Alerta de seguridad informática	8FFR20-00185-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Enero de 2020
Última revisión	17 de Enero 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 seis portales fraudulentos asociados a cuatro 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 Compromisos

URL´s

URL Sitio Clonado:

bancoestado[.]cl[.]personas[.]pasteleriatiarosa[.]com/costal/cl/Portal/

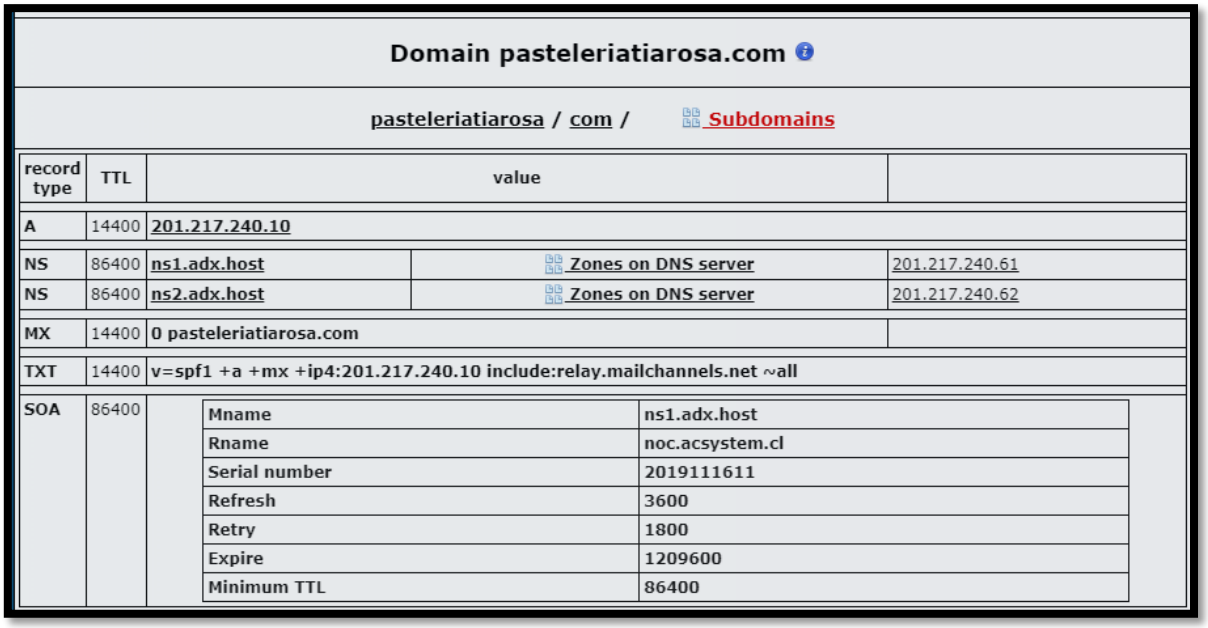
bancoestado[.]cl[.]personas[.]pasteleriatiarosa[.]com/costal/cl/Portal/?STP=login

