Alerta de seguridad informática	**8FFR-00093-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**16 de Octubre de 2019**
Última revisión	**16 de Octubre 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 un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de **Banco Estado**, lo 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

https[://]www[.]banccoestado[.]xyz
https[://]www[.]banccoestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php
http[://]banco[.]estado[.]in/comun2019
https[://]turismoenperuviajes[.]com/wp-content/cl/

URL Redirector:

https[://]foaminsulationshop[.]com/wp-content/afysag/

Domain banccoestado.xyz

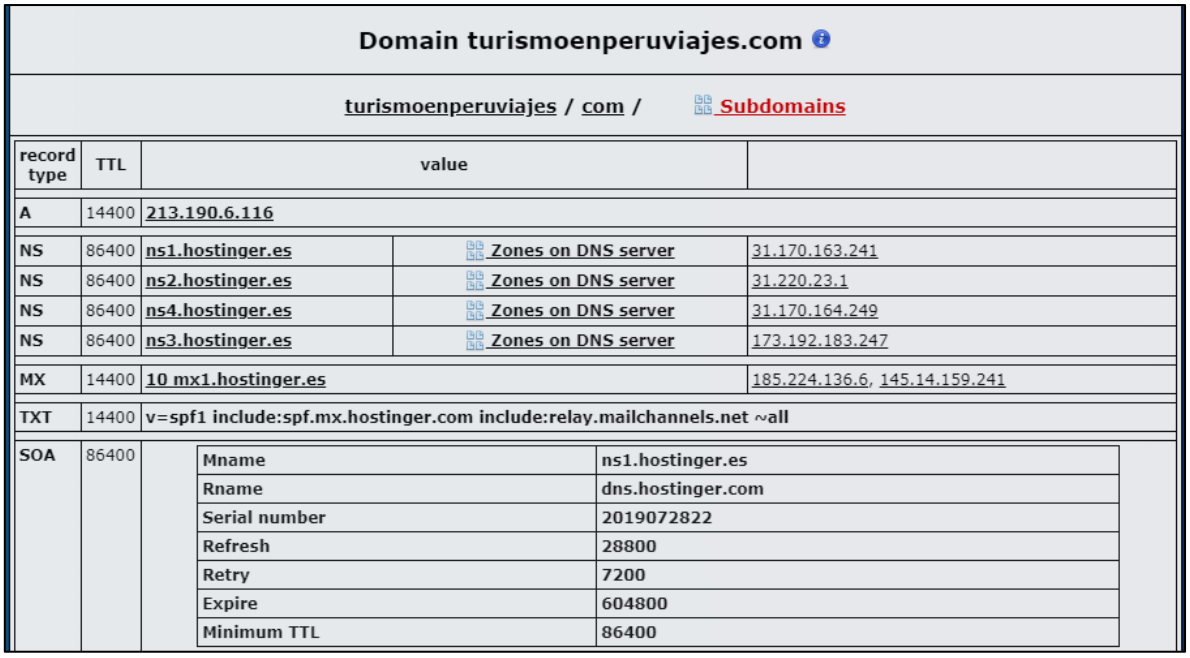
banccoestado / xyz / Subdomains

record type	TTL	value		
A	7207	139.59.37.14		
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	45.32.237.128, 64.32.22.100, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1571145598	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain estado.in

estado / in / Subdomains

record type	TTL	value		
A	600	47.254.25.68		
NS	600	c.dnspod.com	Zones on DNS server	119.28.48.231, 180.163.8.114
NS	600	a.dnspod.com	Zones on DNS server	101.226.79.205, 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	1571143832	
		Refresh	3600	
		Retry	180	
		Expire	1209600	
		Minimum TTL	180	



Domain turismoenperuviajes.com

turismoenperuviajes / com / Subdomains

record type	TTL	value		
A	14400	213.190.6.116		
NS	86400	ns1.hostinger.es	Zones on DNS server	31.170.163.241
NS	86400	ns2.hostinger.es	Zones on DNS server	31.220.23.1
NS	86400	ns4.hostinger.es	Zones on DNS server	31.170.164.249
NS	86400	ns3.hostinger.es	Zones on DNS server	173.192.183.247
MX	14400	10 mx1.hostinger.es		185.224.136.6, 145.14.159.241
TXT	14400	v=spf1 include:spf.mx.hostinger.com include:relay.mailchannels.net ~all		
SOA	86400	Mname	ns1.hostinger.es	
		Rname	dns.hostinger.com	
		Serial number	2019072822	
		Refresh	28800	
		Retry	7200	
		Expire	604800	
		Minimum TTL	86400	

