Alerta de seguridad informática	8FFR20-00283-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Marzo de 2020
Última revisión	24 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 tres portales fraudulentos asociados a tres 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´s

acceso[.]bacoestado[.]icu
wwc[.]acceso[.]enstado[.]chile[.]stdo[.]live
www[.]creditoefectivo-bancaestada[.]xyz

IP

142[.]93[.]232[.]49
165[.]22[.]215[.]57
165[.]22[.]223[.]59

DOMINIOS DONDE SE ALOJA URL

Domain bacoestado.icu

bacoestado / icu / Subdomains

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

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584964300
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain stdo.live

stdo / live / Subdomains

record type	TTL	value		
A	7207	165.22.215.57		
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	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1584975992
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain creditoefectivo-bancaestada.xyz

creditoefectivo-bancaestada / xyz / Subdomains

record type	TTL	value		
A	7207	165.22.223.59		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 104.207.141.138, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
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	1584979592
Refresh	7200
Retry	1800
Expire	1209600
Minimum TTL	600

CERTIFICADOS

Subject DN	CN=acceso.bacoestado.icu
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	298900187453845832314299333396842578884442
Validity	2020-03-20 23:34:10 **to** 2020-06-18 23:34:10 (90 days, 0:00:00)
Names	acceso.bacoestado.icu

Subject DN	CN=wwc.acceso.enstado.chile.stdo.live
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	333607496845821738995428512678929336552788
Validity	2020-03-22 17:14:08 **to** 2020-06-20 17:14:08 (90 days, 0:00:00)
Names	wwc.acceso.enstado.chile.stdo.live

Subject DN	CN=www.creditoefectivo-bancaestada.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	379193833868121969826755409255062160906573
Validity	2020-03-22 07:03:00 **to** 2020-06-20 07:03:00 (90 days, 0:00:00)
Names	www.creditoefectivo-bancaestada.xyz

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain acceso.bacoestado.icu is located on IP address << 142.93.232.49 >>

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.

Domain wwc.acceso.enstado.chile.stdo.live is located on IP address << 165.22.215.57 >>

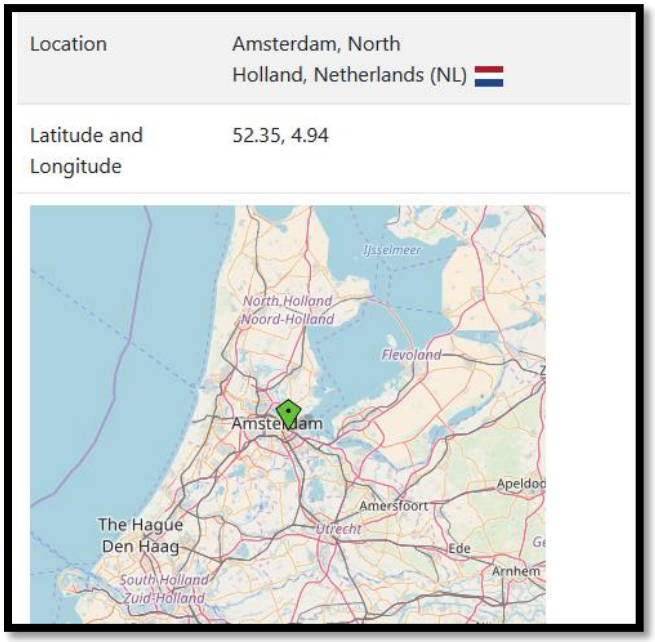
Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices

Domain creditoefectivo-bancaestada.xyz is located on IP address << 165.22.223.59 >>

Block start	165.22.0.0
End of block	165.22.255.255
Block size	65536 Domains in block
Block name	CELTECH1
AS number	14061
Parent block	165.0.0.0 - 165.255.255.255
Organization	CellularTechnicalServices