tuswebstad[.]com

www1[.]banestado[.]cl[.]lad0[.]info

www1[.]banestado[.]cl[.]lad0[.]info/imagenes/comun2009/en-linea-personas[.]php

tustadoowe[.]com

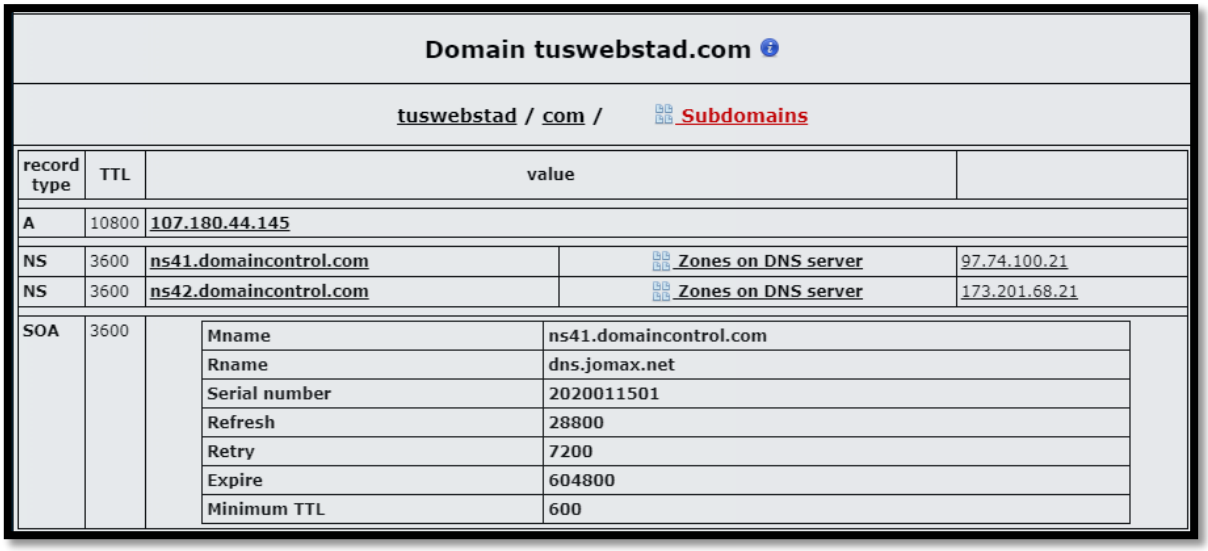


Domain pasteleriatiarosa.com

pasteleriatiarosa / com / Subdomains

record type	TTL	value		
A	14400	201.217.240.10		
NS	86400	ns1.adx.host	Zones on DNS server	201.217.240.61
NS	86400	ns2.adx.host	Zones on DNS server	201.217.240.62
MX	14400	0 pasteleriatiarosa.com		
TXT	14400	v=spf1 +a +mx +ip4:201.217.240.10 include:relay.mailchannels.net ~all		

SOA	86400	Mname	ns1.adx.host
		Rname	noc.acsystem.cl
		Serial number	2019111611
		Refresh	3600
		Retry	1800
		Expire	1209600
		Minimum TTL	86400

