Alerta de seguridad cibernética	8FFR20-00303-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de abril de 2020
Última revisión	02 de abril 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 asociados a dos 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 COMPROMISO

URL
bancapersonasbancoestado[.]com
estado[.]chileacessomovil[.]com

IP
217[.]182[.]64[.]245
80[.]211[.]29[.]8

DOMINIOS DONDE SE ALOJA URL

Domain bancapersonasbancoestado.com

bancapersonasbancoestado / com / Subdomains

record type	TTL	value		
A	1799	217.182.64.245		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		
SOA	3601	Mname: dns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 1585745966 Refresh: 43200 Retry: 3600 Expire: 604800 Minimum TTL: 3601		

Domain chileacessomovil.com

chileacessomovil / com / Subdomains

record type	TTL	value		
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: 10 Refresh: 21600 Retry: 3600 Expire: 259200 Minimum TTL: 300		

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2653689106	2020-04-01	2020-04-01	2020-06-30	bancapersonasbancoestado.com www.bancapersonasbancoestado.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN	CN=estado.chileacessomovil.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	304341047455002122458335702056374933626649
Validity	2020-03-31 21:17:51 **to** 2020-06-29 21:17:51 (90 days, 0:00:00)
Names	estado.chileacessomovil.com

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain bancapersonasbancoestado.com is located on IP address << 217.182.64.245 >>

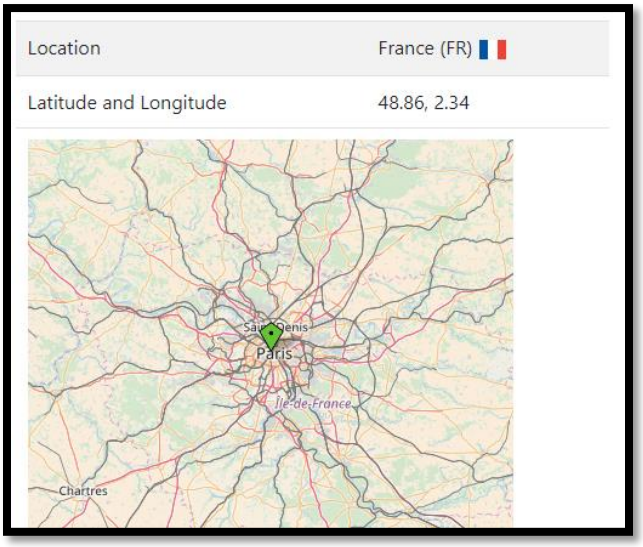
Block start	217.182.0.0
End of block	217.182.255.255
Block size	65536 Domains in block
Block name	FR-OVH-20010302
AS number	16276
Parent block	217.0.0.0 - 217.255.255.255
Organization	ORG-OS3-RIPE

Domain estado.chileacessomovil.com is located on IP address << 80.211.29.8 >>

Block start	80.211.29.0
End of block	80.211.29.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.0.0 - 80.211.127.255
Organization	Aruba S.p.A. - Cloud Services DC1

