Alerta de seguridad informática	8FFR20-00266-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 una IP que suplanta 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

www[.]estadochileapp[.]com

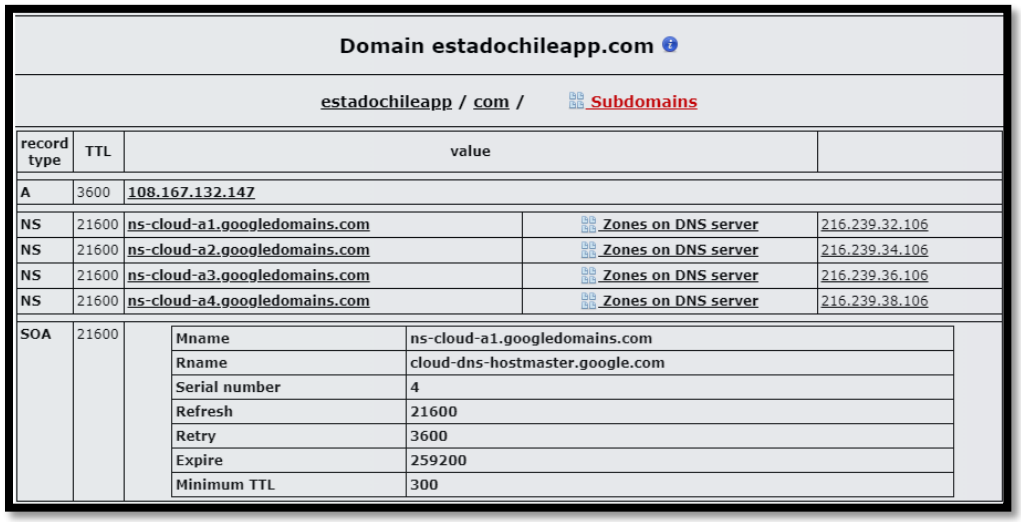
www[.]estadochileapp[.]com/site/control[.]php

www[.]verificaciones-estado[.]xyz

www[.]verificaciones-estado[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]php?html

estado-portal[.]info

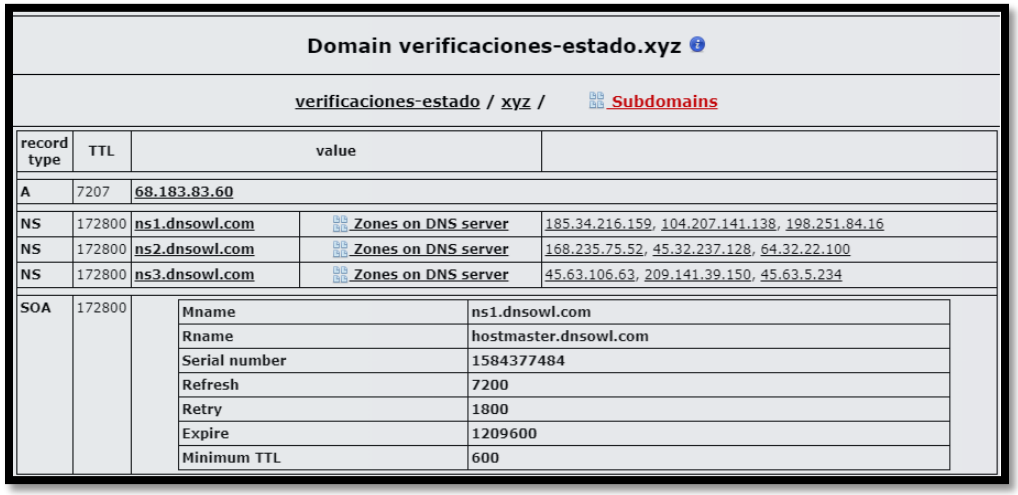
estado-portal[.]info/personas/comun2008/banca-en-linea-personas[.]html



Domain estadochileapp.com

estadochileapp / com / Subdomains

record type	TTL	value		
A	3600	108.167.132.147		
NS	21600	ns-cloud-a1.googledomains.com	Zones on DNS server	216.239.32.106
NS	21600	ns-cloud-a2.googledomains.com	Zones on DNS server	216.239.34.106
NS	21600	ns-cloud-a3.googledomains.com	Zones on DNS server	216.239.36.106
NS	21600	ns-cloud-a4.googledomains.com	Zones on DNS server	216.239.38.106
SOA	21600	Mname: ns-cloud-a1.googledomains.com Rname: cloud-dns-hostmaster.google.com Serial number: 4 Refresh: 21600 Retry: 3600 Expire: 259200 Minimum TTL: 300		



