Alerta de seguridad informática	8FFR-00142-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de Diciembre de 2019
Última revisión	6 de Diciembre de 2019

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 ocho portales bancarios 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.

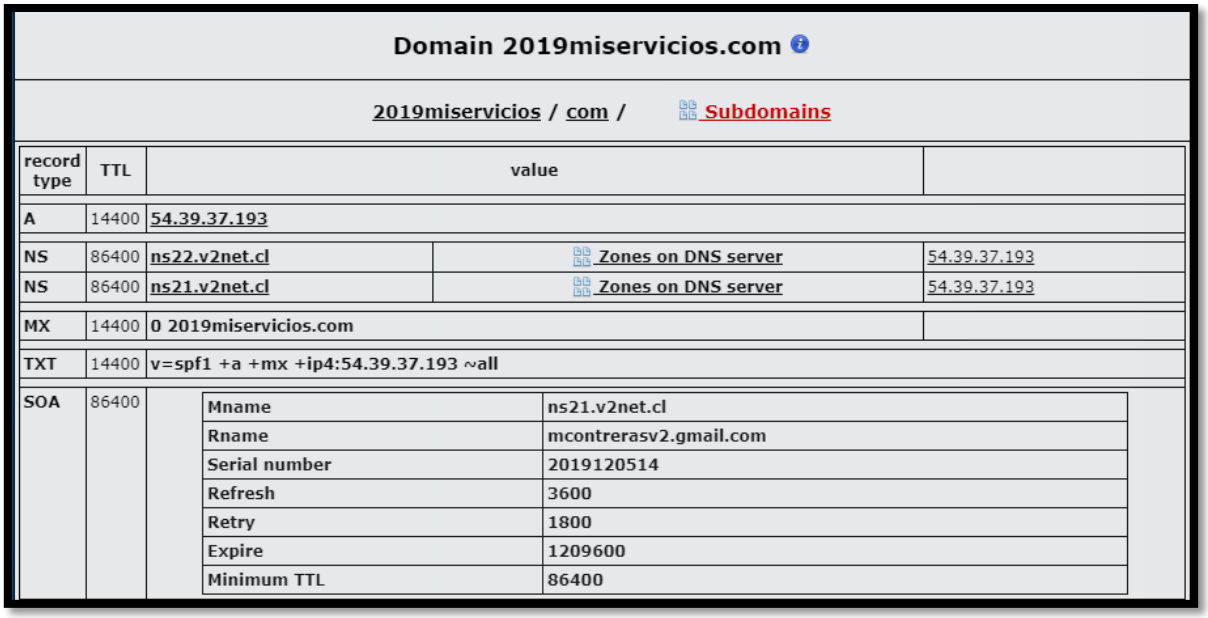
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

URL Sitio Clonado:

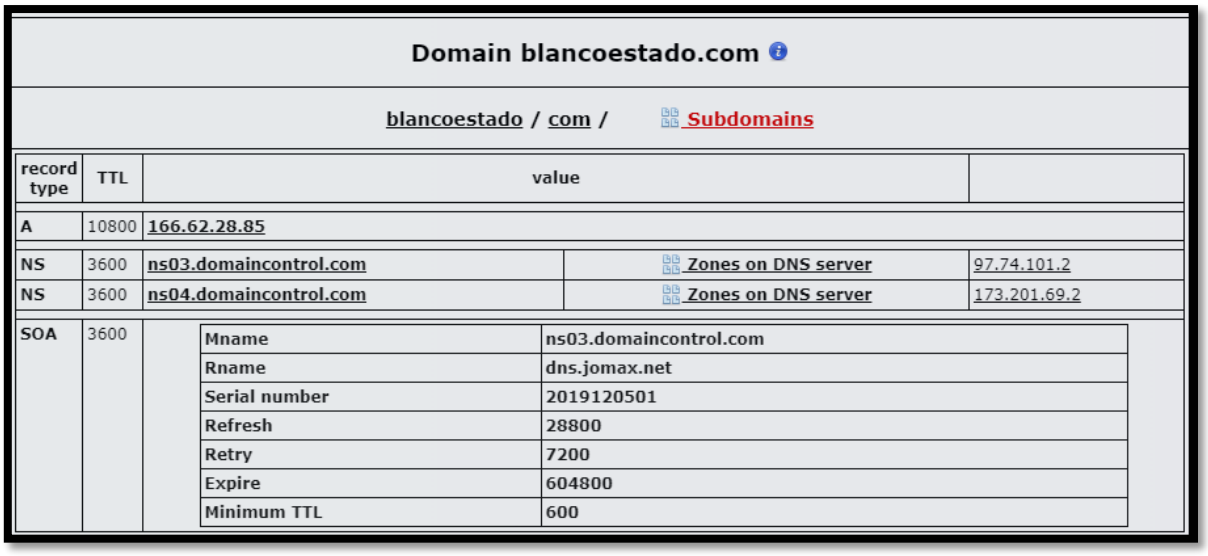
2019miservicios[.]com
www[.]actualizacion[.]personas[.]2019miservicios[.]com/profesional/imagenes/comun2008/banca-en-linea-personas[.]html
www[.]actualizacion[.]personas[.]2019miservicios[.]com/profesional/
bancoestado[.]cl[.]2019miservicios[.]com/profesional/imagenes/comun2008/banca-en-linea-personas[.]html
bancoestado[.]cl[.]2019miservicios[.]com/profesional/
blancoestado[.]com
blancoestado[.]com/imagenes/_personas/home/default[.]html
blancoestado[.]com/imagenes/comun2008/banca-en-linea-personas[.]html



