Alerta de seguridad informática	8FFR20-00249-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 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

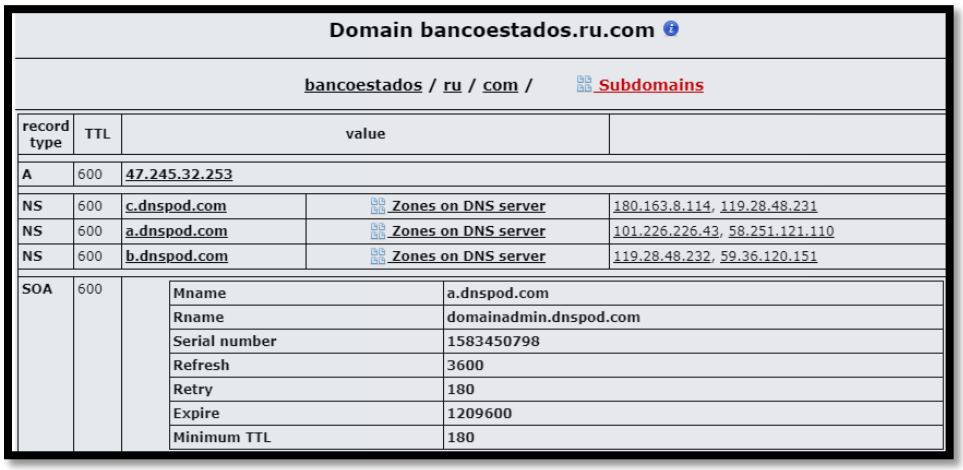
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

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

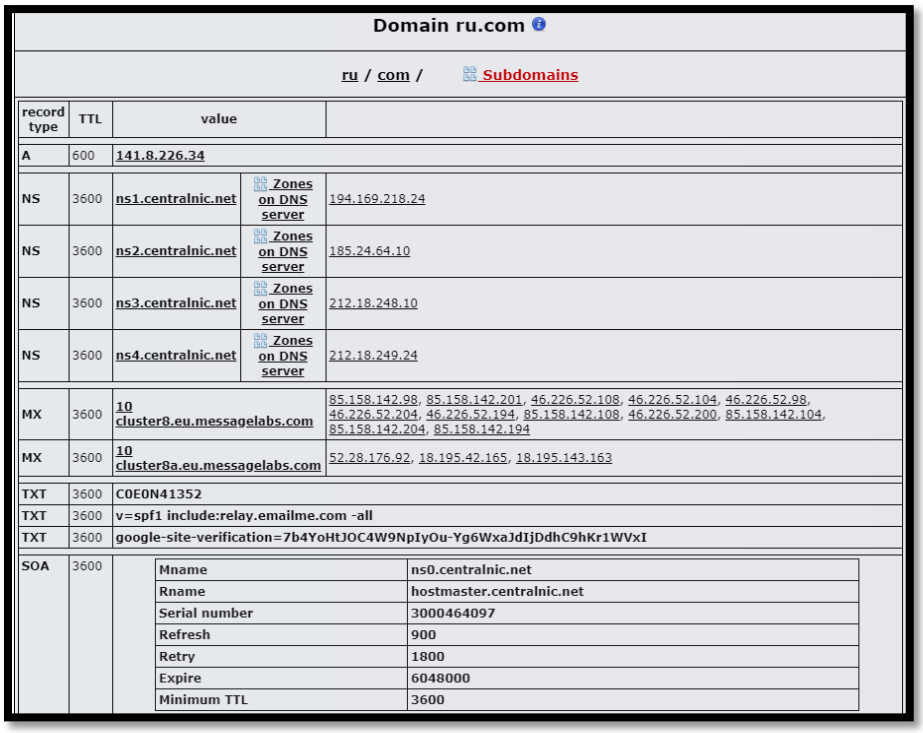
bancoestados[.]ru[.]com/imagenes/comun2008/
cuenta-rut[.]bacoestado[.]online
banco[.]estadomobilecl[.]com
banco[.]estadomobilecl[.]com/site/control[.]php



