Alerta de seguridad informática	8FFR-00143-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de Diciembre de 2019
Última revisión	8 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.

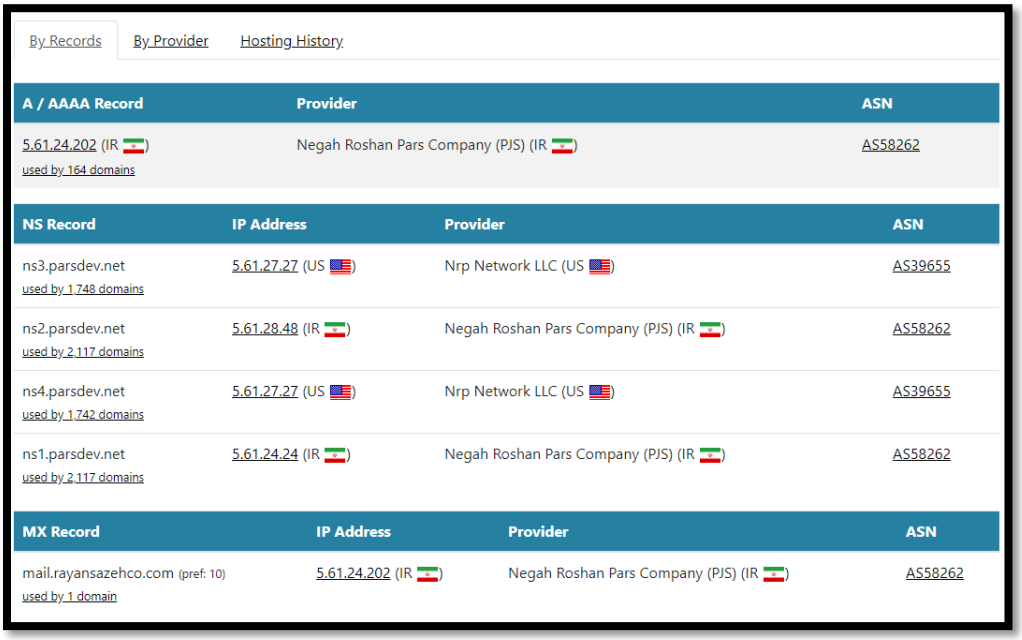
Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales bancarios fraudulentos asociados a tres una 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:
rayansazehco[.]com/wp-content/plugins/duplicate-page/www[.]bancoestado[.]cl[.]bloqueo/estado[.]cl/www[.]bancoestado[.]cl/actualizaciondedatos[.]info
banco-estado[.]actualizaciondedatos[.]info
banco-estado[.]actualizaciondedatos[.]info/comun2019/banca-en-linea-personas[.]php
bancoestado[.]actualizaciondedatos[.]info
bancoestado[.]actualizaciondedatos[.]info/comun2019/banca-en-linea-personas[.]php
bestrate[.]ie/fckeditor/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html



By Records | By Provider | Hosting History

A / AAAA Record	Provider	ASN
5.61.24.202 (IR) used by 164 domains	Negah Roshan Pars Company (PJS) (IR)	AS58262

NS Record	IP Address	Provider	ASN
ns3.parsdev.net used by 1,748 domains	5.61.27.27 (US)	Nrp Network LLC (US)	AS39655
ns2.parsdev.net used by 2,117 domains	5.61.28.48 (IR)	Negah Roshan Pars Company (PJS) (IR)	AS58262
ns4.parsdev.net used by 1,742 domains	5.61.27.27 (US)	Nrp Network LLC (US)	AS39655
ns1.parsdev.net used by 2,117 domains	5.61.24.24 (IR)	Negah Roshan Pars Company (PJS) (IR)	AS58262

MX Record	IP Address	Provider	ASN
mail.rayansazehco.com (pref: 10) used by 1 domain	5.61.24.202 (IR)	Negah Roshan Pars Company (PJS) (IR)	AS58262

