Alerta de seguridad informática	8FFR20-00261-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 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

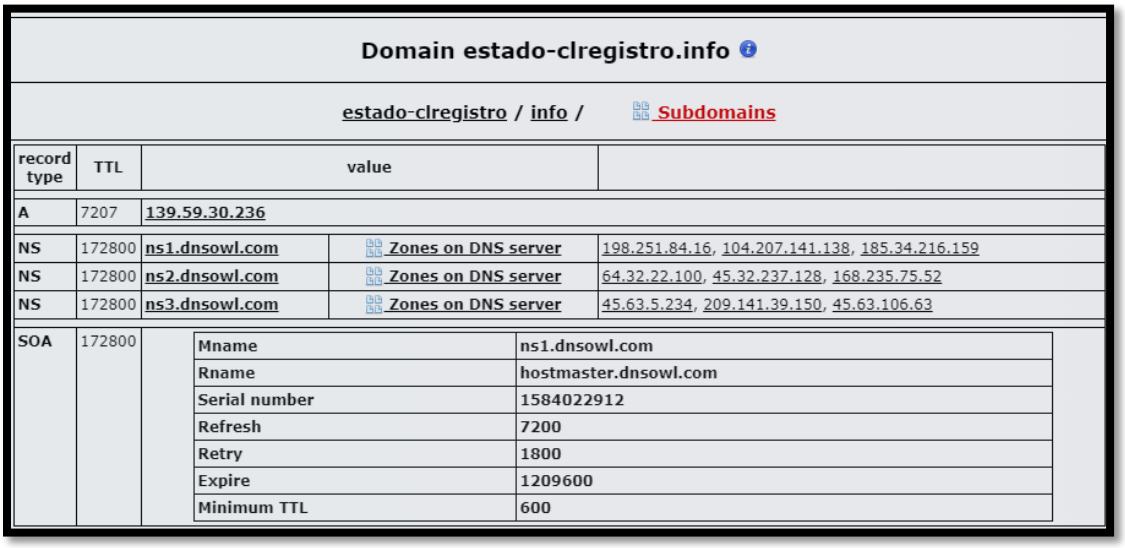
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociado a tres IPs que suplantan el sitio web oficial del Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

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

estado-registrocl[.]site/portada[.]html
estado-registrocl[.]site/personas/comun2008/banca-en-linea-personas[.]html
acceso[.]bacoestado[.]digital
acceso[.]bacoestado[.]digital/inicio