Domain verificaciones-estado.xyz

verificaciones-estado / xyz / Subdomains

record type	TTL	value		
A	7207	68.183.83.60		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 45.32.237.128, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234
SOA	172800	Mname: ns1.dnsowl.com Rname: hostmaster.dnsowl.com Serial number: 1584377484 Refresh: 7200 Retry: 1800 Expire: 1209600 Minimum TTL: 600		

Domain estado-portal.info

estado-portal / info / Subdomains

record type	TTL	value		
A	7207	178.128.123.25		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
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, 45.63.106.63, 209.141.39.150
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1584378398	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2577935573	2020-03-14	2020-03-14	2020-06-12	estadochileapp.com www.estadochileapp.com	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
2586099874	2020-03-14	2020-03-14	2020-06-12	www.verificaciones-estado.xyz	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2576046751	2020-03-14	2020-03-14	2020-06-12	www.verificaciones-estado.xyz	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
2583771044	2020-03-16	2020-03-16	2020-06-14	estado-portal.info	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 1 Certificado Utilizado en Url del sitio Falso del Banco Estado

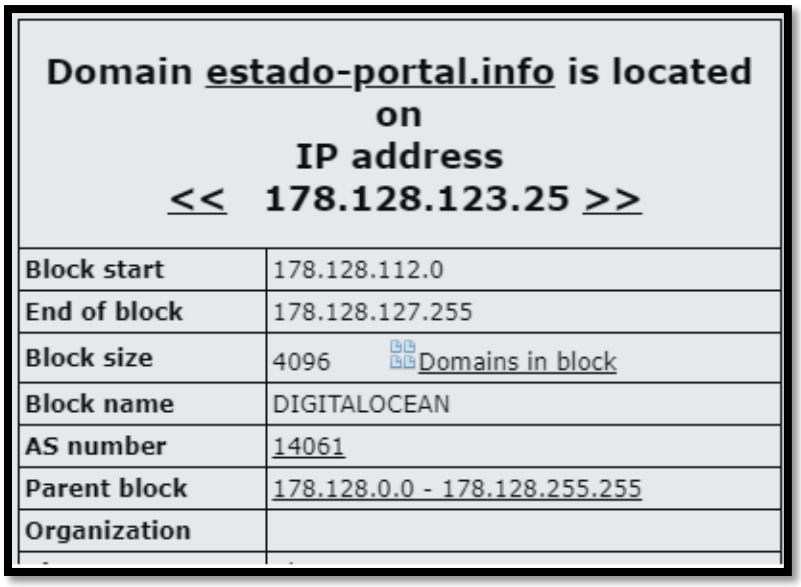
IP
108[.]167[.]132[.]147
68[.]183[.]83[.]60
178[.]128[.]123[.]25

Domain www.estadochileapp.com is located on IP address << 108.167.132.147 >>

Block start	108.167.128.0
End of block	108.167.191.255
Block size	16384 Domains in block
Block name	HGBLOCK-4
AS number	46606
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM

Domain www.verificaciones-estado.xyz is located on IP address << 68.183.83.60 >>

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



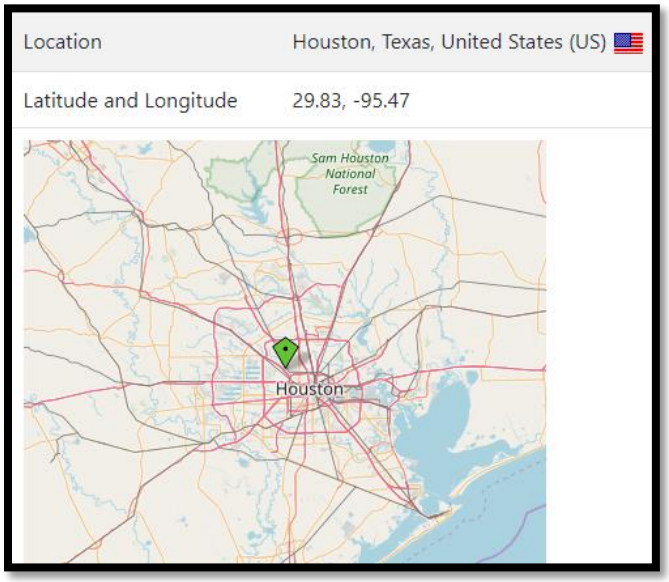
Domain estado-portal.info is located on IP address << 178.128.123.25 >>