Domain bancoestados.ru.com

bancoestados / ru / com / Subdomains

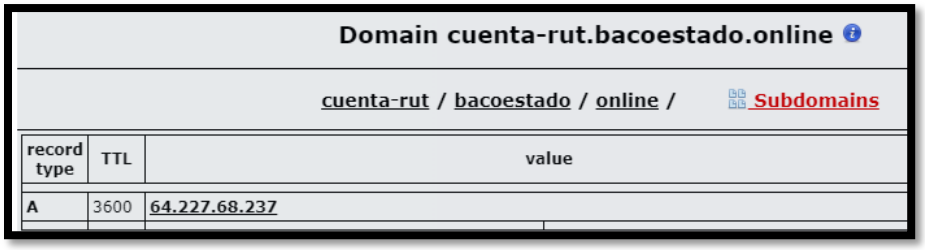
record type	TTL	value		
A	600	47.245.32.253		
NS	600	c.dnspod.com	Zones on DNS server	180.163.8.114, 119.28.48.231
NS	600	a.dnspod.com	Zones on DNS server	101.226.226.43, 58.251.121.110
NS	600	b.dnspod.com	Zones on DNS server	119.28.48.232, 59.36.120.151
SOA	600	Mname	a.dnspod.com	
		Rname	domainadmin.dnspod.com	
		Serial number	1583450798	
		Refresh	3600	
		Retry	180	
		Expire	1209600	
		Minimum TTL	180	



