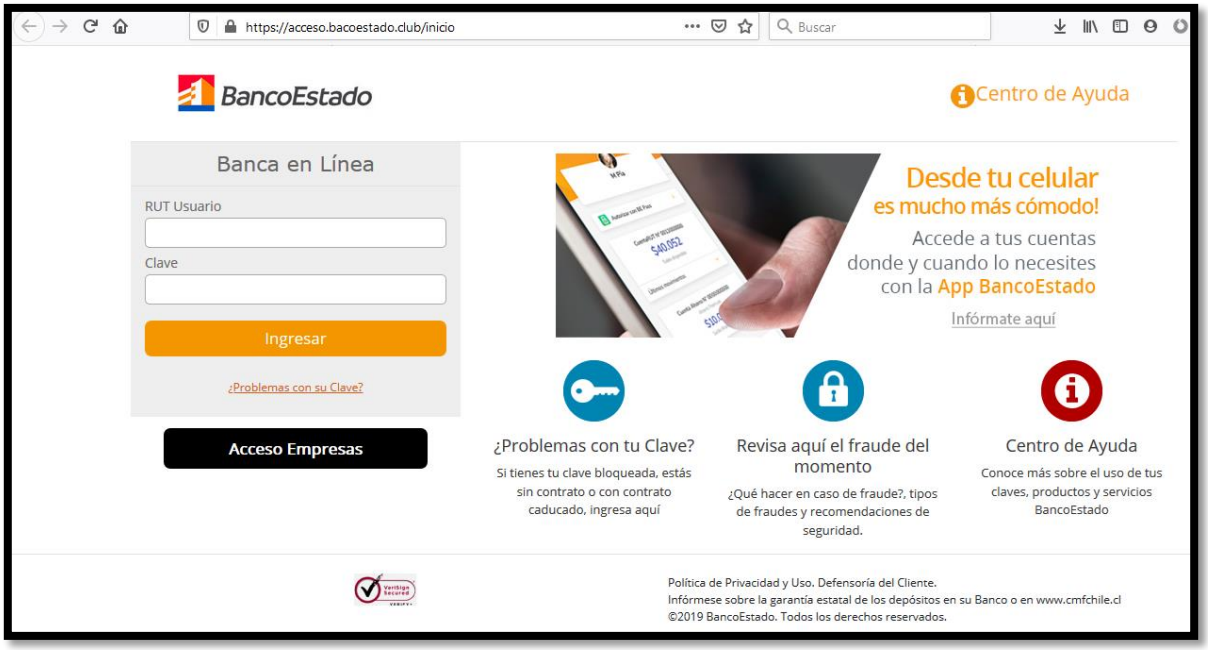
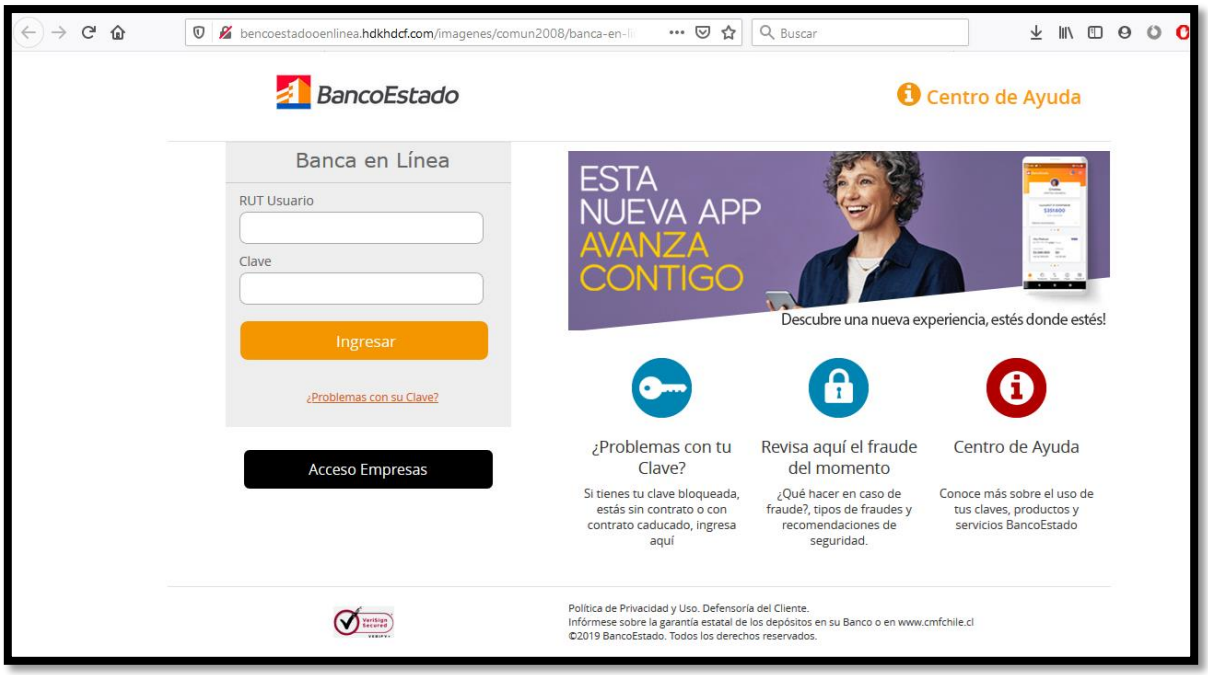