Domain 2019miservicios.com

2019miservicios / com / Subdomains

record type	TTL	value		
A	14400	54.39.37.193		
NS	86400	ns22.v2net.cl	Zones on DNS server	54.39.37.193
NS	86400	ns21.v2net.cl	Zones on DNS server	54.39.37.193
MX	14400	0 2019miservicios.com		
TXT	14400	v=spf1 +a +mx +ip4:54.39.37.193 ~all		
SOA	86400	Mname	ns21.v2net.cl	
		Rname	mcontrerasv2.gmail.com	
		Serial number	2019120514	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	



Domain blancoestado.com

blancoestado / com / Subdomains

record type	TTL	value		
A	10800	166.62.28.85		
NS	3600	ns03.domaincontrol.com	Zones on DNS server	97.74.101.2
NS	3600	ns04.domaincontrol.com	Zones on DNS server	173.201.69.2
SOA	3600	Mname: ns03.domaincontrol.com Rname: dns.jomax.net Serial number: 2019120501 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

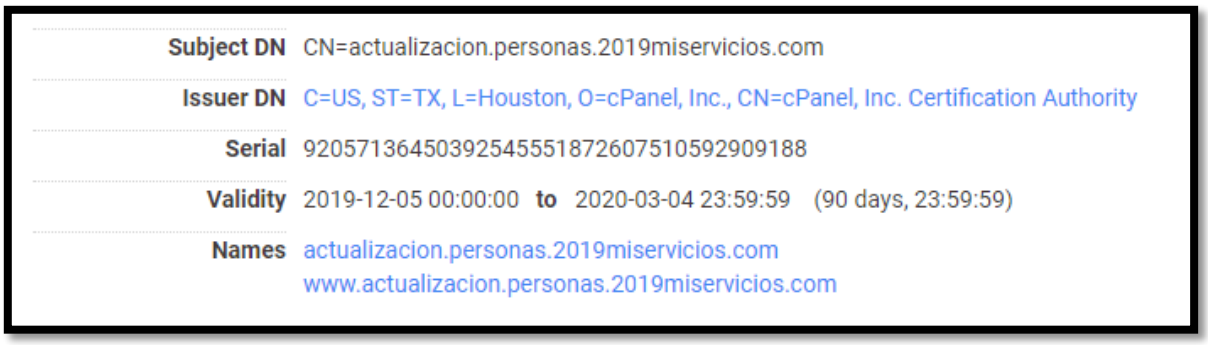
Subject DN CN=2019miservicios.com

Issuer DN C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority

Serial 297123779884147140023803251751020871625

Validity 2019-12-04 00:00:00 **to** 2020-03-03 23:59:59 (90 days, 23:59:59)

Names 2019miservicios.com
cpanel.2019miservicios.com
mail.2019miservicios.com
webdisk.2019miservicios.com
webmail.2019miservicios.com
www.2019miservicios.com