Domain ru.com

ru / com / Subdomains

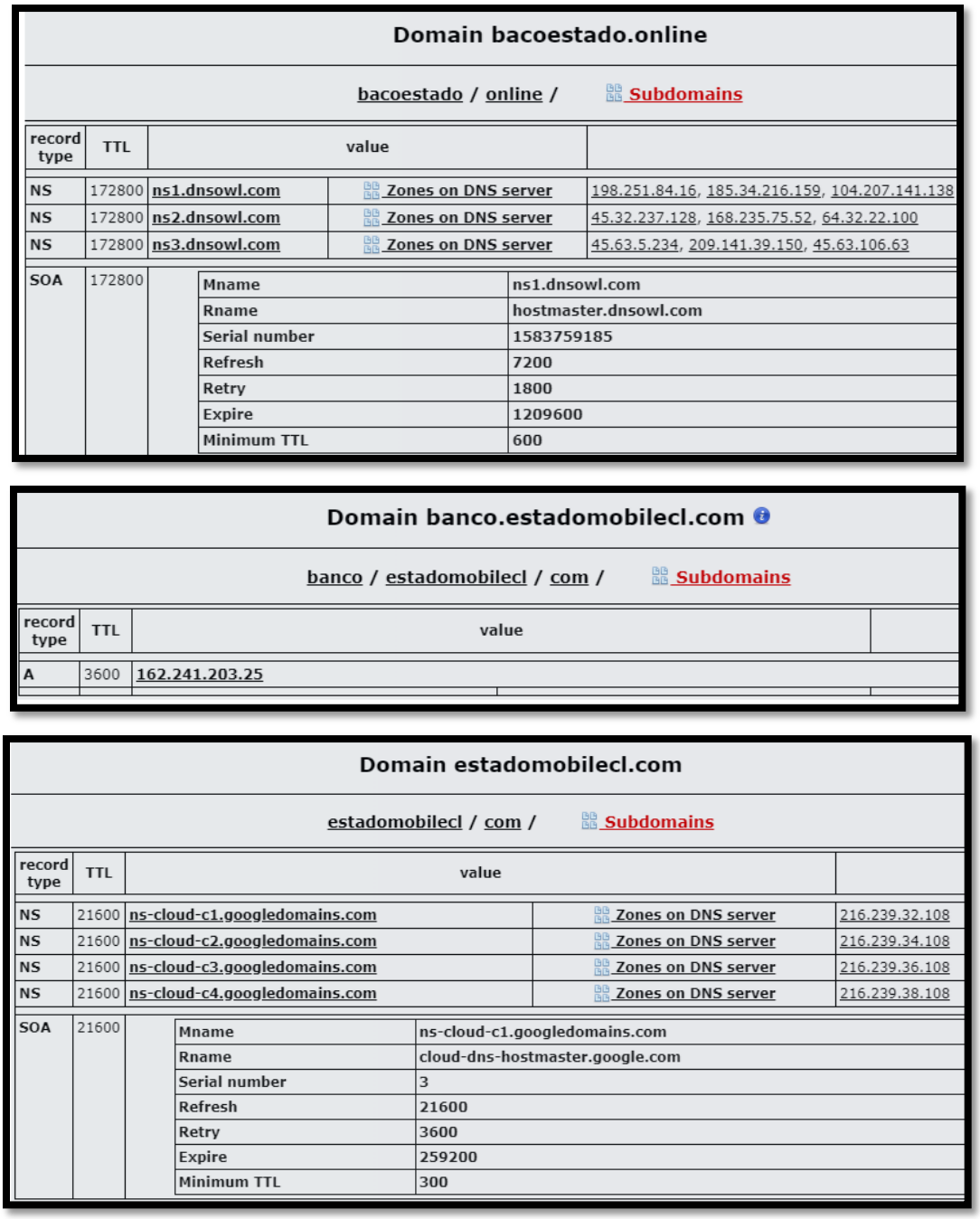
record type	TTL	value		
A	600	141.8.226.34		
NS	3600	ns1.centralnic.net	Zones on DNS server	194.169.218.24
NS	3600	ns2.centralnic.net	Zones on DNS server	185.24.64.10
NS	3600	ns3.centralnic.net	Zones on DNS server	212.18.248.10
NS	3600	ns4.centralnic.net	Zones on DNS server	212.18.249.24
MX	3600	10 cluster8.eu.messagelabs.com		85.158.142.98, 85.158.142.201, 46.226.52.108, 46.226.52.104, 46.226.52.98, 46.226.52.204, 46.226.52.194, 85.158.142.108, 46.226.52.200, 85.158.142.104, 85.158.142.204, 85.158.142.194
MX	3600	10 cluster8a.eu.messagelabs.com		52.28.176.92, 18.195.42.165, 18.195.143.163
TXT	3600	C0E0N41352		
TXT	3600	v=spf1 include:relay.emailme.com -all		
TXT	3600	google-site-verification=7b4YoHtJOC4W9NpIyOu-Yg6WxaJdIjDdhC9hKr1WVxI		
SOA	3600	Mname: ns0.centralnic.net Rname: hostmaster.centralnic.net Serial number: 3000464097 Refresh: 900 Retry: 1800 Expire: 6048000 Minimum TTL: 3600		



Domain cuenta-rut.bacoestado.online

cuenta-rut / bacoestado / online / Subdomains

record type	TTL	value
A	3600	64.227.68.237



Domain bacoestado.online

bacoestado / online / 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, 168.235.75.52, 64.32.22.100
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	1583759185
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain banco.estadomobilecl.com

banco / estadomobilecl / com / Subdomains

record type	TTL	value
A	3600	162.241.203.25

Domain estadomobilecl.com

estadomobilecl / com / Subdomains

record type	TTL	value		
NS	21600	ns-cloud-c1.googledomains.com	Zones on DNS server	216.239.32.108
NS	21600	ns-cloud-c2.googledomains.com	Zones on DNS server	216.239.34.108
NS	21600	ns-cloud-c3.googledomains.com	Zones on DNS server	216.239.36.108
NS	21600	ns-cloud-c4.googledomains.com	Zones on DNS server	216.239.38.108