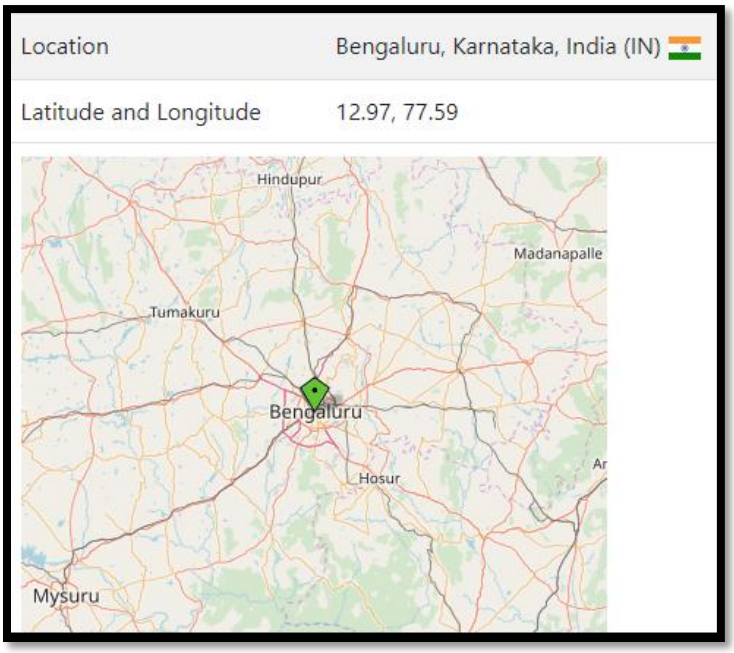
Block start	178.128.112.0
End of block	178.128.127.255
Block size	4096 Domains in block
Block name	DIGITALOCEAN
AS number	14061
Parent block	178.128.0.0 - 178.128.255.255
Organization	

Ilustración 1 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Houston, Texas, Estados Unidos
Bengaluru, Karkataka, India
Singapur, Singapur




Location
Bengaluru, Karnataka, India (IN)
Latitude and Longitude
12.97, 77.59
Hindupur
Madanapalle
Tumakuru
Bengaluru
Hosur
Mysuru

