Alerta de seguridad cibernética	8FFR20-00438-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Junio de 2020
Última revisión	01 de Junio 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 un portal fraudulento asociado 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 compromiso

URL
https[://]www[.]bancapersonas-bancoestado[.]euromob[.]cl

IP
186[.]64[.]117[.]55

Dominios donde se aloja url

Domain bancapersonas-bancoestado.euromob.cl

bancapersonas-bancoestado / euromob / cl / Subdomains

record type	TTL	value
A	14400	186.64.117.55

Domain euromob.cl

euromob / cl / Subdomains

record type	TTL	value		
A	14400	186.64.117.55		
NS	86400	ns1.empresadns.net	Zones on DNS server	186.64.112.88
NS	86400	ns2.empresadns.net	Zones on DNS server	45.79.207.167
NS	86400	ns3.empresadns.net	Zones on DNS server	144.217.14.214
MX	14400	0 mail.euromob.cl		
TXT	14400	v=spf1 +a +mx +ip4:186.64.117.55 ~all		

SOA	86400	Mname	ns1.empresadns.net
		Rname	notificaciones_whm.haulmer.net
		Serial number	2020060107
		Refresh	3600
		Retry	7200
		Expire	1209600
		Minimum TTL	86400

Certificados

Subject DN	CN=bancapersonas-bancoestado.euromob.cl
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	Decimal: 399653618859534197597449121555871820739580 Hex: 0x49679f731c62a873206ff28605636c0f3fc
Validity	2020-06-01 15:15:28 **to** 2020-08-30 15:15:28 (90 days, 0:00:00)
Names	bancapersonas-bancoestado.euromob.cl www.bancapersonas-bancoestado.euromob.cl

Ip de origen donde se aloja sitio

Domain bancapersonas-bancoestado.euromob.cl is located on IP address
<< 186.64.117.55 >>

Block start	186.64.112.0
End of block	186.64.119.255
Block size	2048 Domains in block
Block name	
AS number	52368
Parent block	186.0.0.0 - 186.255.255.255
Organization	ZAM LTDA.

Localización

Santiago, Chile

Location	Chile (CL)
Latitude and Longitude	-33.44, -70.64

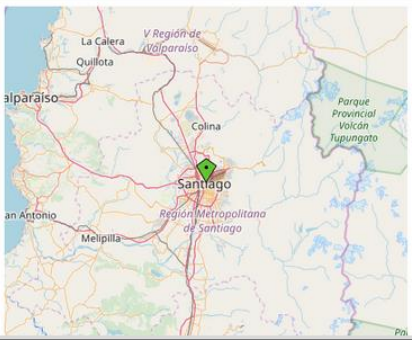
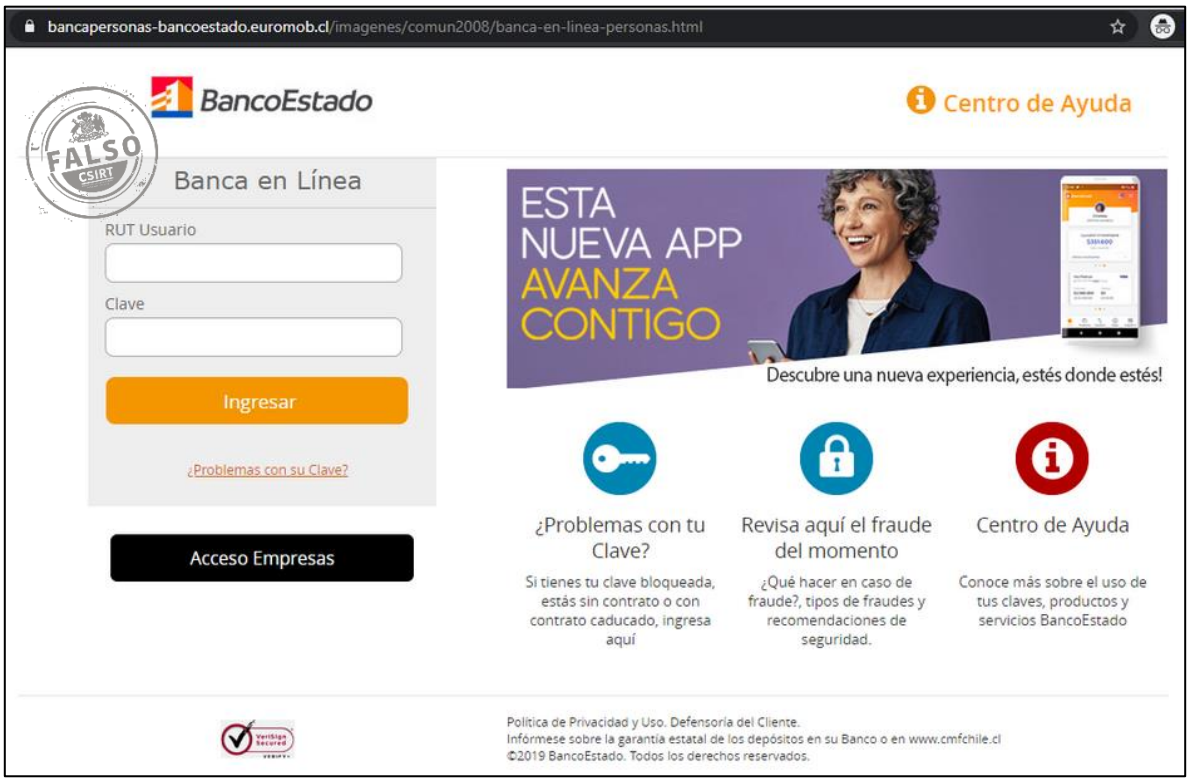


Imagen del sitio



Whois

```
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: euromob.cl
Registrant name: Departamento de marketing (JOSE MOISES LEAL MORALES)
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2005-12-30 20:39:43 CLST
Expiration date: 2024-01-25 17:39:43 CLST
Name server: ns1.empresadns.net
Name server: ns2.empresadns.net
Name server: ns3.empresadns.net

%%
%% For communication with domain contacts please use website.
%% See https://www.nic.cl/registry/Whois.do?d=euromob.cl
%%
```

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.