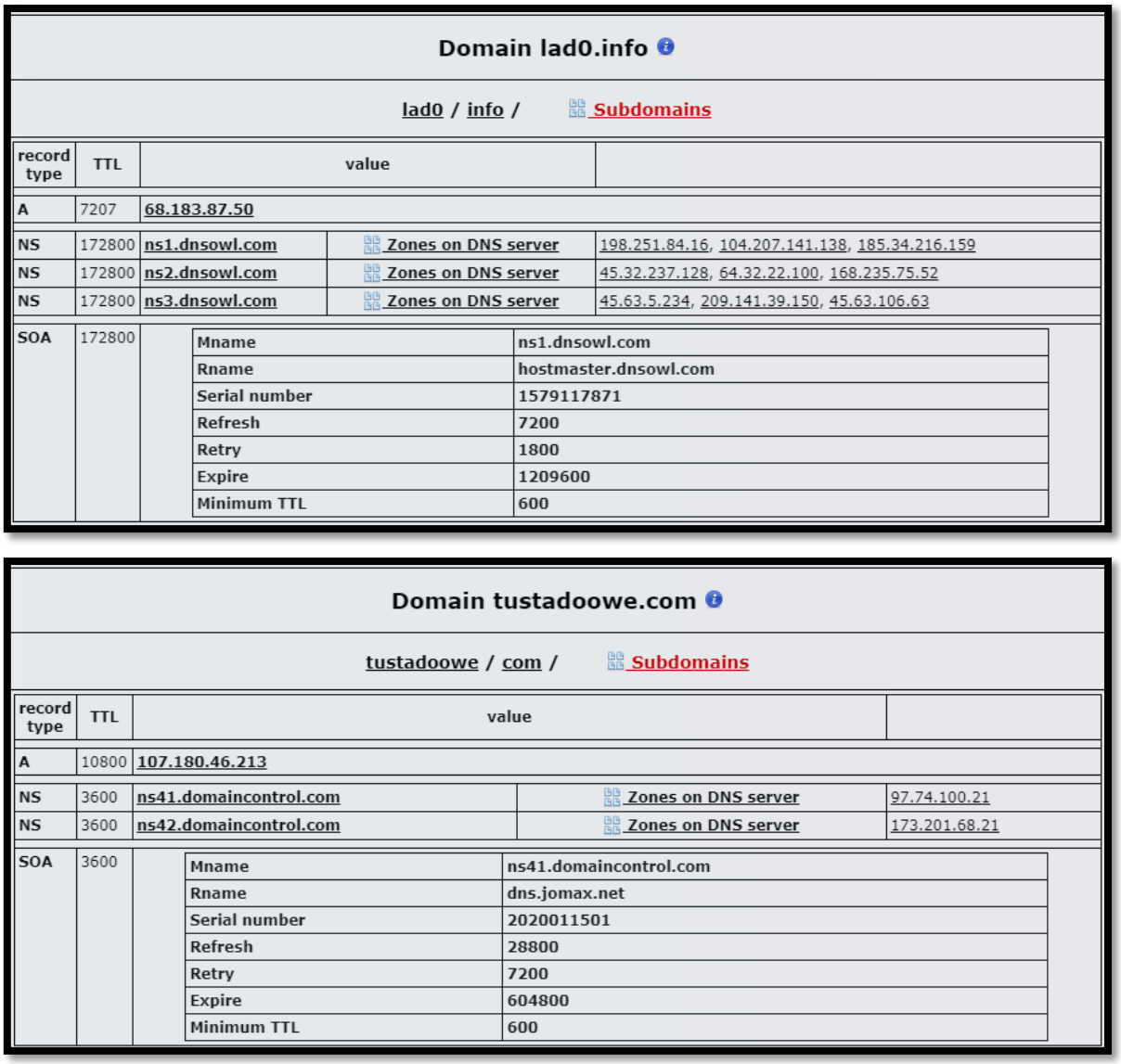


Domain tuswebstad.com

tuswebstad / com / Subdomains

record type	TTL	value		
A	10800	107.180.44.145		
NS	3600	ns41.domaincontrol.com	Zones on DNS server	97.74.100.21
NS	3600	ns42.domaincontrol.com	Zones on DNS server	173.201.68.21

SOA	3600	Mname	ns41.domaincontrol.com
		Rname	dns.jomax.net
		Serial number	2020011501
		Refresh	28800
		Retry	7200
		Expire	604800
		Minimum TTL	600



Domain lad0.info

lad0 / info / Subdomains

record type	TTL	value		
A	7207	68.183.87.50		
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	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	1579117871	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain tustadoowe.com

tustadoowe / com / Subdomains

record type	TTL	value		
A	10800	107.180.46.213		
NS	3600	ns41.domaincontrol.com	Zones on DNS server	97.74.100.21
NS	3600	ns42.domaincontrol.com	Zones on DNS server	173.201.68.21
SOA	3600	Mname	ns41.domaincontrol.com	
		Rname	dns.jomax.net	
		Serial number	2020011501	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	600	

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

Certificados

Subject DN	CN=bancoestado.cl.personas.pasteleriatiarosa.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	322906719107200960077553153718892470646868
Validity	2019-11-16 15:37:25 **to** 2020-02-14 15:37:25 (90 days, 0:00:00)
Names	bancoestado.cl.personas.pasteleriatiarosa.com www.bancoestado.cl.personas.pasteleriatiarosa.com

Subject DN	CN=www1.banestado.cl.lad0.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	275579245354860741855834063607304174663267
Validity	2020-01-15 18:31:15 **to** 2020-04-14 18:31:15 (90 days, 0:00:00)
Names	www1.banestado.cl.lad0.info

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

IP
201.217.240.10
107.180.44.145
68.183.87.50
107.180.46.213

Domain bancoestado.cl.personas.pasteleriatiarosa.com is located on IP address << 201.217.240.10 >>

Block start	201.217.240.0
End of block	201.217.243.255
Block size	1024 Domains in block
Block name	
AS number	263237
Parent block	201.0.0.0 - 201.255.255.255
Organization	POWER HOST E.I.R.L.
City	Santiago
Region/State	Region Metropolitana de Santiago
Country	CL , Chile
Reg. date	2014-05-22
Host name	ast24010scl-static.adx.cl

Domain tuswebstad.com is located on IP address << 107.180.44.145 >>

Block start	107.180.0.0
End of block	107.180.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	107.0.0.0 - 107.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2014-02-11
Host name	ip-107-180-44-145.ip.secureserver.net
Web server	Apache/2.4.23