Location
Provo, Utah, United States (US)
Latitude and Longitude
40.23, -111.64
Salt Lake City
Provo
Springville

Imagen del sitio






bencoestadooenlinea.hdkhdcf.com/imagenes/comun2008/banca-en-l
Buscar
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés donde estés!
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: bacoestado.top
Registry Domain ID: D20200315G10001G_35645039-top
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-03-15T10:31:15Z
Creation Date: 2020-03-15T10:17:23Z
Registry Expiry Date: 2021-03-15T10:17:23Z
Registrar: NameSilo
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID: C20200315C_53330673-top
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country:
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
Registry Admin ID: C20200315C_53330673-top
Admin Name:
Admin Organization:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:
Registry Tech ID: C20200315C_53330673-top
Tech Name:
Tech Organization:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:
Name Server: ns1.dnsowl.com
Name Server: ns2.dnsowl.com
Name Server: ns3.dnsowl.com
DNSSEC: unsigned
```

```
Domain Name: bacoestado.club
Registry Domain ID: D3CBC9F07BA2B4179A530C227BBA53F26-NSR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-15T07:00:00Z
Creation Date: 2020-03-15T07:00:00Z
Registrar Registration Expiration Date: 2021-03-15T07:00:00Z
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-1ffd3185bcff298372e014ecb9f64b5c@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-1ffd3185bcff298372e014ecb9f64b5c@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-1ffd3185bcff298372e014ecb9f64b5c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: HDKHDCF.COM
Registry Domain ID: 2497918255_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.bluehost.com
Registrar URL: http://www.bluehost.com/
Updated Date: 2020-02-28T17:25:18Z
Creation Date: 2020-02-28T17:25:17Z
Registrar Registration Expiration Date: 2021-02-28T17:25:17Z
Registrar: FastDomain Inc.
Registrar IANA ID: 1154
Registrar Abuse Contact Email: support@bluehost.com
Registrar Abuse Contact Phone: +1.8017659400
Reseller: BlueHost.Com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Registrant Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Registrant Street: 10 CORPORATE DR, STE 300
Registrant City: BURLINGTON
Registrant State/Province: MASSACHUSETTS
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8017659400
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: WHOIS@BLUEHOST.COM
Registry Admin ID:
Admin Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Admin Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Admin Street: 10 CORPORATE DR, STE 300
Admin City: BURLINGTON
Admin State/Province: MASSACHUSETTS
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8017659400
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: WHOIS@BLUEHOST.COM
Registry Tech ID:
Tech Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Tech Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Tech Street: 10 CORPORATE DR, STE 300
Tech City: BURLINGTON
Tech State/Province: MASSACHUSETTS
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8017659400
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: WHOIS@BLUEHOST.COM
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.17 07:00:15 -03'00'