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso

IP´s

139[.]59[.]37[.]14

47[.]254[.]25[.]68

213[.]190[.]6[.]116

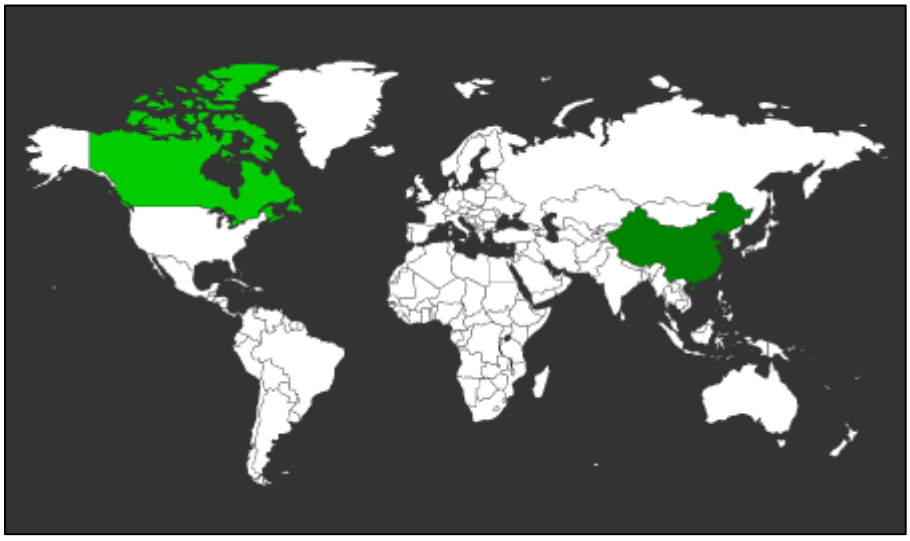
Domain banccoestado.xyz is located on IP address << 139.59.37.14 >>	
Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone
Domains	1 banccoestado.xyz

Domain banco.estado.in is located on IP address << 47.254.25.68 >>	
Block start	47.128.0.0
End of block	47.255.255.255
Block size	8388608 Domains in block
Block name	BNR
AS number	45102
Parent block	47.74.0.0 - 47.255.255.255
Organization	Bell-Northern Research
Country	CA , Canada
Reg. date	2015-05-07
Host name	no record in reverse zone
Domains	1 banco.estado.in

Domain turismoenperuviajes.com is located on IP address << 213.190.6.116 >>	
Block start	213.190.6.0
End of block	213.190.6.255
Block size	256 Domains in block
Block name	HOSTINGER-HOSTING
AS number	47583
Parent block	213.190.4.0 - 213.190.7.255
Organization	ORG-HIL9-RIPE
City	-
Country	
Host name	no record in reverse zone
Domains	1 turismoenperuviajes.com

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización
Singapore
Canada



Certificados

Criteria	Identity = 'www.banccoestado.xyz'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2000589068	2019-10-15	2019-10-15	2020-01-13	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria	Identity = 'estado.in'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
976826741	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976826184	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976823646	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976823540	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976711010	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976710735	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976707051	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
976706952	2018-11-26	2018-11-26	2019-06-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
974215578	2018-11-25	2018-11-25	2019-06-03	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
974215548	2018-11-25	2018-11-25	2019-06-03	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972729906	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972729859	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972535195	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972535131	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972226279	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
972226216	2018-11-24	2018-11-24	2019-06-02	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
969819702	2018-11-23	2018-11-23	2019-06-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
969819598	2018-11-23	2018-11-23	2019-06-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
969270671	2018-11-23	2018-11-23	2019-06-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
969270558	2018-11-23	2018-11-23	2019-06-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
963772115	2018-11-21	2018-11-21	2019-05-30	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
963771911	2018-11-21	2018-11-21	2019-05-30	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
960758740	2018-11-20	2018-11-20	2019-05-29	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
960758756	2018-11-20	2018-11-20	2019-05-29	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
947425945	2018-11-15	2018-11-15	2019-05-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
947425370	2018-11-15	2018-11-15	2019-05-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
923802338	2018-11-06	2018-11-06	2019-05-15	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
923802189	2018-11-06	2018-11-06	2019-05-15	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
917637915	2018-11-04	2018-11-04	2019-05-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
917638042	2018-11-04	2018-11-04	2019-05-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
855742121	2018-10-13	2018-10-13	2019-04-21	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
855741983	2018-10-13	2018-10-13	2019-04-21	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
854894560	2018-10-12	2018-10-12	2019-04-20	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
854893755	2018-10-12	2018-10-12	2019-04-20	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
705772098	2018-09-02	2018-09-02	2019-03-11	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
705771966	2018-09-02	2018-09-02	2019-03-11	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
694372448	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
694372544	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
694372045	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
694372221	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
692202759	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
692202761	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
691864963	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
691864558	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
691859360	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
691859195	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
691858932	2018-08-29	2018-08-29	2019-03-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2