Domain actualizaciondedatos.info

actualizaciondedatos / info / Subdomains

record type	TTL	value		
A	86400	82.194.70.31		
NS	86400	ns2.actualizaciondedatos.info	Zones on DNS server	82.194.70.31
NS	86400	ns1.actualizaciondedatos.info	Zones on DNS server	82.194.70.31
MX	86400	10 mail.actualizaciondedatos.info		82.194.70.31
TXT	86400	v=spf1 a mx include:spf.mail-servicios.com ~all		
SOA	86400	Mname	ns1.actualizaciondedatos.info	
		Rname	ag6601763.gmail.com	
		Serial number	2019120604	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	10800	

Domain bestrate.ie

bestrate / ie / Subdomains

record type	TTL	value		
A	3600	160.153.129.228		
NS	3600	ns3.blacknight.com	Zones on DNS server	162.88.60.11
NS	3600	ns2.blacknight.com	Zones on DNS server	81.17.254.6
NS	3600	ns1.blacknight.com	Zones on DNS server	78.153.212.176
NS	3600	ns4.blacknight.com	Zones on DNS server	162.88.61.11
MX	3600	10 mail.bestrate.ie		
TXT	3600	v=spf1 a include:spf.blacknight.ie ~all		
SOA	3600	Mname	ns1.blacknight.com	
		Rname	hostmaster.blacknight.com	
		Serial number	1270161890	
		Refresh	14400	
		Retry	7200	
		Expire	2419200	
		Minimum TTL	3600	

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

Certificados

Criteria	Identity = 'rayansazehco.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2054966570	2019-10-30	2019-10-30	2020-01-28	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2054968501	2019-10-30	2019-10-30	2020-01-28	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN CN=actualizaciondedatos.info

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 281961388999848251947348712521029149236669

Validity 2019-11-21 05:45:22 **to** 2020-02-19 05:45:22 (90 days, 0:00:00)

Names actualizaciondedatos.info
www.actualizaciondedatos.info

Subject DN CN=bancoestado.actualizaciondedatos.info

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 268937618864683190919194758784446212184330

Validity 2019-12-06 16:02:20 **to** 2020-03-05 16:02:20 (90 days, 0:00:00)

Names bancoestado.actualizaciondedatos.info

Subject DN CN=banco-estado.actualizaciondedatos.info

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 303793013133208371966257124180278910032929

Validity 2019-12-06 16:12:05 **to** 2020-03-05 16:12:05 (90 days, 0:00:00)

Names banco-estado.actualizaciondedatos.info

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

IP

5.61.24.202

82.194.70.31

160.153.129.228

Network information

IP address	5.61.24.202
Reverse DNS (PTR record)	5-61-24-202.nrp.co
DNS server (NS record)	ns1.nrp.co (5.61.28.48) ns2.nrp.co (5.61.27.8) ns3.nrp.co (5.61.24.24)
ASN number	58262
ASN name (ISP)	Negah Roshan Pars Company (PJS)
IP-range/subnet	5.61.24.0/24 5.61.24.0 - 5.61.24.255

Domain actualizaciondedatos.info is located on IP address << 82.194.70.31 >>

Block start	82.194.70.0
End of block	82.194.70.255
Block size	256 Domains in block
Block name	Hostalia-DL-2
AS number	16371
Parent block	82.194.64.0 - 82.194.95.255
Organization	Hostalia-DL-2
City	Madrid
Region/State	Madrid, Comunidad de
Country	ES , Spain
Host name	hs-1610.servidores-dedicados.es
Domains	1 actualizaciondedatos.info