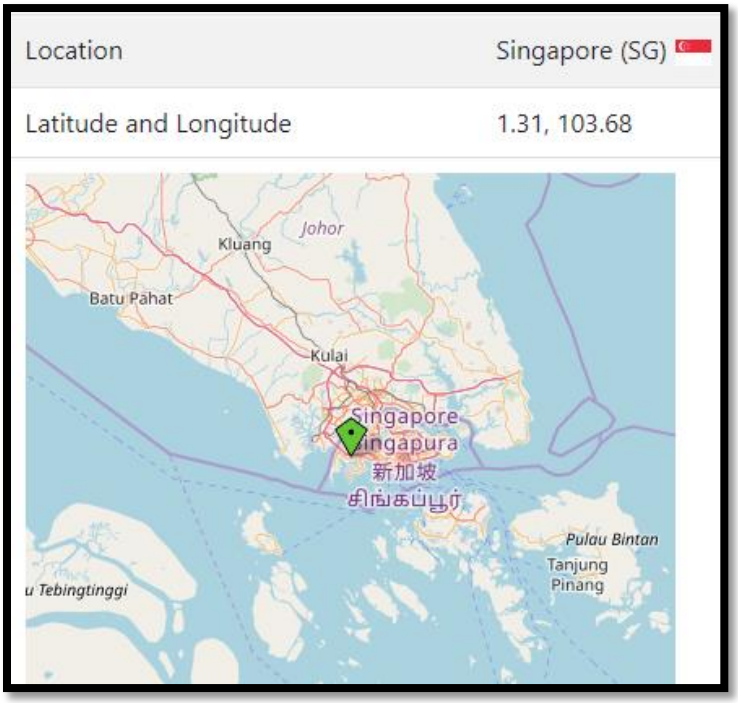
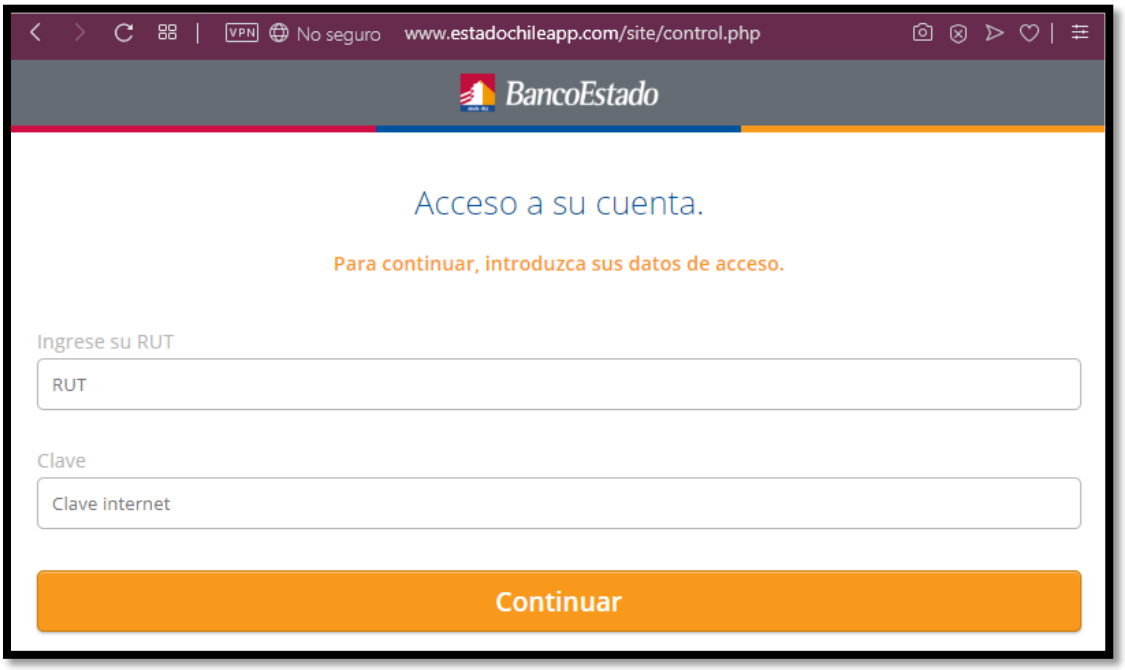
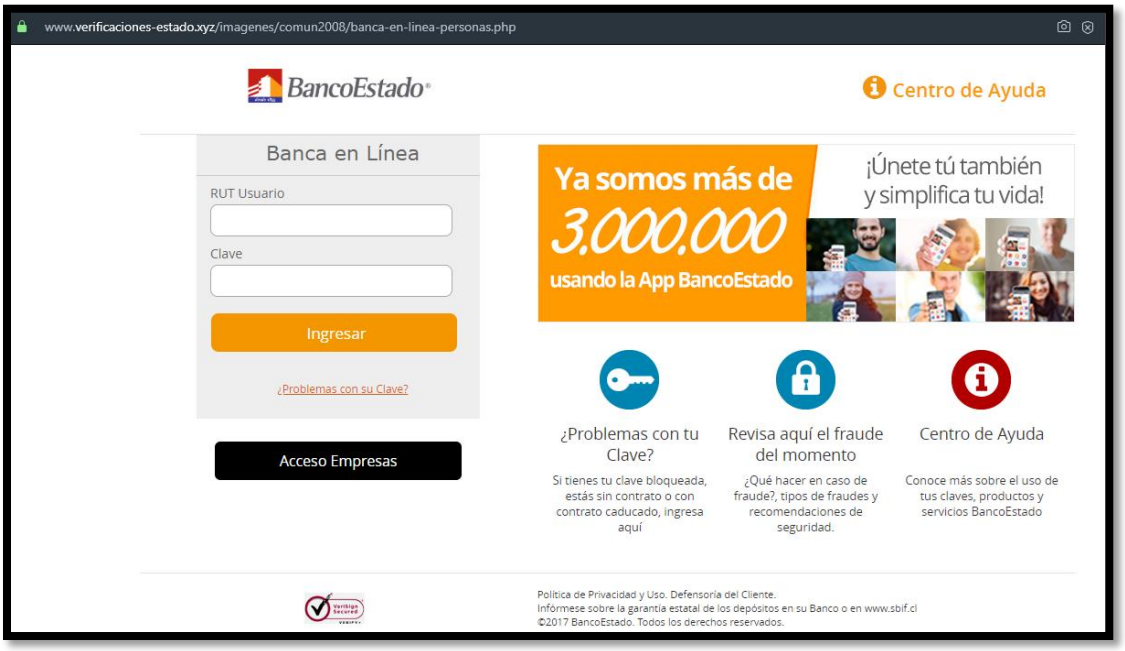
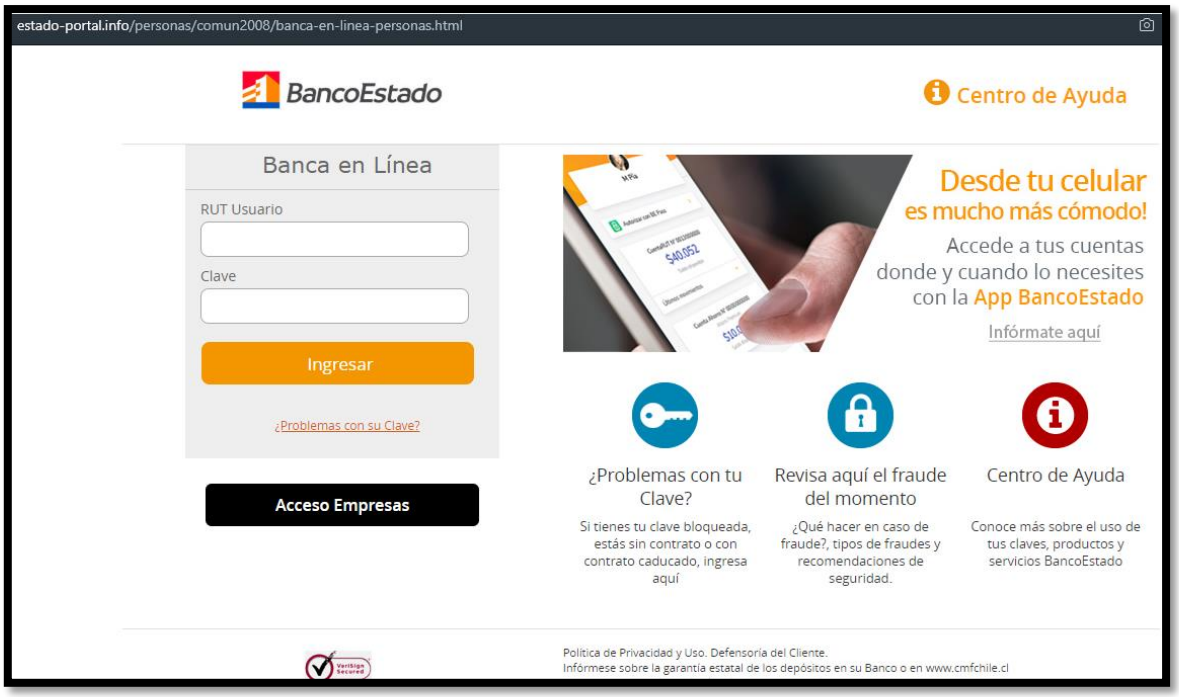