Domain estado-clregistro.info

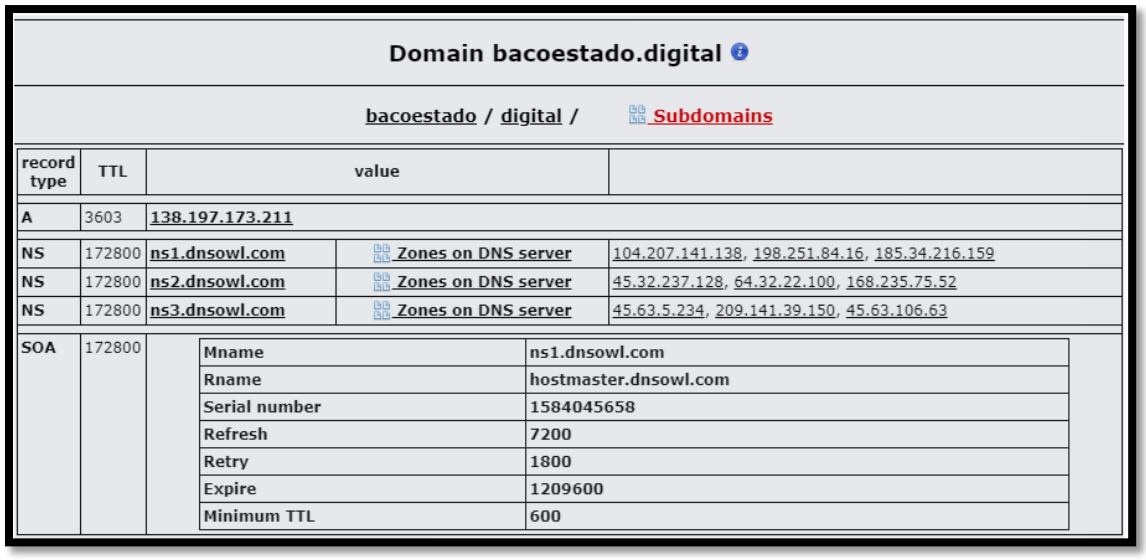
estado-clregistro / info / Subdomains

record type	TTL	value		
A	7207	139.59.30.236		
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, 45.32.237.128, 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	1584022912	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain acceso.bacoestado.digital

acceso / bacoestado / digital / Subdomains

record type	TTL	value
A	3603	138.197.173.211



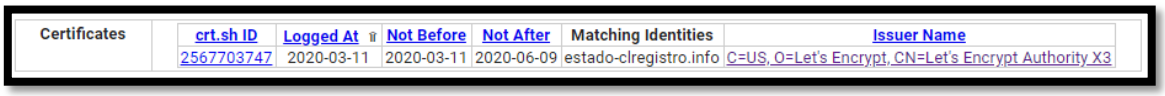
Domain bacoestado.digital

bacoestado / digital / Subdomains

record type	TTL	value		
A	3603	138.197.173.211		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 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	1584045658	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

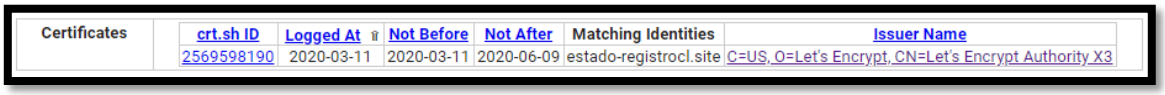
Ilustración 1 Dominio donde se Aloja Url del Banco Estado Falso y DNS que utilza

Certificados



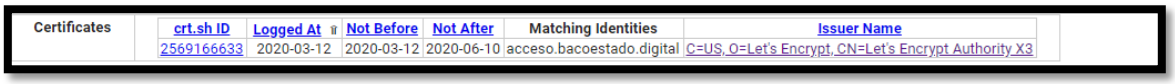
Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2567703747	2020-03-11	2020-03-11	2020-06-09	estado-clregistro.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3



Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2569598190	2020-03-11	2020-03-11	2020-06-09	estado-registrocl.site	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3



Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2569166633	2020-03-12	2020-03-12	2020-06-10	acceso.bacoestado.digital	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP
139[.]59[.]30[.]236
178[.]128[.]115[.]229
138[.]197[.]173[.]211

Domain estado-clregistro.info is located on IP address << 139.59.30.236 >>	
Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC

Domain estado-registrocl.site is located on IP address << 178.128.115.229 >>	
Block start	178.128.112.0
End of block	178.128.127.255
Block size	4096 Domains in block
Block name	DIGITALOCEAN
AS number	14061
Parent block	178.128.0.0 - 178.128.255.255
Organization	

Domain acceso.bacoestado.digital is located on IP address << 138.197.173.211 >>

Block start	138.197.0.0
End of block	138.197.255.255
Block size	65536 Domains in block
Block name	DIGITALOCEAN-16
AS number	14061
Parent block	138.0.0.0 - 138.255.255.255
Organization	Digital Ocean, Inc.

Localización
Bengaluru, Karnataka, India
Singapur, Singapur
New York City, New York, Estados Unidos