Domain www1.banestado.cl.lad0.info is located on IP address << 68.183.87.50 >>

Block start	68.183.0.0
End of block	68.183.255.255
Block size	65536 Domains in block
Block name	DSLEXTREME-NWK-6
AS number	14061
Parent block	68.0.0.0 - 68.255.255.255
Organization	DSL Extreme
City	Chatsworth
Region/State	California
Country	US , United States
Reg. date	2005-04-14
Host name	estaldo.info
Domains	1 www1.banestado.cl.lad0.info

Domain tustadoowe.com is located on IP address << 107.180.46.213 >>

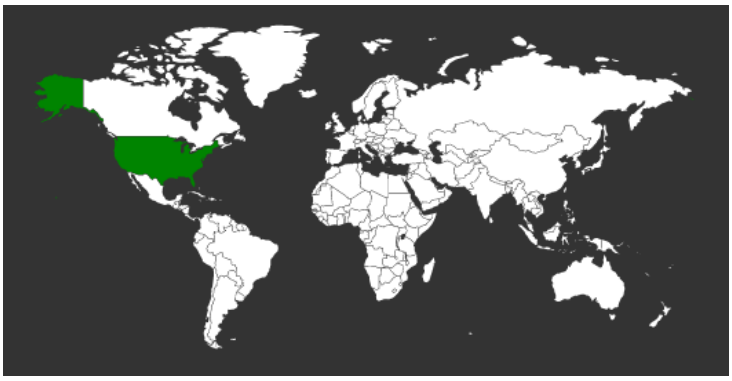
Block start	107.180.0.0
End of block	107.180.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	107.0.0.0 - 107.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2014-02-11
Host name	ip-107-180-46-213.ip.secureserver.net
Web server	Apache/2.4.23