LOCALIZACIÓN

Roubaix, Hauts-de-France, Francia



Arezzo, Toscana, Italia

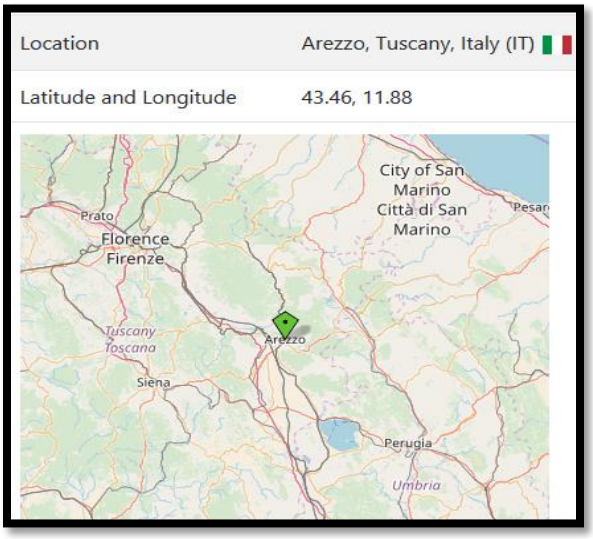
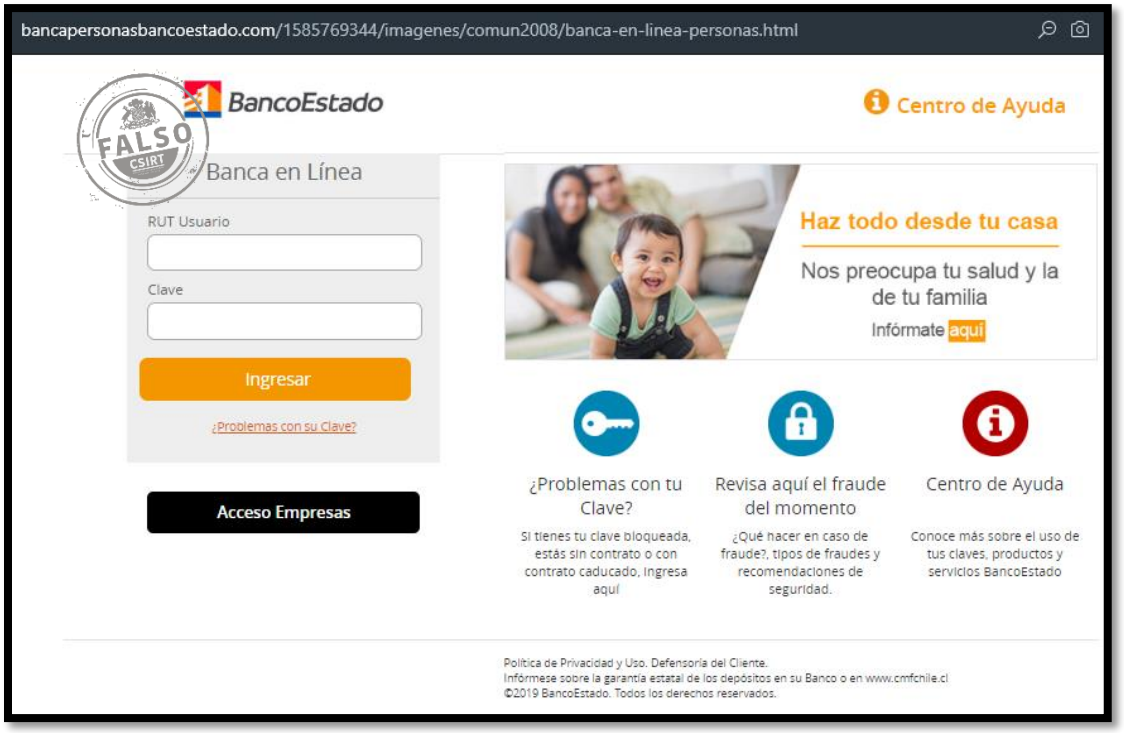
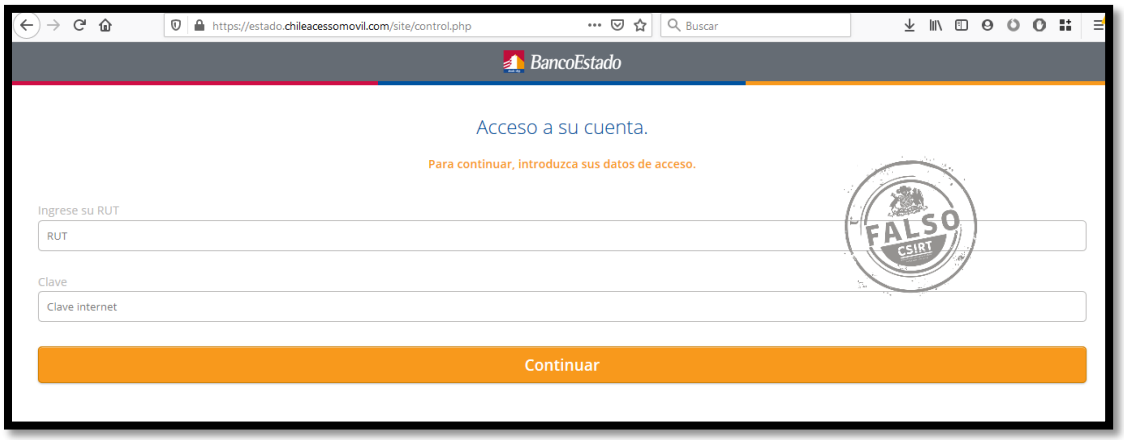


IMAGEN DEL SITIO





WHOIS

```
Domain name: bancapersonasbancoestado.com
Registry Domain ID: 2509846345_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-04-01T12:13:04.00Z
Registrar Registration Expiration Date: 2021-04-01T12:13:04.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 1f213189e6674b7ba9f9104feb64c9ef.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: 1f213189e6674b7ba9f9104feb64c9ef.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: 1f213189e6674b7ba9f9104feb64c9ef.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: chileacessomovil.com
Registry Domain ID: 2504845931_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-18T18:39:08Z
Creation Date: 2020-03-18T18:39:07Z
Registrar Registration Expiration Date: 2021-03-18T18:39:07Z
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 1246707704
Registrant Organization: Contact Privacy Inc. Customer 1246707704
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: m4egn7wnjvnr@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246707704
Admin Organization: Contact Privacy Inc. Customer 1246707704
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: m4egn7wnjvnr@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246707704
Tech Organization: Contact Privacy Inc. Customer 1246707704
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
```

```
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246707704
Tech Organization: Contact Privacy Inc. Customer 1246707704
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: m4egn7wnjvnr@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
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-04-01T19:42:41Z <<<
```

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: 2020.04.02 10:53:49 -03'00'