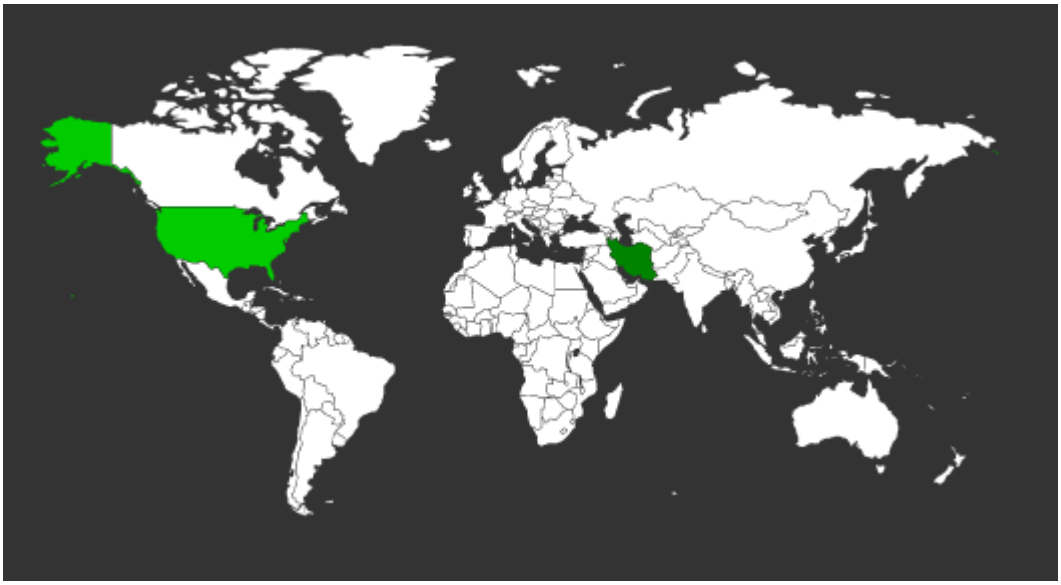
Domain bestrate.ie is located on IP address
<< 160.153.129.228 >>

Block start	160.153.0.0
End of block	160.153.255.255
Block size	65536 Domains in block
Block name	GO-DADDY-COM-LLC
AS number	26496
Parent block	160.0.0.0 - 160.255.255.255
Organization	GoDaddy.com, LLC
City	Scottsdale
Region/State	Arizona
Country	US , United States
Reg. date	2011-09-01
Host name	ip-160-153-129-228.ip.secureserver.net
Web server	Apache/2.4.23