SOA	21600	Mname	ns-cloud-c1.googledomains.com
		Rname	cloud-dns-hostmaster.google.com
		Serial number	3
		Refresh	21600
		Retry	3600
		Expire	259200
		Minimum TTL	300

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

Certificados

Subject DN	CN=bancoestados.ru.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	389763753621934071232597246565699132393110
Validity	2020-03-05 22:47:54 **to** 2020-06-03 22:47:54 (90 days, 0:00:00)
Names	bancoestados.ru.com

Subject DN	CN=cuenta-rut.bacoestado.online
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	289949264247121541230406577470567178045083
Validity	2020-03-07 19:12:15 **to** 2020-06-05 19:12:15 (90 days, 0:00:00)
Names	cuenta-rut.bacoestado.online

Subject DN	CN=banco.estadomobilecl.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	357208705465465865149169714785933450820092
Validity	2020-03-08 20:41:02 **to** 2020-06-06 20:41:02 (90 days, 0:00:00)
Names	banco.estadomobilecl.com

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

IP

47[.]245[.]32[.]253
64[.]227[.]68[.]237
162[.]241[.]203[.]25

Domain bancoestados.ru.com is located on IP address << 47.245.32.253 >>

Block start	47.235.0.0
End of block	47.246.255.255
Block size	786432 Domains in block
Block name	AL-3
AS number	45102
Parent block	47.224.0.0 - 47.246.255.255
Organization	Alibaba.com LLC

Domain cuenta-rut.bacoestado.online is located on IP address << 64.227.68.237 >>

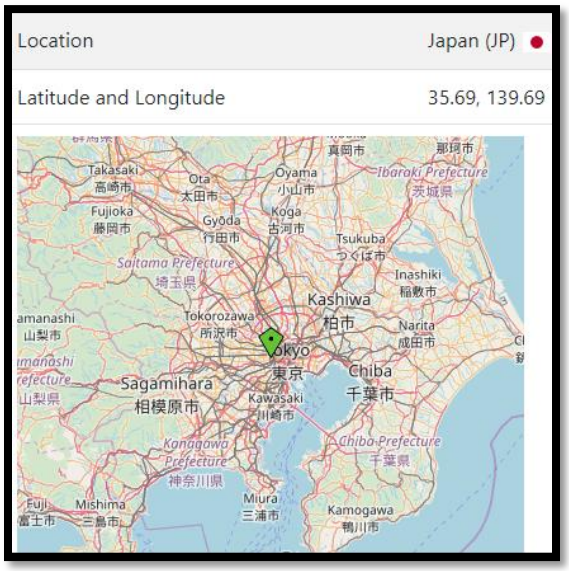
Block start	64.227.68.0
End of block	64.227.68.255
Block size	256 Domains in block
Block name	64-227-68-0-NET
AS number	14061
Parent block	64.224.0.0 - 64.227.255.255
Organization	Web.com, Inc.

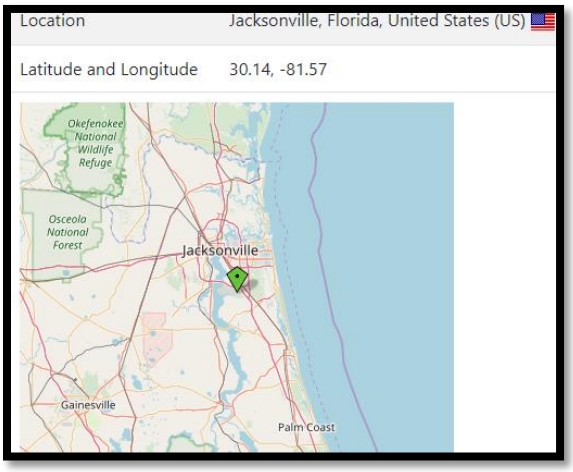
Domain banco.estadomobilecl.com is located on IP address << 162.241.203.25 >>

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

Localización
Tokyo, Japón
Jacksonville, Florida, Estados Unidos
Provo, Utah, Estados Unidos