Location	Bengaluru, Karnataka, India (IN)
Latitude and Longitude	12.97, 77.59

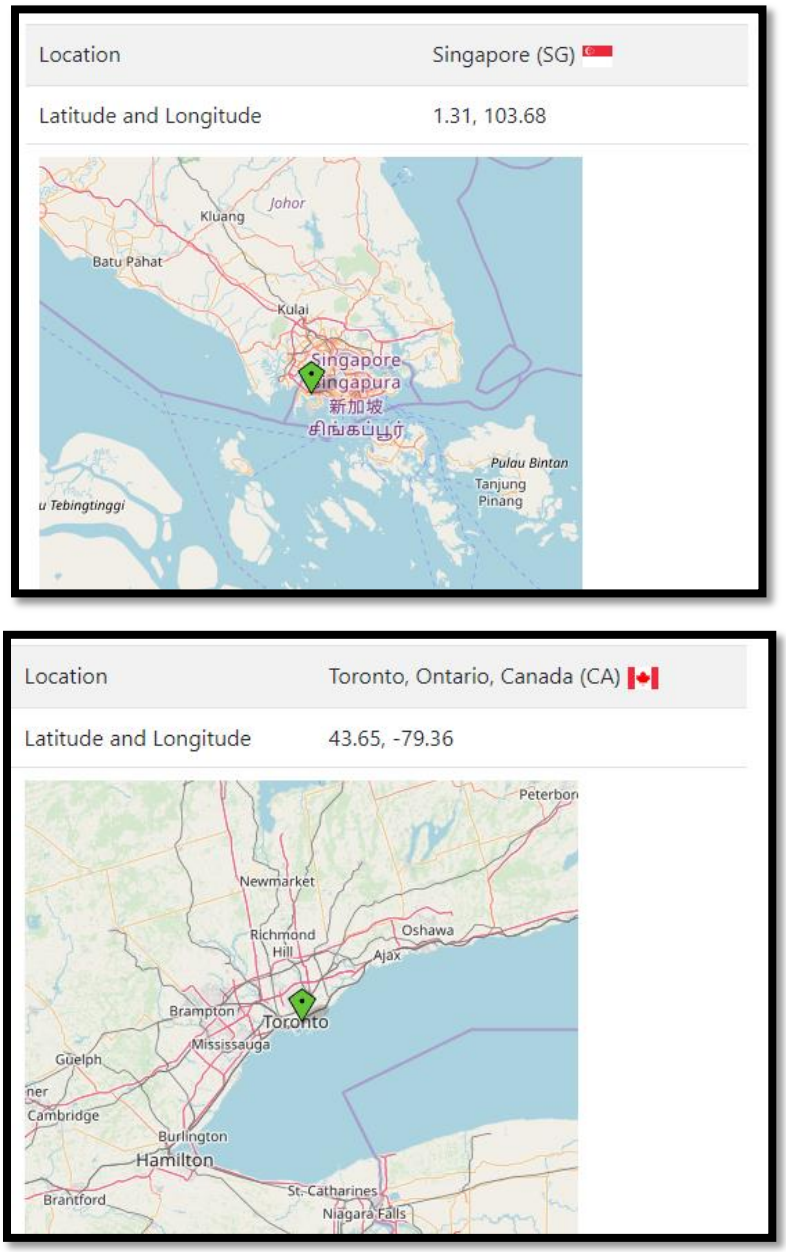