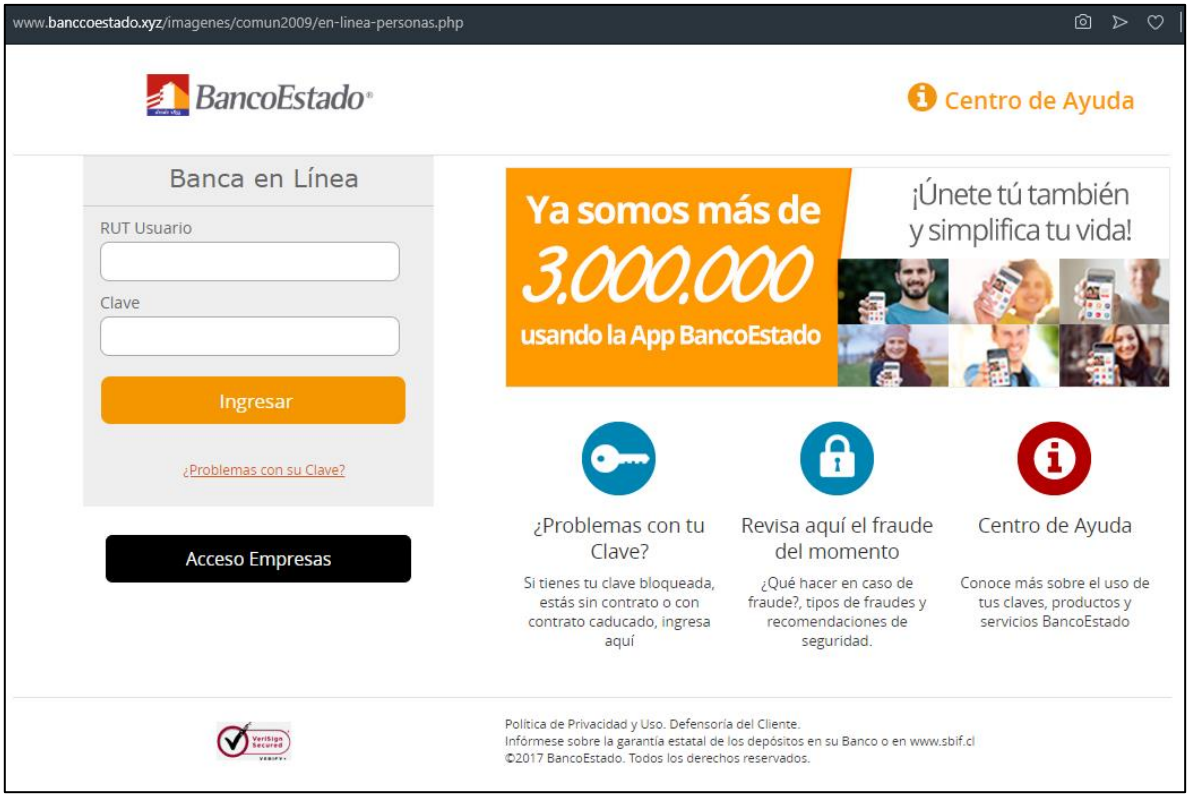
Criteria	Identity = 'turismoenperuviajes.com'