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

Localización

Santiago, Región Metropolitana, Chile

Scotdale, Arizona, Estados Unidos



Bangalore, Karnataka, India

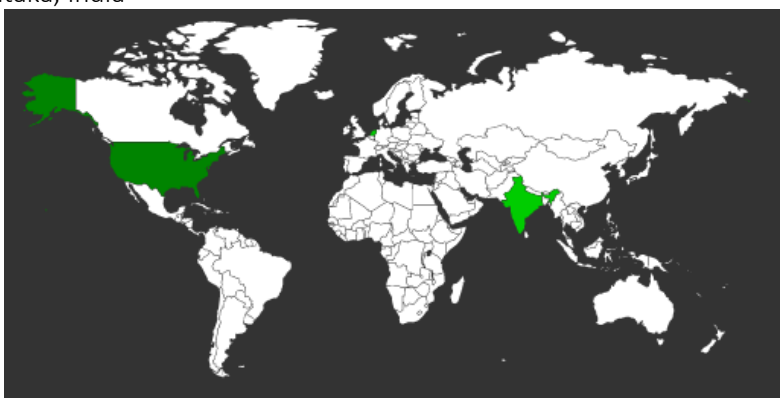
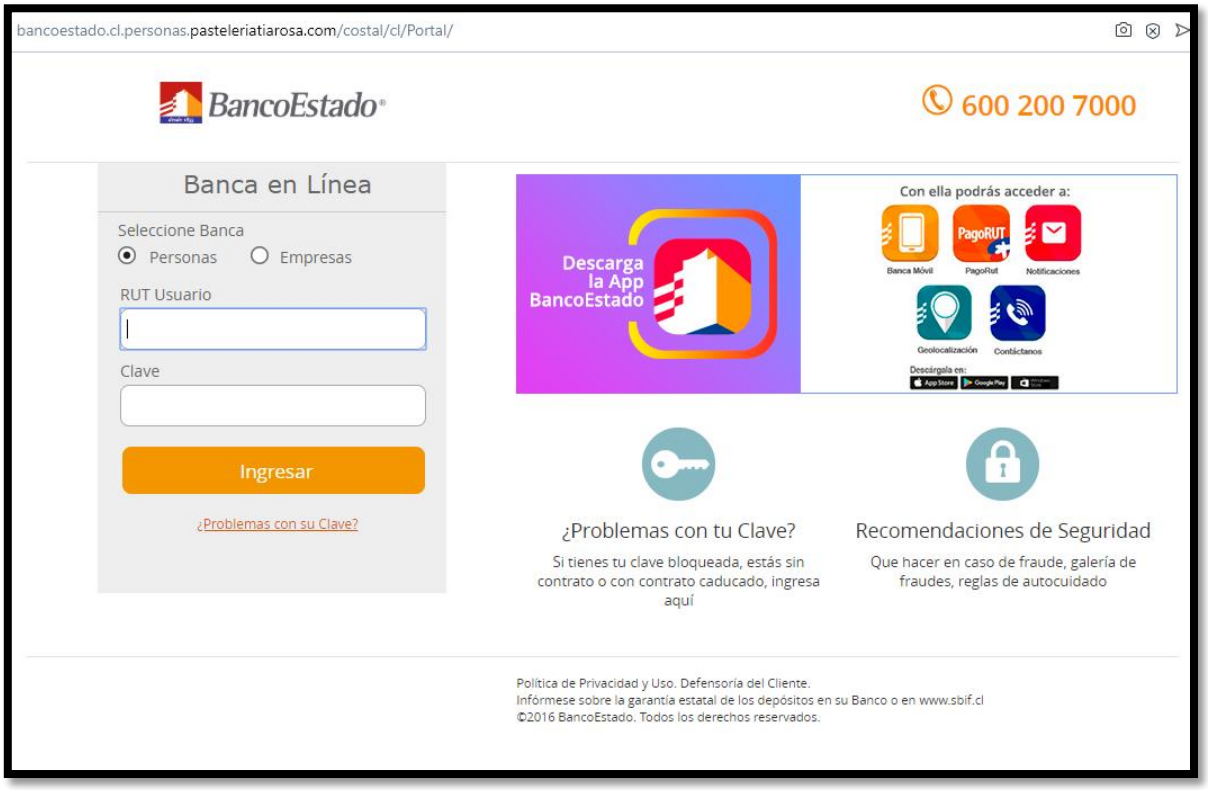