Subject DN CN=actualizacion.personas.2019miservicios.com

Issuer DN C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority

Serial 92057136450392545551872607510592909188

Validity 2019-12-05 00:00:00 **to** 2020-03-04 23:59:59 (90 days, 23:59:59)

Names actualizacion.personas.2019miservicios.com
www.actualizacion.personas.2019miservicios.com

Subject DN	CN=bancoestado.cl.2019miservicios.com
Issuer DN	C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority
Serial	862168743423743163604525868370167390 90
Validity	2019-12-05 00:00:00 **to** 2020-03-04 23:59:59 (90 days, 23:59:59)
Names	bancoestado.cl.2019miservicios.com www.bancoestado.cl.2019miservicios.com

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

IP

54.39.37.193

166.62.28.85

Domain 2019miservicios.com is located on IP address << 54.39.37.193 >>

Block start	54.0.0.0
End of block	54.63.255.255
Block size	4194304 Domains in block
Block name	MERCK2
AS number	16276
Parent block	54.0.0.0 - 54.255.255.255
Organization	Merck and Co., Inc.
City	Rahway
Region/State	New Jersey
Country	US , United States 40735
Reg. date	1992-03-17
Host name	morty.v2net.cl

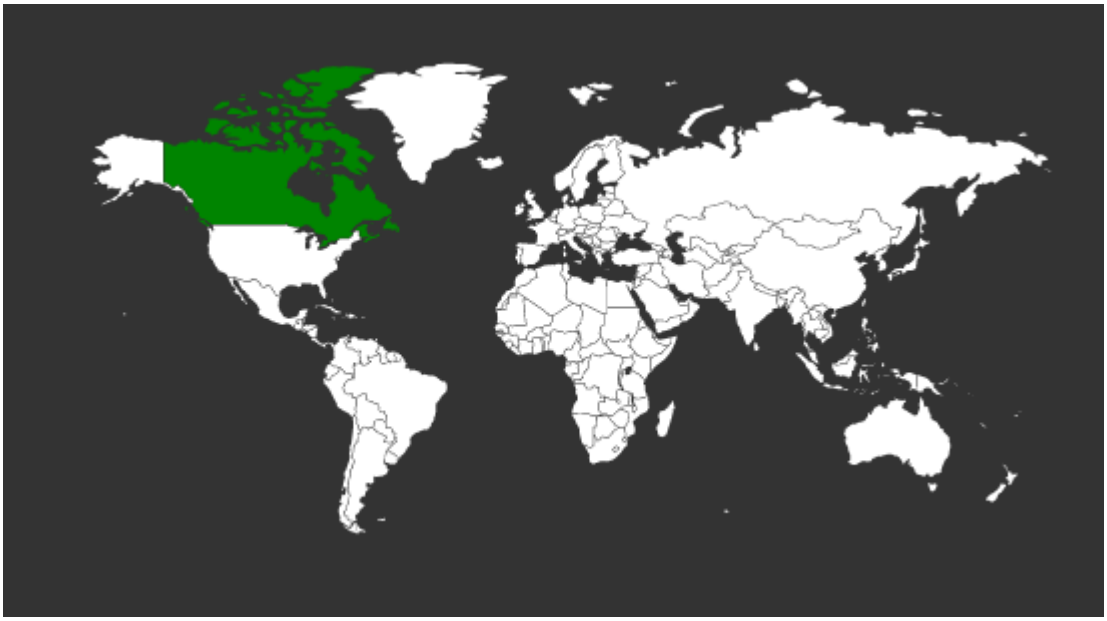
Domain blancoestado.com is located on IP address << 166.62.28.85 >>

Block start	166.62.0.0
End of block	166.62.127.255
Block size	32768 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	166.0.0.0 - 166.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2012-11-14
Host name	ip-166-62-28-85.ip.secureserver.net
Web server	Apache/2.4.23