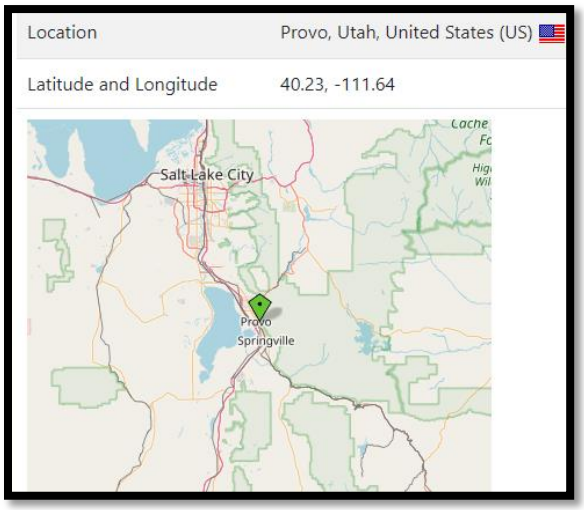
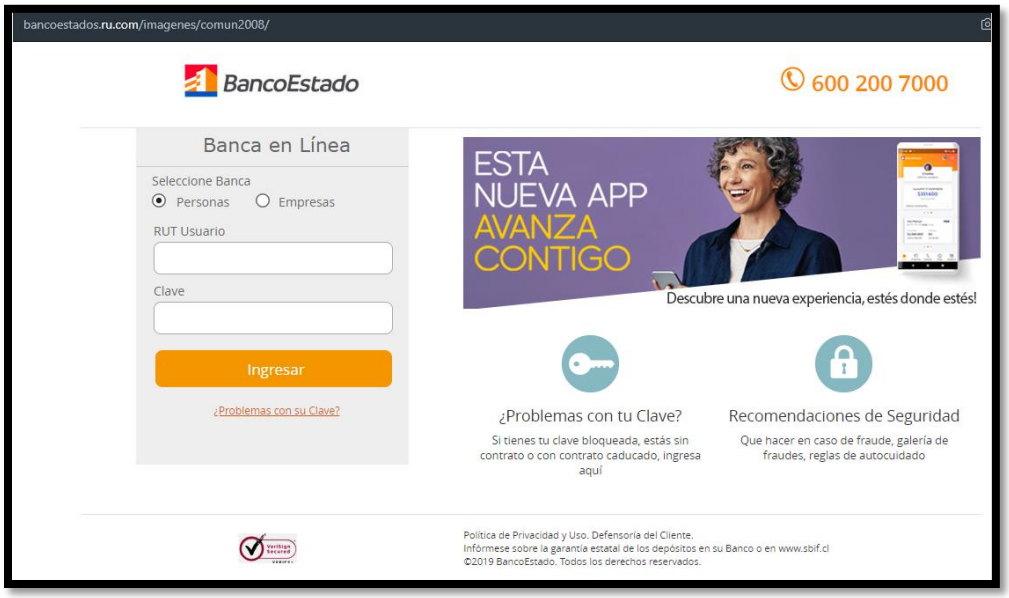