Location
Singapore (SG)
Latitude and Longitude
1.31, 103.68
Johor
Kluang
Batu Pahat
Kulai
Singapore
新加坡
சிங்கப்பூர்
Pulau Bintan
Tanjung
Pinang

Imagen del sitio






estado-portal.info/personas/comun2008/banca-en-linea-personas.html
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

Whois

```
Domain Name: estadochileapp.com
Registry Domain ID: 2503241940_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-14T17:02:10Z
Creation Date: 2020-03-14T17:02:08Z
Registrar Registration Expiration Date: 2021-03-14T17:02:08Z
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#clientTransfer
Prohibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246676373
Registrant Organization: Contact Privacy Inc. Customer 1246676373
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: pwlef8uajso3@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246676373
Admin Organization: Contact Privacy Inc. Customer 1246676373
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: pwlef8uajso3@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246676373
Tech Organization: Contact Privacy Inc. Customer 1246676373
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: pwlef8uajso3@contactprivacy.email
Name Server: NS-CLOUD-A1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A4.GOOGLEDOMAINS.COM
DNSSEC: signedDelegation
```

```
Domain Name: verificaciones-estado.xyz
Registry Domain ID: D178760064-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-14T07:00:00Z
Creation Date: 2020-03-14T07:00:00Z
Registrar Registration Expiration Date: 2021-03-14T07:00:00Z
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: 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-012e41eda10892ccb4315c11cf712fe5@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-012e41eda10892ccb4315c11cf712fe5@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-012e41eda10892ccb4315c11cf712fe5@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: estado-portal.info
Registry Domain ID: D503300001183536188-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-16T07:00:00Z
Creation Date: 2020-03-15T07:00:00Z
Registrar Registration Expiration Date: 2021-03-15T07:00:00Z
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: 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-4c1b8d5195129e61e9475178a7c80c64@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-4c1b8d5195129e61e9475178a7c80c64@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-4c1b8d5195129e61e9475178a7c80c64@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.17 07:31:19 -03'00'