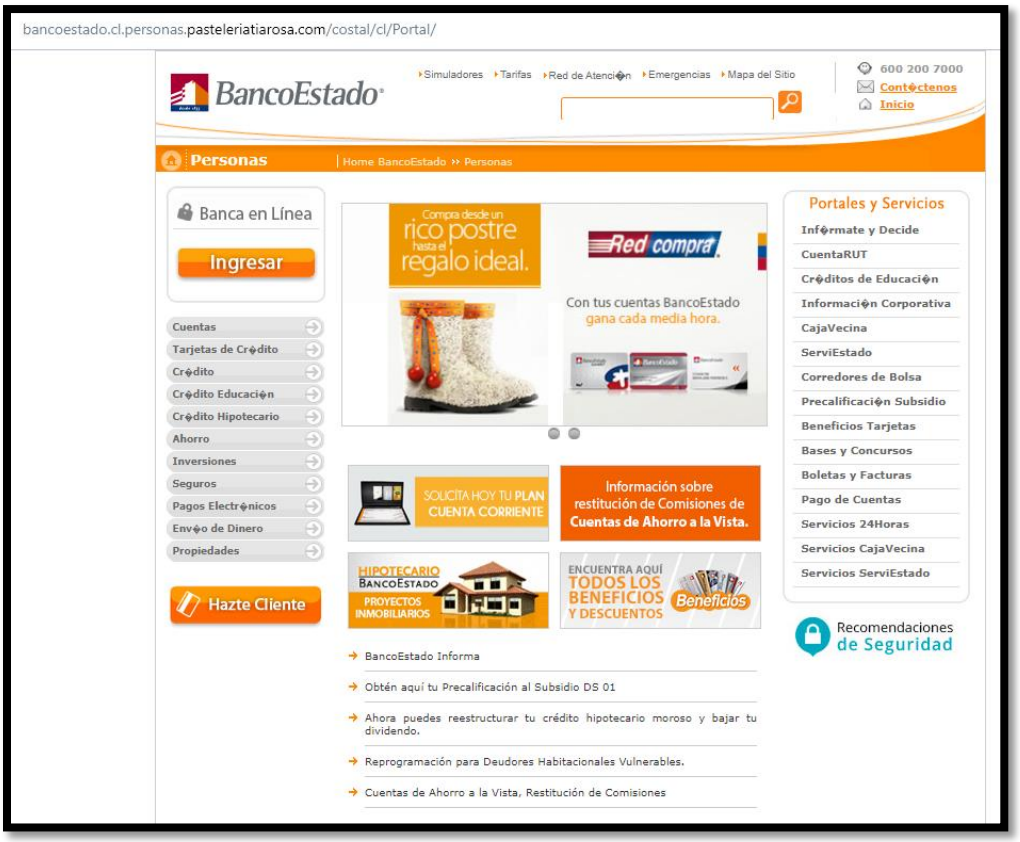
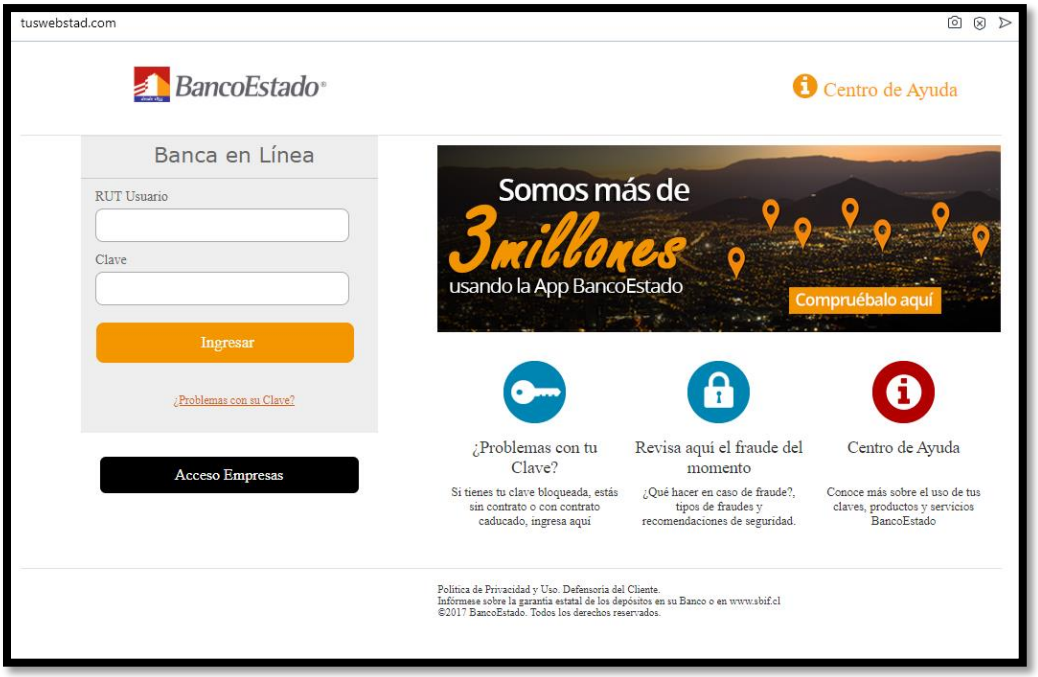
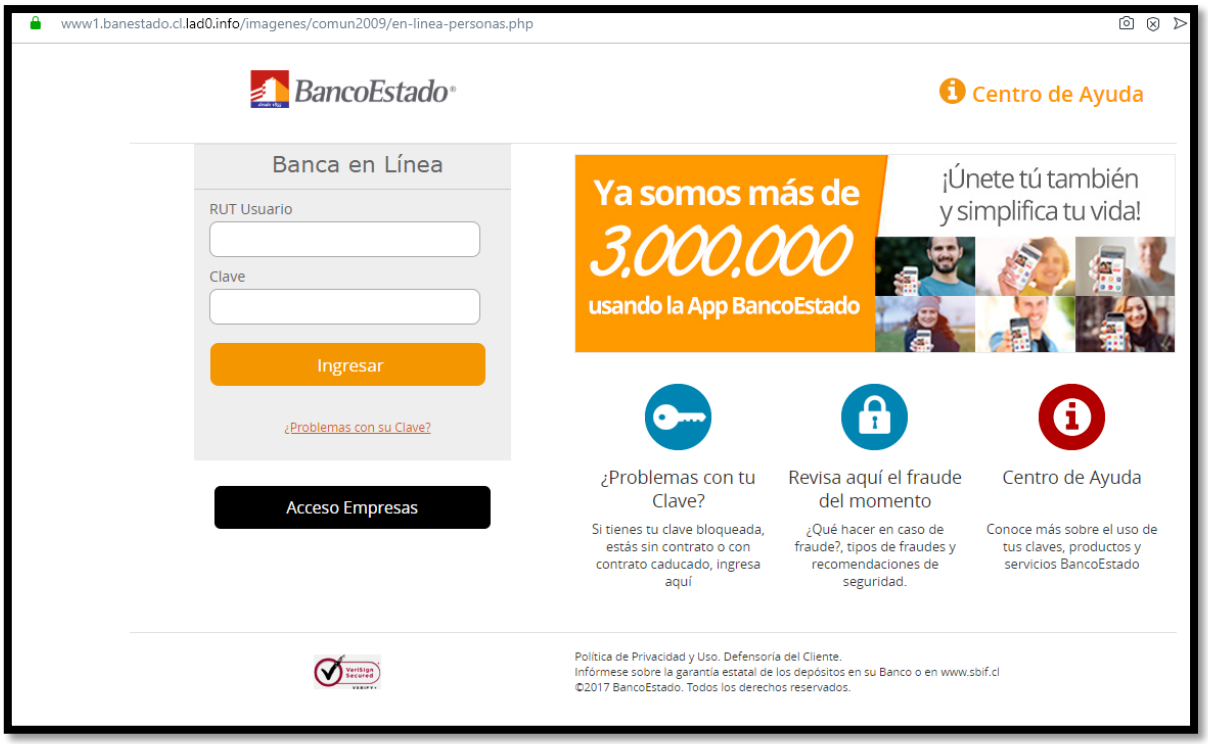