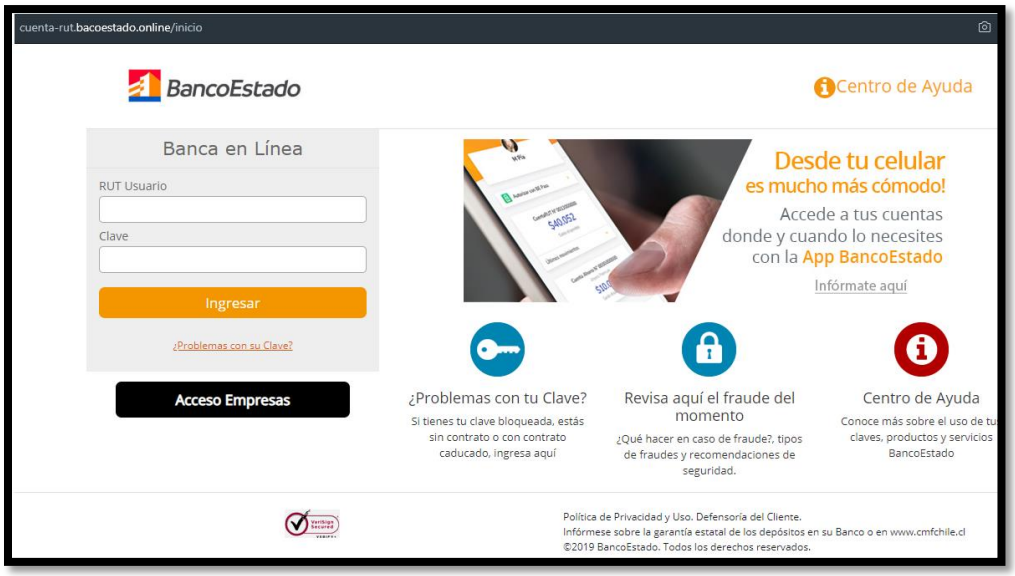
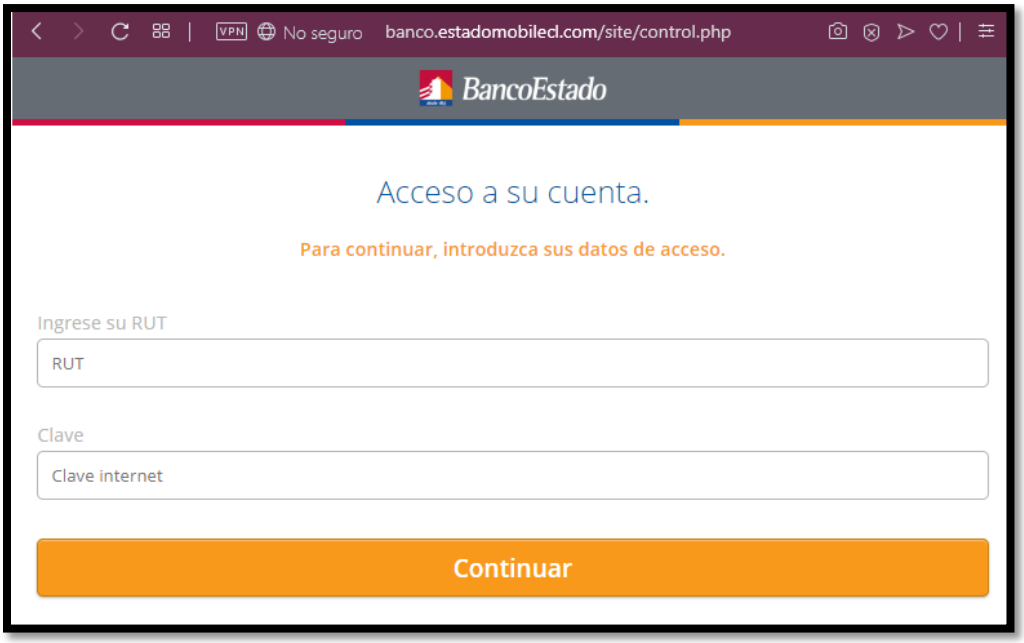