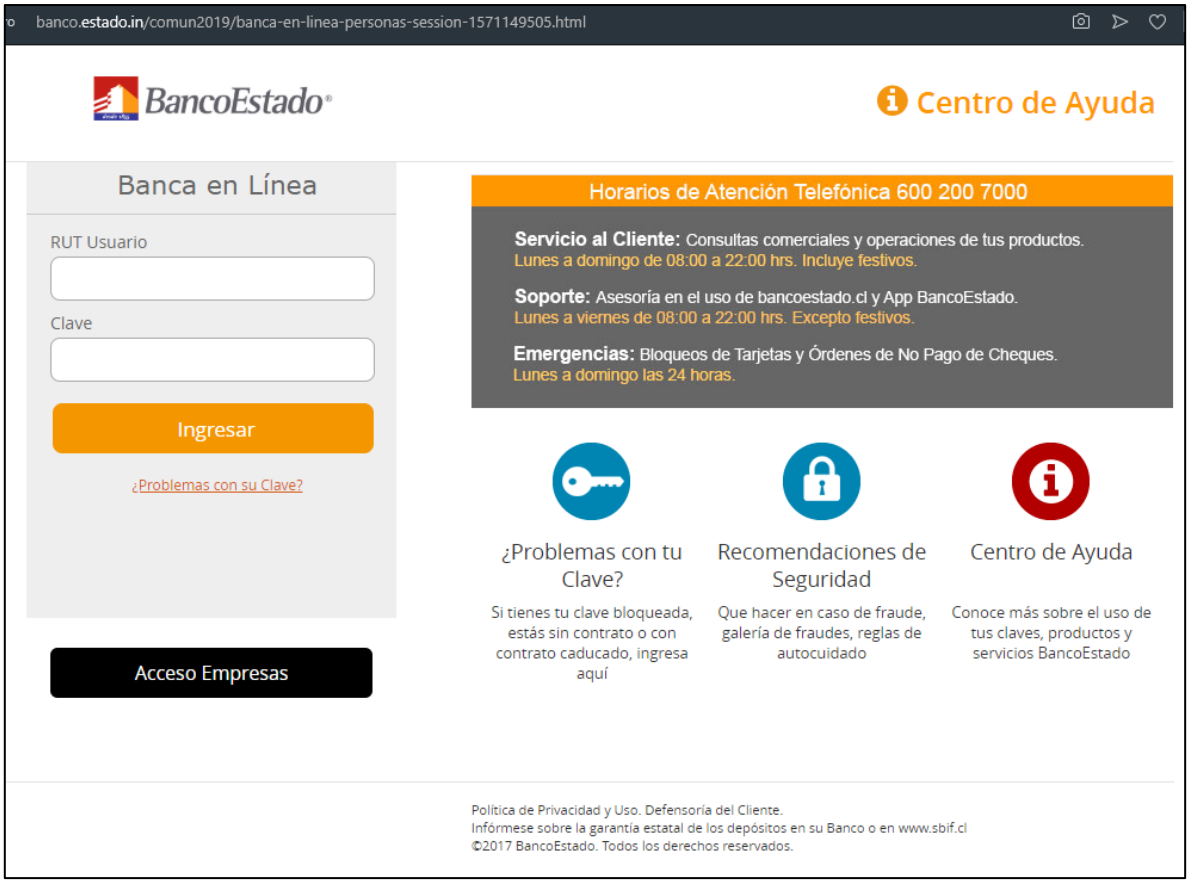
Certificates

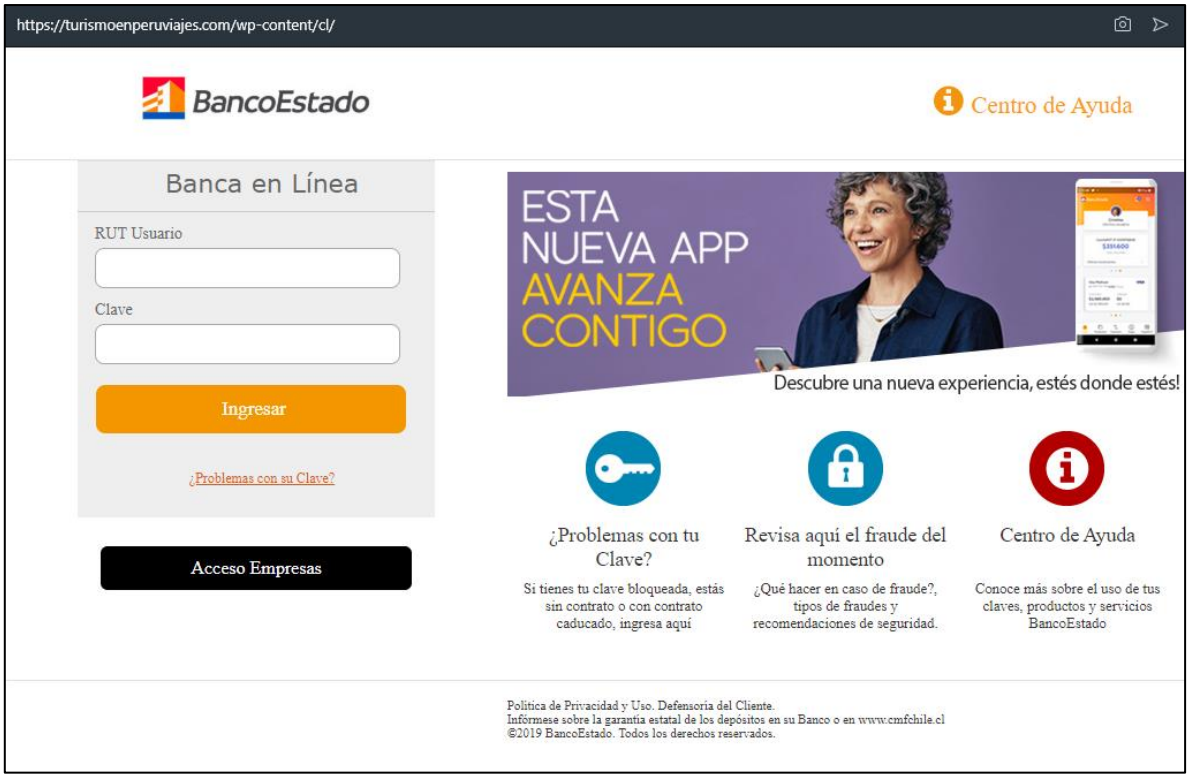
crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1989715284	2019-10-11	2019-10-11	2020-01-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1985331749	2019-10-11	2019-10-11	2020-01-09	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1772079642	2019-08-12	2019-08-12	2019-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1762449003	2019-08-12	2019-08-12	2019-11-10	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 3 Certificado Utilizado en Url del sitio Falso del Banco Estado

Imagen del sitio


www.banccoestado.xyz/imagenes/comun2009/en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿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.


banco.estado.in/comun2019/banca-en-linea-personas-session-1571149505.html
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
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.


https://turismoenperuviajes.com/wp-content/cl/
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.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Whois

```
soc@ITQ-ivps3:~$ whois bancoestado.xyz
Domain Name: BANCOESTADO.XYZ
Registry Domain ID: D100333804-CNIC
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://www.tucows.com/
Updated Date: 2019-08-09T18:43:40.0Z
Creation Date: 2019-04-15T11:35:34.0Z
Registry Expiry Date: 2020-04-15T23:59:59.0Z
Registrar: Tucows.com Co.
Registrar IANA ID: 69
Domain Status: serverHold https://icann.org/epp#serverHold
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Data Protected
Registrant State/Province: ON
Registrant Country: CA
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS1.DOMINIOS.UOL.COM.BR
Name Server: NS2.DOMINIOS.UOL.COM.BR
Name Server: NS3.DOMINIOS.UOL.COM.BR