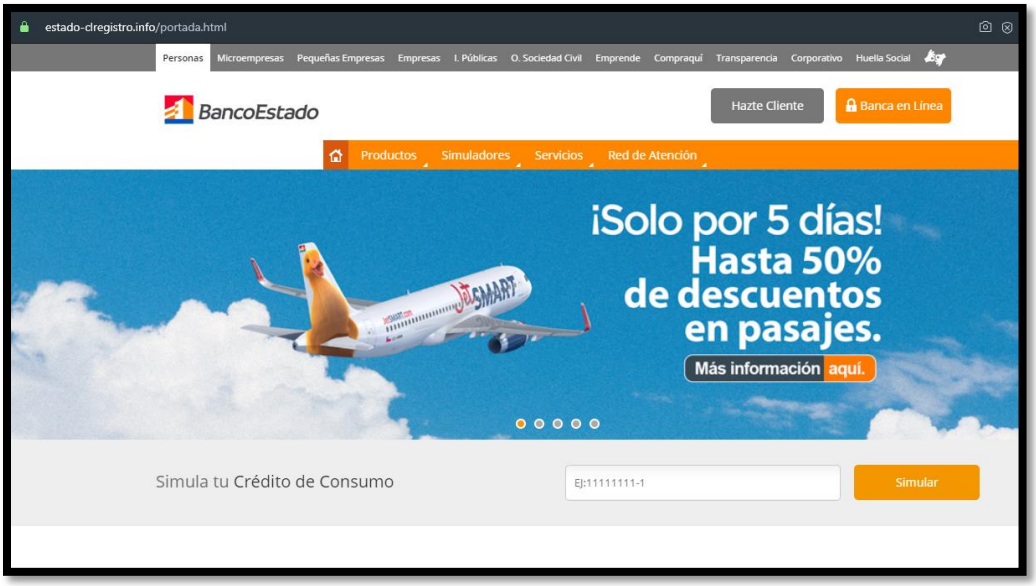
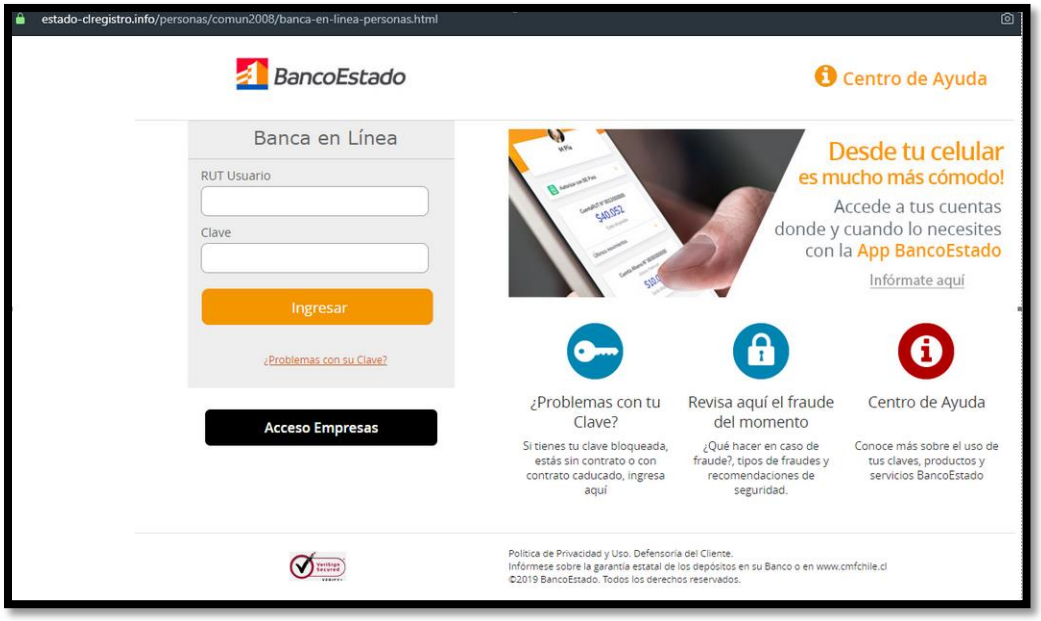
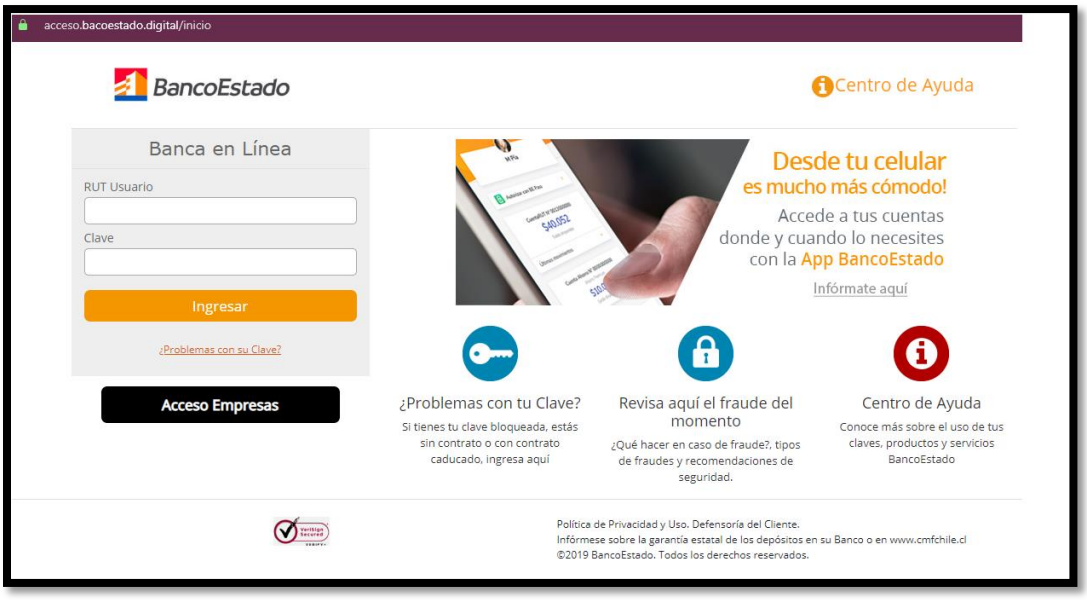


Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Imagen del sitio






acceso.bacoestado.digital/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 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.

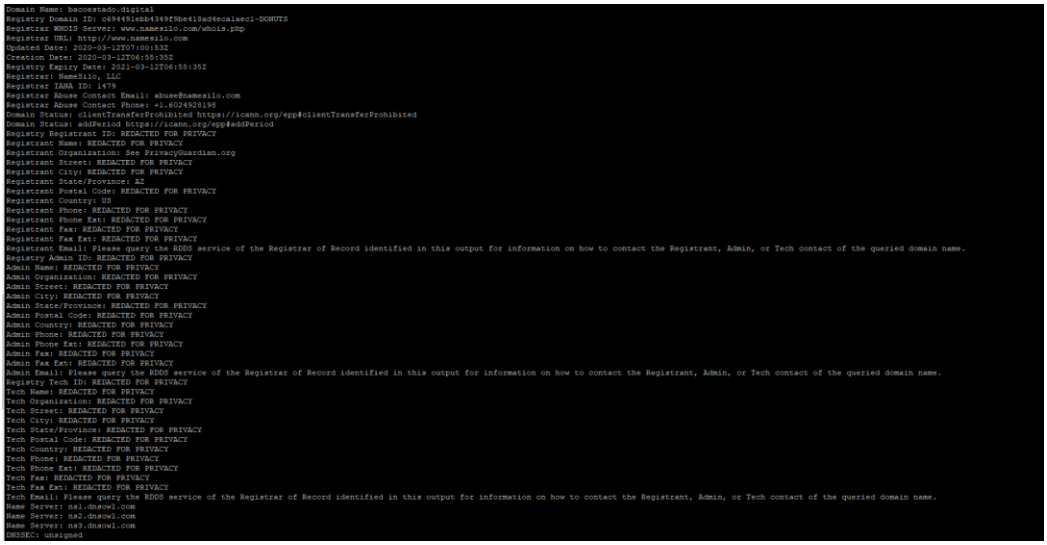
Whois

```
Domain Name: estado-clregistro.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-12T07:00:00Z
Creation Date: 2020-03-11T07:00:00Z
Registrar Registration Expiration Date: 2021-03-11T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
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-e242e2b640e9824f8fbe61f1923dde4b@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-e242e2b640e9824f8fbe61f1923dde4b@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
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-e242e2b640e9824f8fbe61f1923dde4b@privacyguardian.org
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: 2020-03-12T07:00:00Z <<<

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

```
Domain Name: estado-clregistro.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-12T07:00:00Z
Creation Date: 2020-03-11T07:00:00Z
Registrar Registration Expiration Date: 2021-03-11T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
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-e242e2b640e9824f8fbe61f1923dde4b@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-e242e2b640e9824f8fbe61f1923dde4b@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
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-e242e2b640e9824f8fbe61f1923dde4b@privacyguardian.org
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: 2020-03-12T07:00:00Z <<<

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



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: 2020.03.13 09:55:31 -03'00'