LOCALIZACIÓN

Amsterdam, North Holland, Holanda
Bengaluru, Karnataka, India



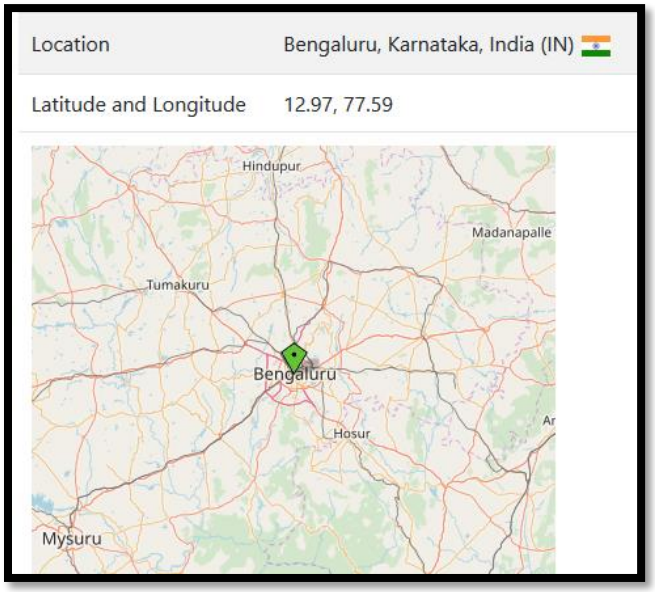
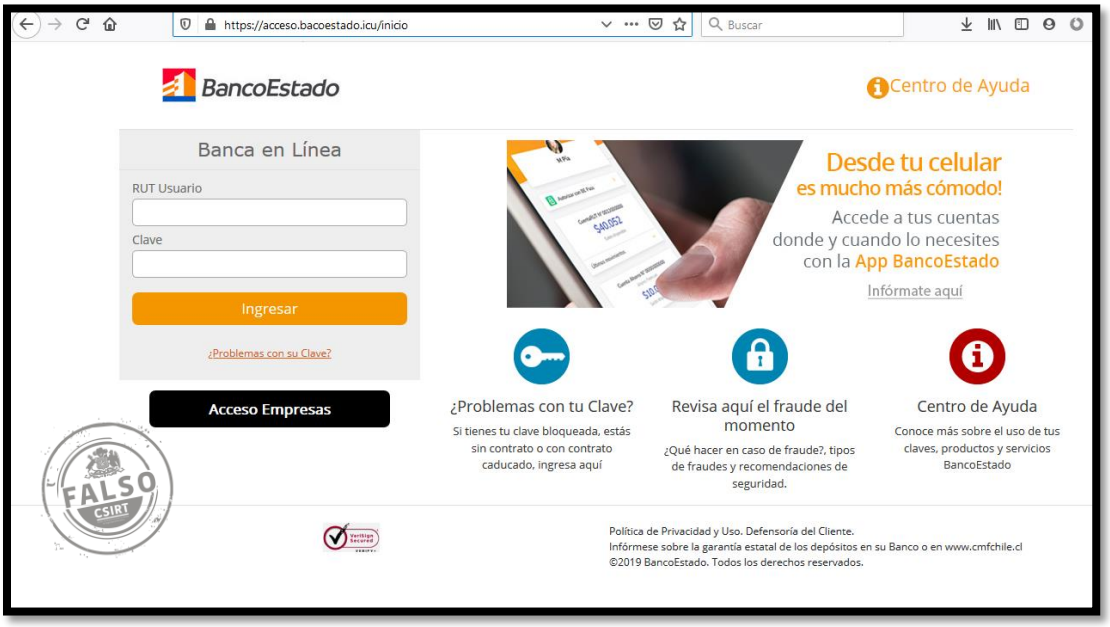
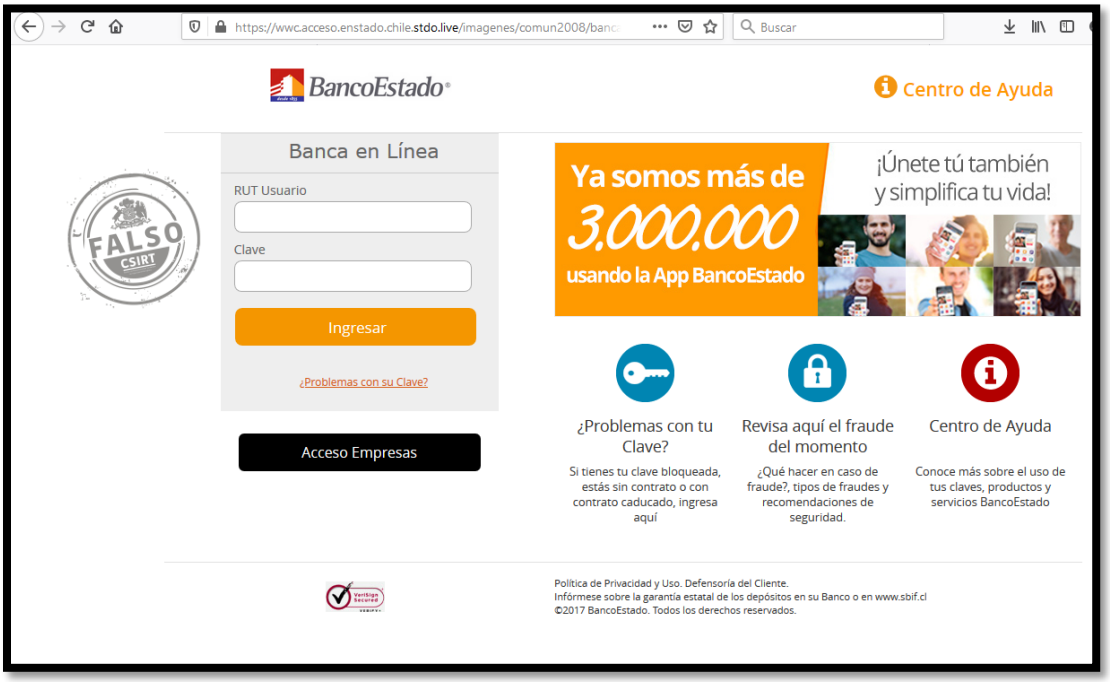
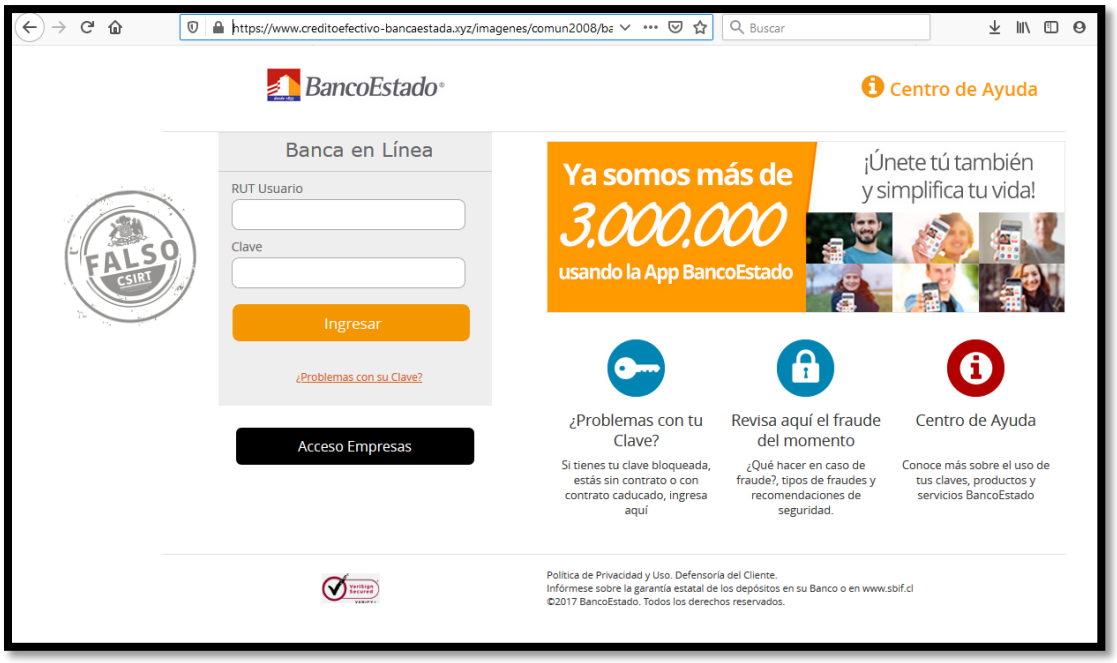