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

Localización

Rasht, Gilan, Iran



Belfast, Northern Ireland, United Kingdom

Scottsdale, Arizona, United States

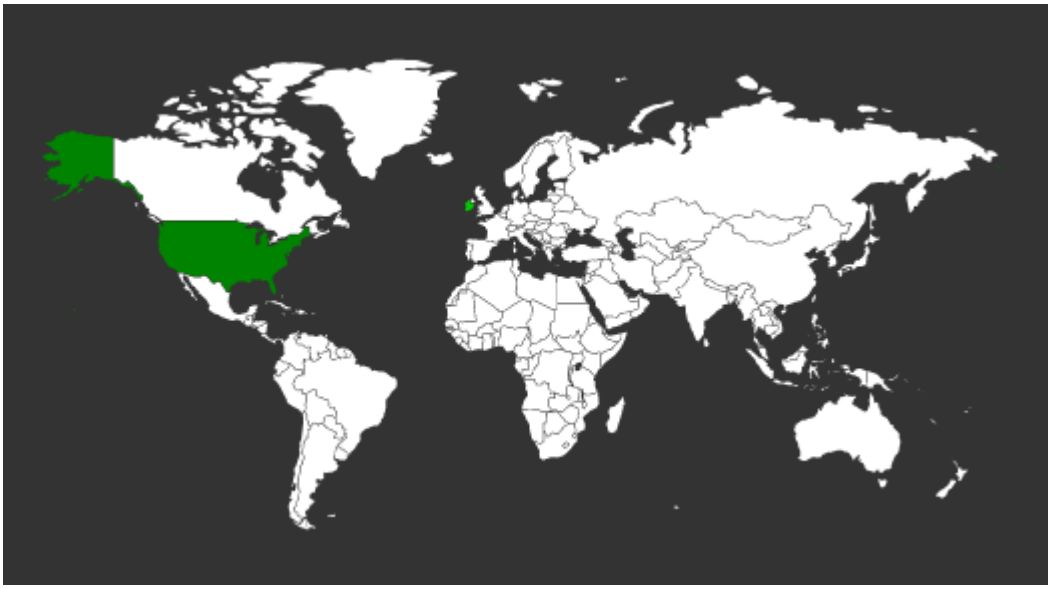
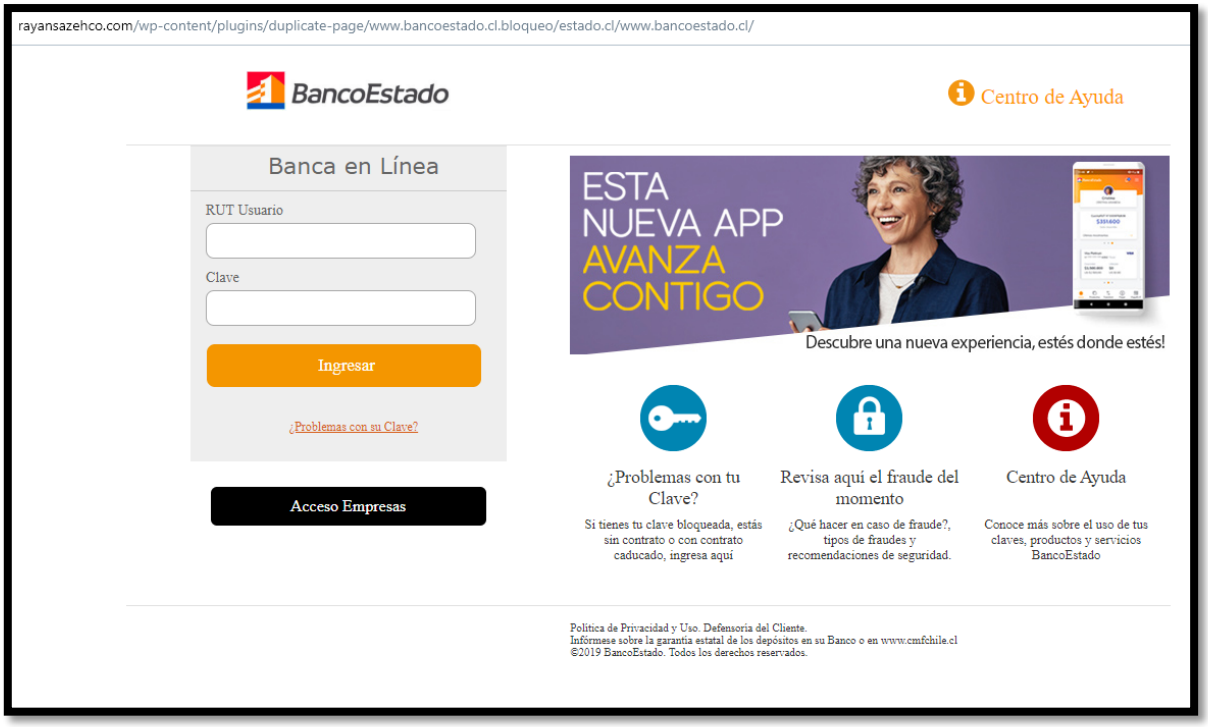