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2019-10-15T13:41:37.0Z <<<

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

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnic.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://registrar-console.centralnic.com/pub/whois_guidance.
```

```
soc@ITQ-ivps3:~$ whois -h whois.registry.in estado.in
Domain Name: estado.in
Registry Domain ID: D6C2D049931704027AF904CDE4CEF7665-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2019-10-15T12:50:11Z
Creation Date: 2019-10-15T12:46:03Z
Registry Expiry Date: 2020-10-15T12:46:03Z
Registrar: Endurance Domains Technology LLP
Registrar IANA ID: 801217
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferP
rohibited
Domain Status: addPeriod http://www.icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name:
Registrant Organization: N/A
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Victoria
Registrant Postal Code:
Registrant Country: AU
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
```

```
soc@ITQ-ivps3:~$ whois turismoenperuviajes.com
   Domain Name: TURISMOENPERUVIAJES.COM
   Registry Domain ID: 2302310120_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2019-08-26T14:33:43Z
   Creation Date: 2018-08-26T04:58:16Z
   Registry Expiry Date: 2020-08-26T04:58:16Z
   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#clientDeleteProhi
bited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibi
ted
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
   Name Server: NS1.HOSTINGER.ES
   Name Server: NS2.HOSTINGER.ES
   Name Server: NS3.HOSTINGER.ES
   Name Server: NS4.HOSTINGER.ES
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-10-15T16:21:49Z <<<
```

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: 2019.10.16 09:58:05 -03'00'