Imagen del sitio




cuenta-rut.bacoestado.online/inicio
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Desde tu celular
es mucho más cómodo!
Accede a tus cuentas
donde y cuando lo necesites
con la App BancoEstado
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 tu 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.


No seguro
banco.estadomobilecl.com/site/control.php
BancoEstado
Acceso a su cuenta.
Para continuar, introduzca sus datos de acceso.
Ingrese su RUT
RUT
Clave
Clave internet
Continuar

Whois

```
Domain name: BANCOESTADOS.RU.COM
Registry Domain ID: D176724684-CNIC
Registrar WHOIS Server: whois.reg.com
Registrar URL: https://www.reg.com
Registrar URL: https://www.reg.ru
Updated Date: 2020-03-05T23:26:02.0Z
Creation Date: 2020-03-05T23:25:23.0Z
Registrar Registration Expiration Date: 2021-03-05T23:59:59.0Z
Registrar: Registrar of domain names REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Status: addPeriod http://www.icann.org/epp#addPeriod
Registrant ID: reg-p706c9p3dvh4
Registrant Name: Protection of Private Person
Registrant Street: PO box 87, REG.RU Protection Service
Registrant City: Moscow
Registrant State/Province:
Registrant Postal Code: 123007
Registrant Country: RU
Registrant Phone: +7.4955801111
Registrant Phone Ext:
Registrant Fax: +7.4955801111
Registrant Fax Ext:
Registrant Email: BANCOESTADOS.RU.COM@regprivate.ru
Admin ID: reg-elxbd83e3imf
Admin Name: Protection of Private Person
Admin Street: PO box 87, REG.RU Protection Service
Admin City: Moscow
Admin State/Province:
Admin Postal Code: 123007
Admin Country: RU
Admin Phone: +7.4955801111
Admin Phone Ext:
Admin Fax: +7.4955801111
Admin Fax Ext:
Admin Email: BANCOESTADOS.RU.COM@regprivate.ru
Tech ID: reg-c2k37sbgab6i
Tech Name: Protection of Private Person
Tech Street: PO box 87, REG.RU Protection Service
Tech City: Moscow
Tech State/Province:
Tech Postal Code: 123007
Tech Country: RU
Tech Phone: +7.4955801111
Tech Phone Ext:
Tech Fax: +7.4955801111
Tech Fax Ext:
Tech Email: BANCOESTADOS.RU.COM@regprivate.ru
Name Server: a.dnspod.com
Name Server: c.dnspod.com
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020.03.09T16:39:52Z <<<
```

```
Domain Name: bacoestado.online
Registry Domain ID: D176712589-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-06T07:00:00Z
Creation Date: 2020-03-05T07:00:00Z
Registrar Registration Expiration Date: 2021-03-05T07:00:00Z
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: Manuel F. Zeledon
Registrant Organization:
Registrant Street: 157 Modoc Place
Registrant City: Idaho
Registrant State/Province: ID
Registrant Postal Code: 85014
Registrant Country: US
Registrant Phone: +1.2327881775
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: chatodark992@gmail.com
Registry Admin ID:
Admin Name: Manuel F. Zeledon
Admin Organization:
Admin Street: 157 Modoc Place
Admin City: Idaho
Admin State/Province: ID
Admin Postal Code: 85014
Admin Country: US
Admin Phone: +1.2327881775
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: chatodark992@gmail.com
Registry Tech ID:
Tech Name: Manuel F. Zeledon
Tech Organization:
Tech Street: 157 Modoc Place
Tech City: Idaho
Tech State/Province: ID
Tech Postal Code: 85014
Tech Country: US
Tech Phone: +1.2327881775
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: chatodark992@gmail.com
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/
>>> Last update of WHOIS database: 2020-03-09T07:00:00Z <<<
```

```
Domain Name: estadomobilecl.com
Registry Domain ID: 2501395461_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-08T21:29:16Z
Creation Date: 2020-03-08T21:29:14Z
Registrar Registration Expiration Date: 2021-03-08T21:29:14Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246635350
Registrant Organization: Contact Privacy Inc. Customer 1246635350
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: guqcflr76jfs@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246635350
Admin Organization: Contact Privacy Inc. Customer 1246635350
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: guqcflr76jfs@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246635350
Tech Organization: Contact Privacy Inc. Customer 1246635350
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: guqcflr76jfs@contactprivacy.email
Name Server: NS-CLOUD-C1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-C4.GOOGLEDOMAINS.COM
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-09T14:10:20Z <<<
```

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.