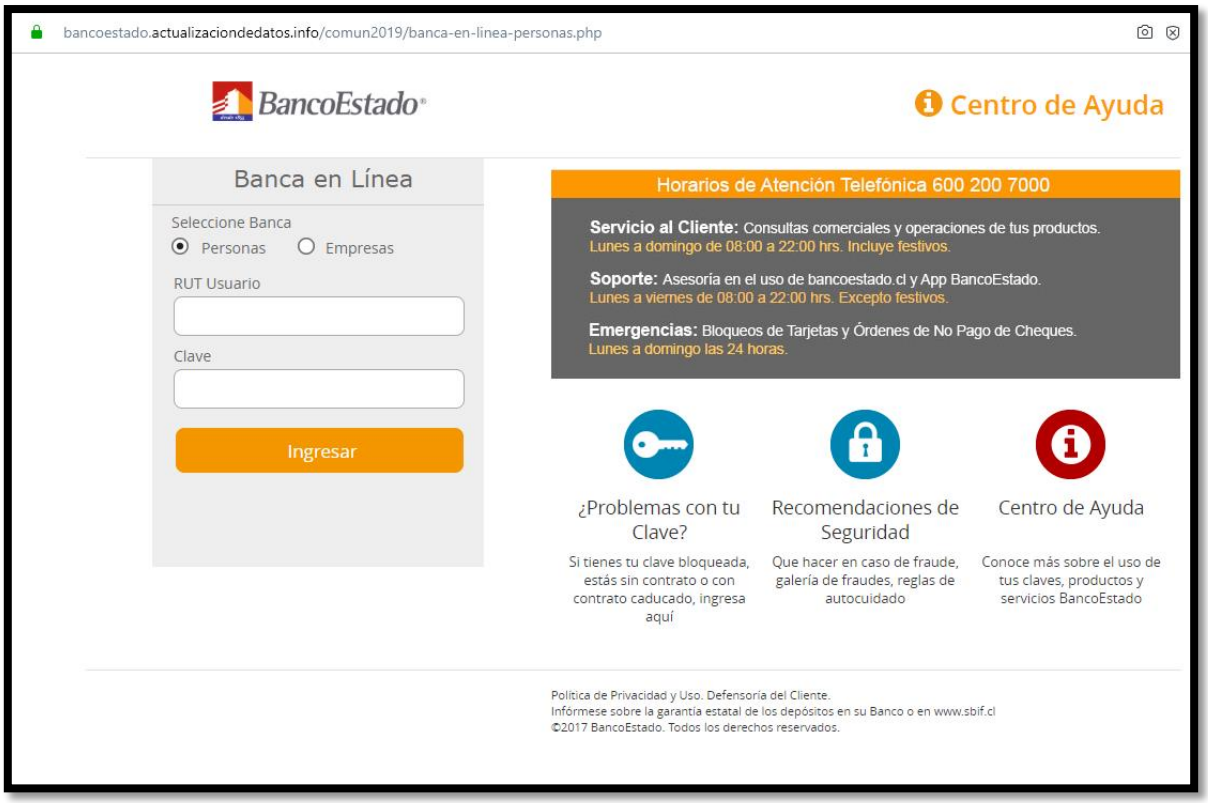
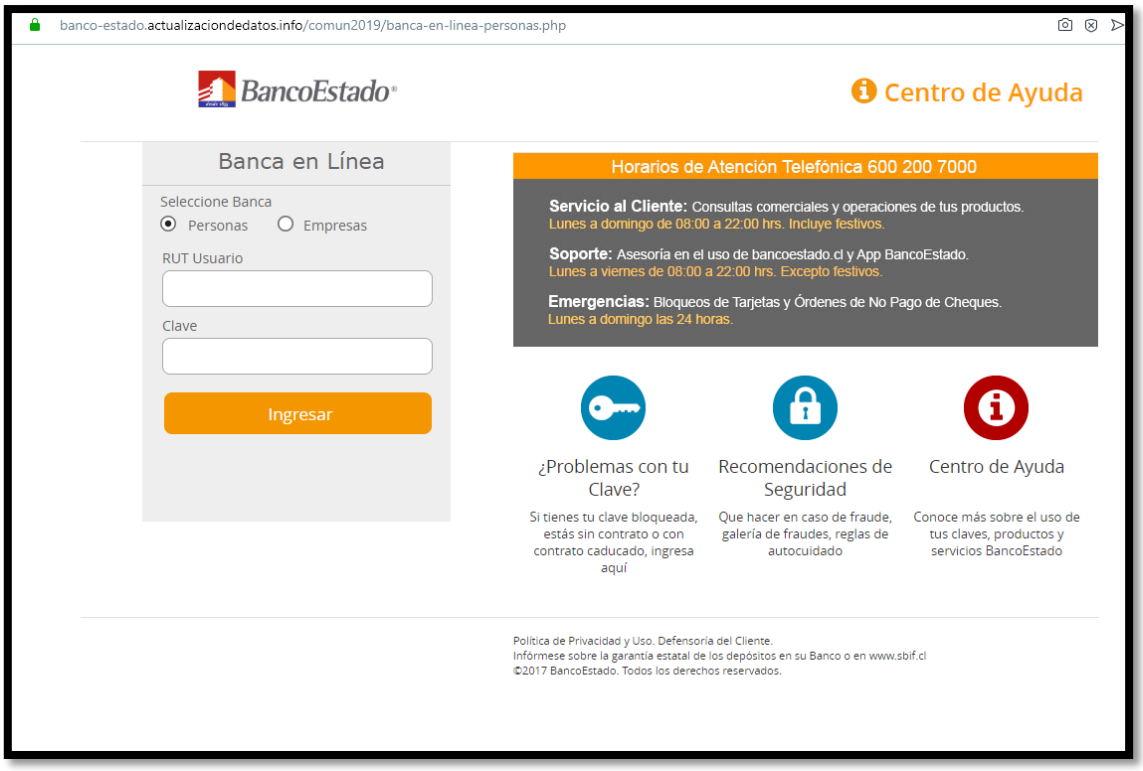
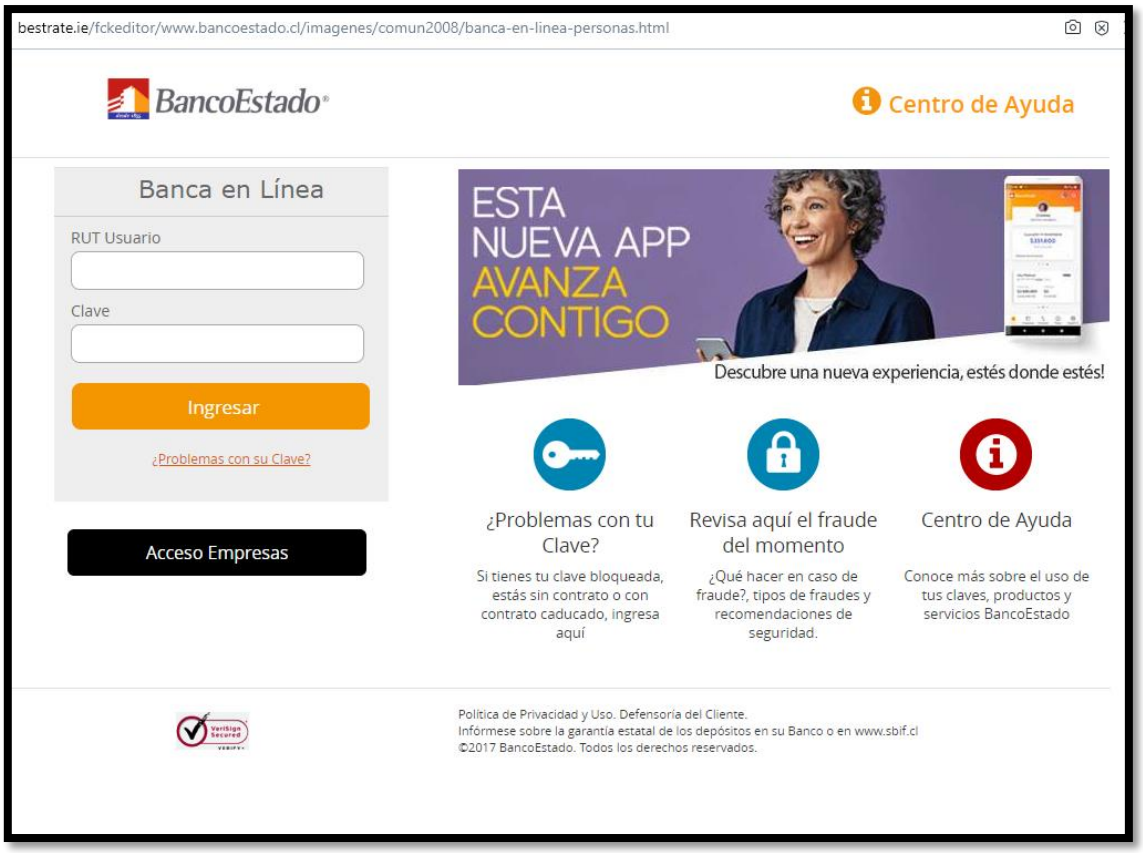