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

Localización

Montreal, Quebec, Canadá



Scottsdale, Arizona, Estados Unidos

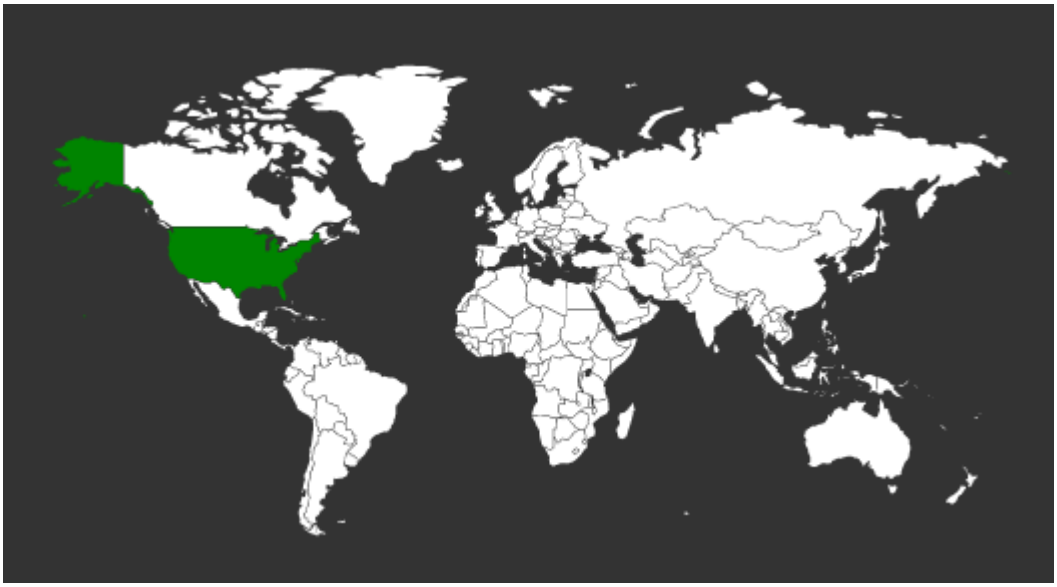