IMAGEN DEL SITIO






https://www.creditoefectivo-bancaestada.xyz/imagenes/comun2008/ba
Buscar
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
FALSO
CSIRT
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿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.sbif.cl
©2017 BancoEstado. Todos los derechos reservados.

WHOIS

```
Domain Name: bacoestado.icu
Registry Domain ID: D179592534-CNIC
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-5be2dcb41779ed7ac6bb120a5836607f@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-5be2dcb41779ed7ac6bb120a5836607f@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
```

```
Domain Name: stdo.live
Registry Domain ID: b936c5f0bd41458fb4efc2f91e24cf9a-DONUTS
Registrar WHOIS Server: www.namesilo.com/whois.php
Registrar URL: http://www.namesilo.com
Updated Date: 2020-03-22T17:30:58Z
Creation Date: 2020-03-22T17:15:59Z
Registry Expiry Date: 2021-03-22T17:15:59Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.6024928198
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: See PrivacyGuardian.org
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: AZ
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record ident
ified in this output for information on how to contact the Registrant, Admin, or
 Tech contact of the queried domain name.
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
```

```
Domain Name: CREDITOEFECTIVO-BANCAESTADA.XYZ
Registry Domain ID: D179690814-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2020-03-22T07:45:27.0Z
Creation Date: 2020-03-22T07:34:20.0Z
Registry Expiry Date: 2021-03-22T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferPro
ibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPro
ibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record iden
ified in this output for information on how to contact the Registrant, Admin, o
 Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identifie
 in this output for information on how to contact the Registrant, Admin, or Tec
 contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified
in this output for information on how to contact the Registrant, Admin, or Tech
contact of the queried domain name.
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identif
ed in this output for information on how to contact the Registrant, Admin, or T
ch contact of the queried domain name.
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-03-23T16:18:59.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<
```

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: 2020.03.24 14:10:12 -03'00'