Alerta de seguridad informática	**8FFR-00099-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**24 de Octubre de 2019**
Última revisión	**24 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 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

http[://]nobaldragas[.]cl/banco_estado/BancoEstado%20Personas%20_%20Banca%20en%20L%c3%adnea[.]html

Domain nobaldragas.cl

nobaldragas / cl / Subdomains

record type	TTL	value		
A	14400	186.64.117.225		
NS	86400	ns2.dnshosty.net	Zones on DNS server	45.79.214.155
NS	86400	ns3.dnshosty.net	Zones on DNS server	144.217.14.211
NS	86400	ns1.dnshosty.net	Zones on DNS server	186.64.112.75
MX	14400	0 mail.nobaldragas.cl		
TXT	14400	v=spf1 ip4:186.64.117.225 ip4:186.64.117.226 +a +mx +ip4:186.64.114.130 +ip4:186.64.114.131 +ip4:186.64.114.132 ~all		

SOA	86400	Mname	ns1.dnshosty.net
		Rname	notificaciones_whm.haulmer.net
		Serial number	2019102305
		Refresh	3600
		Retry	7200
		Expire	1209600
		Minimum TTL	86400

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

Certificado

Criteria: Identity = 'nobaldragas.cl'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2007522747	2019-10-17	2019-10-17	2020-01-15	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2007416819	2019-10-17	2019-10-17	2020-01-15	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1882886991	2019-09-06	2019-09-06	2019-12-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1852775598	2019-09-06	2019-09-06	2019-12-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1691988002	2019-07-07	2019-07-07	2019-10-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1648436824	2019-07-07	2019-07-07	2019-10-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1465903968	2019-05-07	2019-05-07	2019-08-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1452493140	2019-05-07	2019-05-07	2019-08-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1266051372	2019-03-07	2019-03-07	2019-06-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1262197660	2019-03-07	2019-03-07	2019-06-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1082735156	2019-01-05	2019-01-05	2019-04-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1082734994	2019-01-05	2019-01-05	2019-04-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
920761901	2018-11-05	2018-11-05	2019-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
920017791	2018-11-05	2018-11-05	2019-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
806923044	2018-09-05	2018-09-05	2018-12-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
717697766	2018-09-05	2018-09-05	2018-12-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
647192595	2018-07-05	2018-07-05	2018-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
576394483	2018-07-05	2018-07-05	2018-10-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
444744521	2018-05-05	2018-05-05	2018-08-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
441933973	2018-05-05	2018-05-05	2018-08-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
347490771	2018-03-05	2018-03-05	2018-06-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
292862547	2018-01-01	2018-01-01	2018-04-01	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
245156196	2017-11-01	2017-11-01	2018-01-30	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
202481648	2017-09-01	2017-09-01	2017-11-30	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
165215866	2017-07-01	2017-07-01	2017-09-29	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
131428803	2017-05-01	2017-05-01	2017-07-30	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
97904099	2017-03-01	2017-03-01	2017-05-30	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´s

186[.]64[.]117[.]225

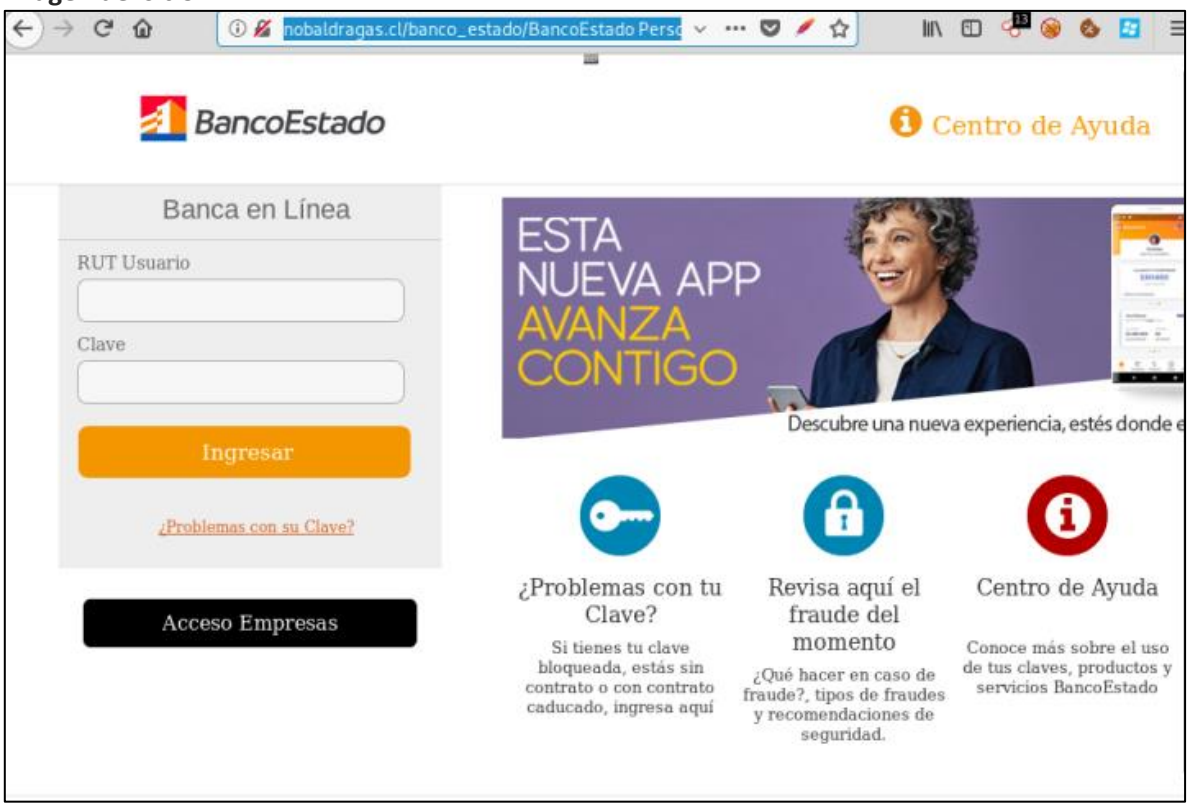
Domain nobaldragas.cl is located on IP address << 186.64.117.225 >>	
Block start	186.64.112.0
End of block	186.64.119.255
Block size	2048 Domains in block
Block name	
AS number	52368
Parent block	186.0.0.0 - 186.255.255.255
Organization	ZAM LTDA.
City	Curico
Region/State	Maule
Country	CL , Chile
Reg. date	2012-11-26
Host name	mail.hosty17.dnshosty.net
Domains	1 nobaldragas.cl

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

Localización

Curico, Maule, Chile

Imagen del sitio



Whois

```
soc@ITQ-ivps3:~$ whois nobaldragas.cl
%%
%% 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: nobaldragas.cl
Registrant name: Sebastian Dinsayants
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2017-02-28 14:46:22 CLST
Expiration date: 2020-02-28 14:46:22 CLST
Name server: ns1.dnshosty.net
Name server: ns2.dnshosty.net
Name server: ns3.dnshosty.net

%%
%% For communication with domain contacts please use website.
%% See https://www.nic.cl/registry/Whois.do?d=nobaldragas.cl
%%
soc@ITQ-ivps3:~$
```

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: 2019.10.25 11:13:00 -03'00'