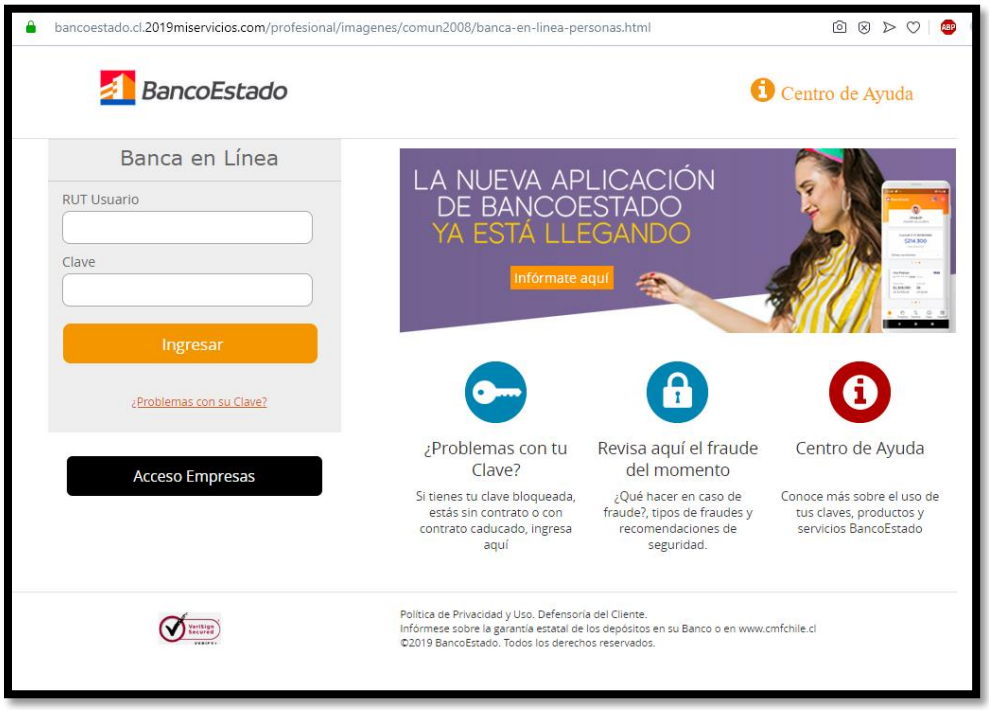
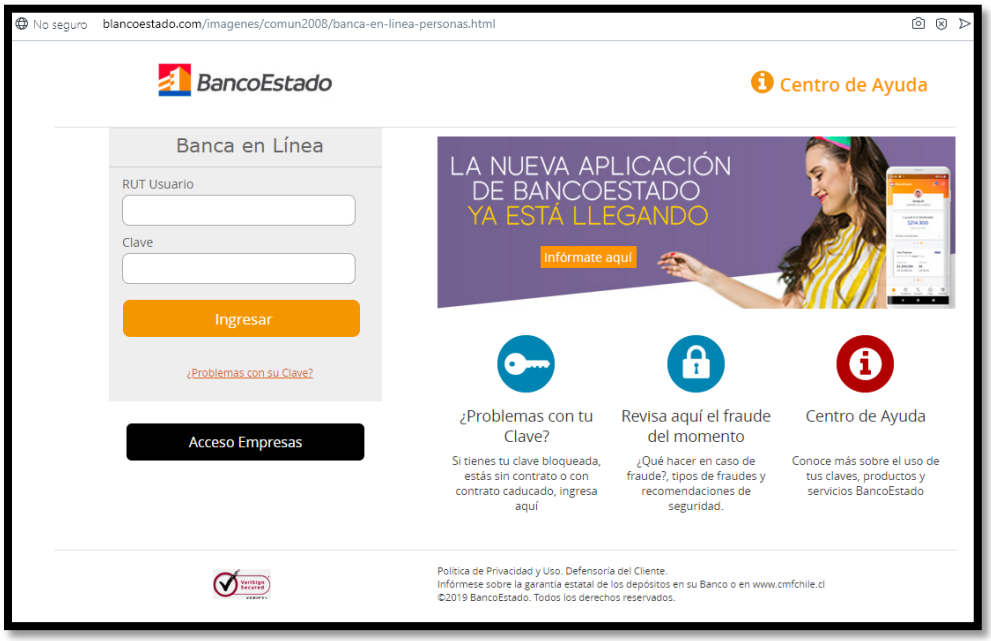
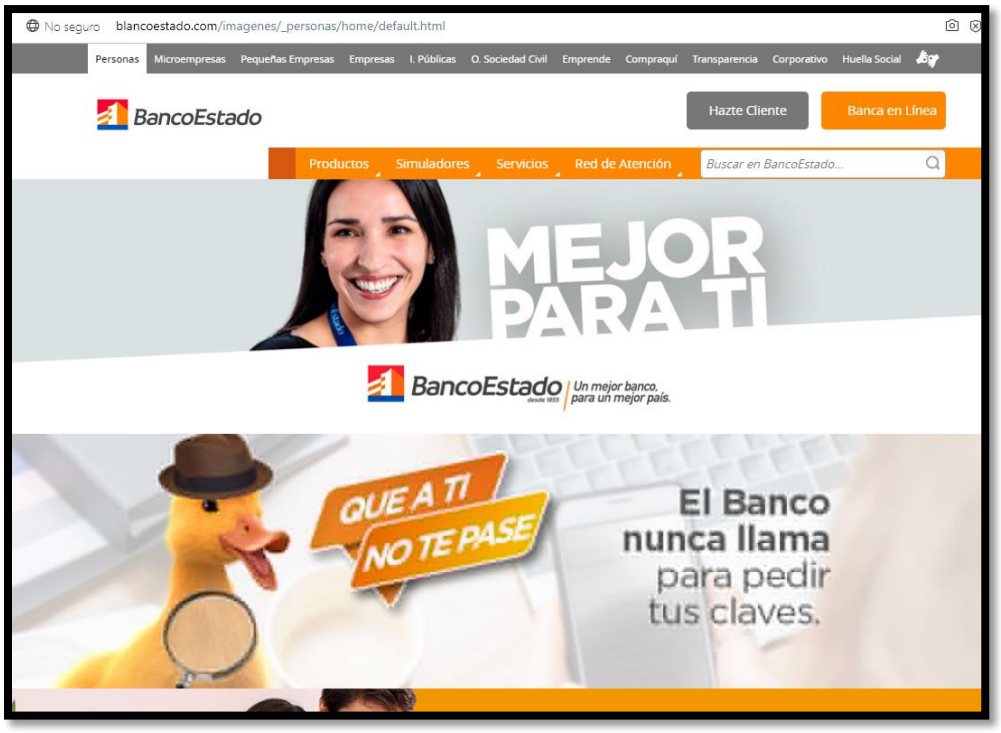
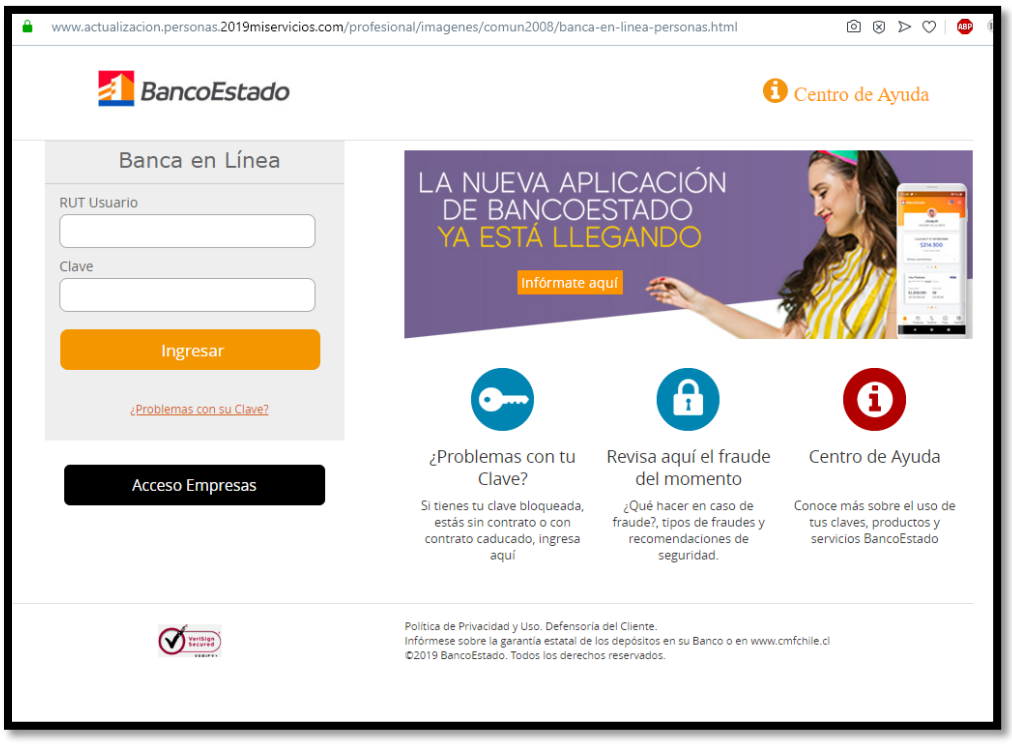