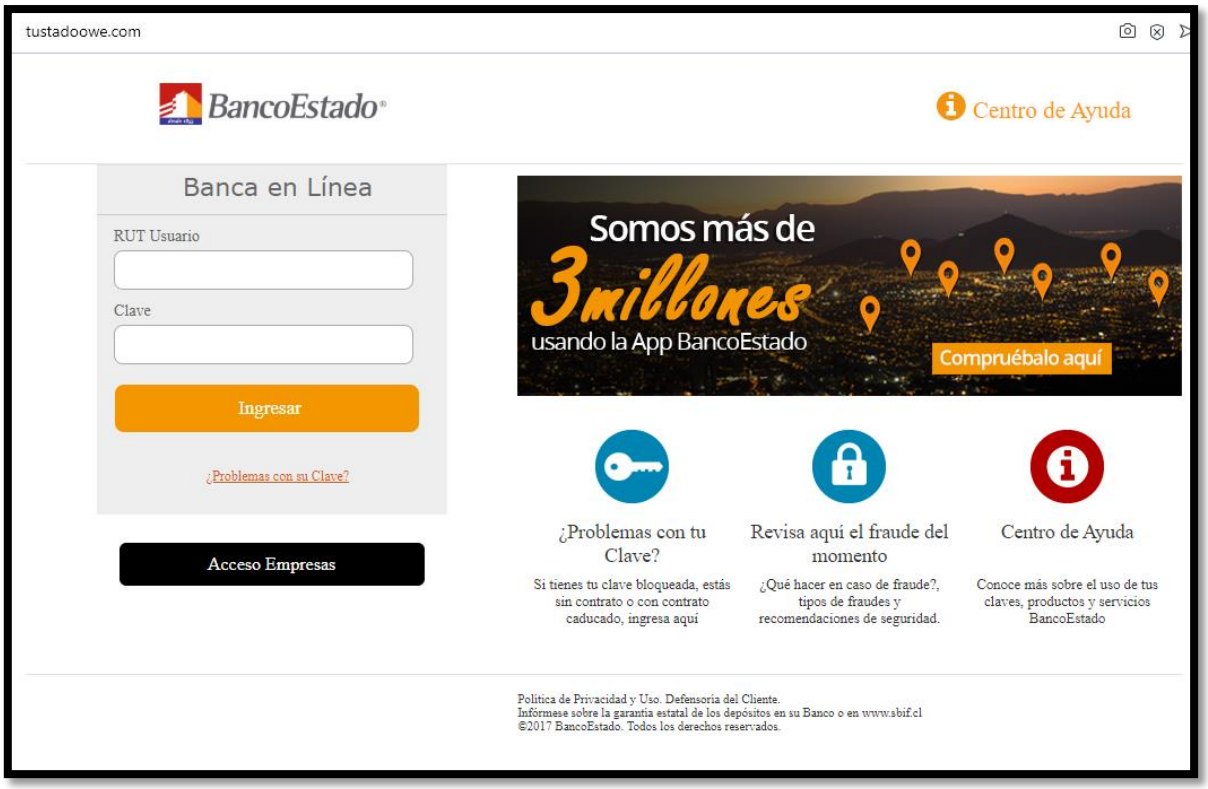
Imagen del sitio




bancoestado.cl.personas.pasteleriatiarosa.com/costal/cl/Portal/
BancoEstado
Simuladores
Tarifas
Red de Atención
Emergencias
Mapa del Sitio
600 200 7000
Contáctenos
Inicio
Personas
Home BancoEstado ›› Personas
Banca en Línea
Ingresar
Cuentas
Tarjetas de Crédito
Crédito
Crédito Educación
Crédito Hipotecario
Ahorro
Inversiones
Seguros
Pagos Electrónicos
Envío de Dinero
Propiedades
Hazte Cliente
Compra desde un rico postre hasta el regalo ideal.
Red compra
Con tus cuentas BancoEstado gana cada media hora.
SOLICITA HOY TU PLAN CUENTA CORRIENTE
Información sobre restitución de Comisiones de Cuentas de Ahorro a la Vista.
HIPOTECARIO BANCOESTADO PROYECTOS INMOBILIARIOS
ENCUENTRA AQUÍ TODOS LOS BENEFICIOS Y DESCUENTOS Beneficios
BancoEstado Informa
Obtén aquí tu Precalificación al Subsidio DS 01
Ahora puedes reestructurar tu crédito hipotecario moroso y bajar tu dividendo.
Reprogramación para Deudores Habitacionales Vulnerables.
Cuentas de Ahorro a la Vista, Restitución de Comisiones
Portales y Servicios
Infórmate y Decide
CuentaRUT
Créditos de Educación
Información Corporativa
CajaVecina
ServiEstado
Corredores de Bolsa
Precalificación Subsidio
Beneficios Tarjetas
Bases y Concursos
Boletas y Facturas
Pago de Cuentas
Servicios 24Horas
Servicios CajaVecina
Servicios ServiEstado
Recomendaciones de Seguridad


tuswebstad.com
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Somos más de 3millones usando la App BancoEstado
Compruébalo aquí
¿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.


www1.banestado.cl.lad0.info/imagenes/comun2009/en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
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.


tustadoowe.com
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Somos más de
3millones
usando la App BancoEstado
Compruébalo aquí
¿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: pasteleriatiarosa.com
Registry Domain ID: 2441273203_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-10-07T23:22:46.00Z
Creation Date: 2019-10-07T23:22:00.00Z
Registrar Registration Expiration Date: 2020-10-07T23:22:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street:
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Recoleta
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/56eb7542-82eb-489d-a06a-551462ca7ac3
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street:
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:
Admin Fax: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street:
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: NS1.ADX.HOST
Name Server: NS2.ADX.HOST
DNSSEC: unsigned
```

```
Domain Name: tuswebstad.com
Registry Domain ID: 2480484939_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-01-15T18:29:46Z
Creation Date: 2020-01-15T18:29:45Z
Registrar Registration Expiration Date: 2021-01-15T18:29:45Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Puerto Rico
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tuswe
bstad.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tuswebstad
.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tuswebstad.
com
Name Server: NS41.DOMAINCONTROL.COM
Name Server: NS42.DOMAINCONTROL.COM
DNSSEC: unsigned
```

```
Domain Name: LAD0.INFO
Registry Domain ID: D503300001182853797-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-01-15T18:30:31Z
Creation Date: 2020-01-15T18:26:29Z
Registry Expiry Date: 2021-01-15T18:26:29Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Name Server: NS3.DNSOWL.COM
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: tustadoowe.com
Registry Domain ID: 2480472067_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-01-15T16:06:32Z
Creation Date: 2020-01-15T16:06:31Z
Registrar Registration Expiration Date: 2021-01-15T16:06:31Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Puerto Rico
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tusta
doowe.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tustadoowe
.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tustadoowe.
com
Name Server: NS41.DOMAINCONTROL.COM
Name Server: NS42.DOMAINCONTROL.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.