Imagen del sitio






banco-estado.actualizaciondedatos.info/comun2019/banca-en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
Seleccione Banca
Personas
Empresas
RUT Usuario
Clave
Ingresar
Horarios de Atención Telefónica 600 200 7000
Servicio al Cliente: Consultas comerciales y operaciones de tus productos.
Lunes a domingo de 08:00 a 22:00 hrs. Incluye festivos.
Soporte: Asesoría en el uso de bancoestado.cl y App BancoEstado.
Lunes a viernes de 08:00 a 22:00 hrs. Excepto festivos.
Emergencias: Bloqueos de Tarjetas y Órdenes de No Pago de Cheques.
Lunes a domingo las 24 horas.
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Recomendaciones de Seguridad
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado
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.


bestrate.ie/fckeditor/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
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.sbif.cl
©2017 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: rayansazehco.com
Registry Domain ID: 2349067727_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.webnic.cc
Registrar URL: webnic.cc
Updated Date: 2019-01-02T08:13:19Z
Creation Date: 2019-01-02T08:13:22Z
Registrar Registration Expiration Date: 2021-01-02T08:13:20Z
Registrar: WEBCC
Registrar IANA ID: 460
Registrar Abuse Contact Email: compliance_abuse@webnic.cc
Registrar Abuse Contact Phone: +60.389966799
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Whoisprotection.cc
Registrant Street: L4-E-2, Level 4, Enterprise 4, Technology Park Malaysia, Buki
t Jalil
Registrant City: Kuala Lumpur
Registrant State/Province: Wilayah Persekutuan
Registrant Postal Code: 57000
Registrant Country: Malaysia
Registrant Phone: +60.389966788
Registrant Phone Ext:
Registrant Fax: +60.389966788
Registrant Fax Ext:
Registrant Email: reg_15633664@whoisprotection.cc
Registry Admin ID: Not Available From Registry
Admin Name: Domain Admin
Admin Organization: Whoisprotection.cc
Admin Street: L4-E-2, Level 4, Enterprise 4, Technology Park Malaysia, Bukit Jal
il
Admin City: Kuala Lumpur
Admin State/Province: Wilayah Persekutuan
Admin Postal Code: 57000
Admin Country: Malaysia
Admin Phone: +60.389966788
Admin Phone Ext:
Admin Fax: +60.389966788
Admin Fax Ext:
Admin Email: adm_15633664@whoisprotection.cc
Registry Tech ID: Not Available From Registry
Tech Name: Domain Admin
Tech Organization: Whoisprotection.cc
Tech Street: L4-E-2, Level 4, Enterprise 4, Technology Park Malaysia, Bukit Jali
l
Tech City: Kuala Lumpur
Tech State/Province: Wilayah Persekutuan
Tech Postal Code: 57000
Tech Country: Malaysia
Tech Phone: +60.389966788
Tech Phone Ext:
Tech Fax: +60.389966788
Tech Fax Ext:
Tech Email: tec_15633664@whoisprotection.cc
Name Server: NS1.PARSDEV.NET
Name Server: NS2.PARSDEV.NET
Name Server: NS3.PARSDEV.NET
Name Server: NS4.PARSDEV.NET
DNSSEC: unsigned
```

```
Domain Name: ACTUALIZACIONDEDATOS.INFO
Registry Domain ID: D503300001182325570-LRMS
Registrar WHOIS Server:
Registrar URL: www.openprovider.nl
Updated Date: 2019-11-21T06:39:32Z
Creation Date: 2019-11-20T22:16:15Z
Registry Expiry Date: 2020-11-20T22:16:15Z
Registrar Registration Expiration Date:
Registrar: Hosting Concepts B.V. dba Openprovider
Registrar IANA ID: 1647
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Registrant Organization: Whois Privacy Protection Foundation
Registrant State/Province: Zuid-Holland
Registrant Country: NL
Name Server: NS1.ACTUALIZACIONES-COL.COM
Name Server: NS2.ACTUALIZACIONES-COL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2019-12-06T19:15:37Z <<<

% Rights restricted by copyright; http://iedr.ie/index.php/mnudomregs/mnudnssearch/96
% Do not remove this notice

Domain:                 bestrate.ie
Domain Holder:          SKYTEL NETWORKS IRELAND LIMITED
Admin-c:                AAO361-IEDR
Tech-c:                 AAM456-IEDR
Account Name:           Blacknight.ie
Registrar Abuse Contact: abuse@blacknight.com
Registration Date:      22-May-2008
Renewal Date:           22-May-2023
Holder-type:            Billable
Locked status:          NO
Renewal status:         Active
In-zone:                1
Nserver:                ns1.blacknight.com
Nserver:                ns2.blacknight.com
Nserver:                ns3.blacknight.com
Nserver:                ns4.blacknight.com
```

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: 2019.12.08 18:04:46 -03'00'