Imagen del sitio






No seguro
blancoestado.com/imagenes/_personas/home/default.html
Personas
Microempresas
Pequeñas Empresas
Empresas
I. Públicas
O. Sociedad Civil
Emprende
Compraquí
Transparencia
Corporativo
Huella Social
BancoEstado
Hazte Cliente
Banca en Línea
Productos
Simuladores
Servicios
Red de Atención
Buscar en BancoEstado...
MEJOR PARA TI
BancoEstado
Un mejor banco, para un mejor país.
QUE A TI NO TE PASE
El Banco nunca llama para pedir tus claves.


www.actualizacion.personas.2019miservicios.com/profesional/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO
Infórmate 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.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: BLANCOESTADO.COM
Registry Domain ID: 2463567159_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-12-05T12:36:29Z
Creation Date: 2019-12-05T12:36:28Z
Registry Expiry Date: 2020-12-05T12:36:28Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS03.DOMAINCONTROL.COM
Name Server: NS04.DOMAINCONTROL.COM
DNSSEC: unsigned
```

```
Domain Name: 2019miservicios.com
Registry Domain ID: 2463223841_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.registrar.eu
Updated Date: 2019-12-04T16:38:47Z
Creation Date: 2019-12-04T15:38:39Z
Registrar Registration Expiration Date: 2020-12-04T15:38:39Z
Registrar: Hosting Concepts B.V. d/b/a Openprovider
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Domain Status: ok https://icann.org/epp#ok
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Disturbudora valdenegro
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Maipu
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: https://contact-form.registrar.eu/?domainName=2019miservicios.com&purpose=owner
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
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: https://contact-form.registrar.eu/?domainName=2019miservicios.com&purpose=admin
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: https://contact-form.registrar.eu/?domainName=2019miservicios.com&purpose=tech
Name Server: ns22.v2net.cl
Name Server: ns21.v2net.cl
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.