Alerta de seguridad informática	**8FFR-00097-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**22 de Octubre de 2019**
Última revisión	**22 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 de 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

https[://]purasangre[.]cl/wp-content/plugins/estado/

Domain purasangre.cl

purasangre / cl / Subdomains

record type	TTL	value		
A	14400	190.107.177.232		
NS	86400	ns1.cphost.cl	Zones on DNS server	190.107.177.11
NS	86400	ns2.cphost.cl	Zones on DNS server	190.107.177.12
MX	14400	0 mail.purasangre.cl		
TXT	14400	v=spf1 +a +mx +ip4:190.107.177.232 +ip4:200.63.101.152 ~all		

SOA	86400	Mname	ns1.cphost.cl
		Rname	ventas.cpanelhost.cl
		Serial number	2019070803
		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 = 'purasangre.cl'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1923003891	2019-09-25	2019-09-25	2019-12-24	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1923002812	2019-09-25	2019-09-25	2019-12-24	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1658754064	2019-07-11	2019-07-11	2019-10-09	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1658753580	2019-07-11	2019-07-11	2019-10-09	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado

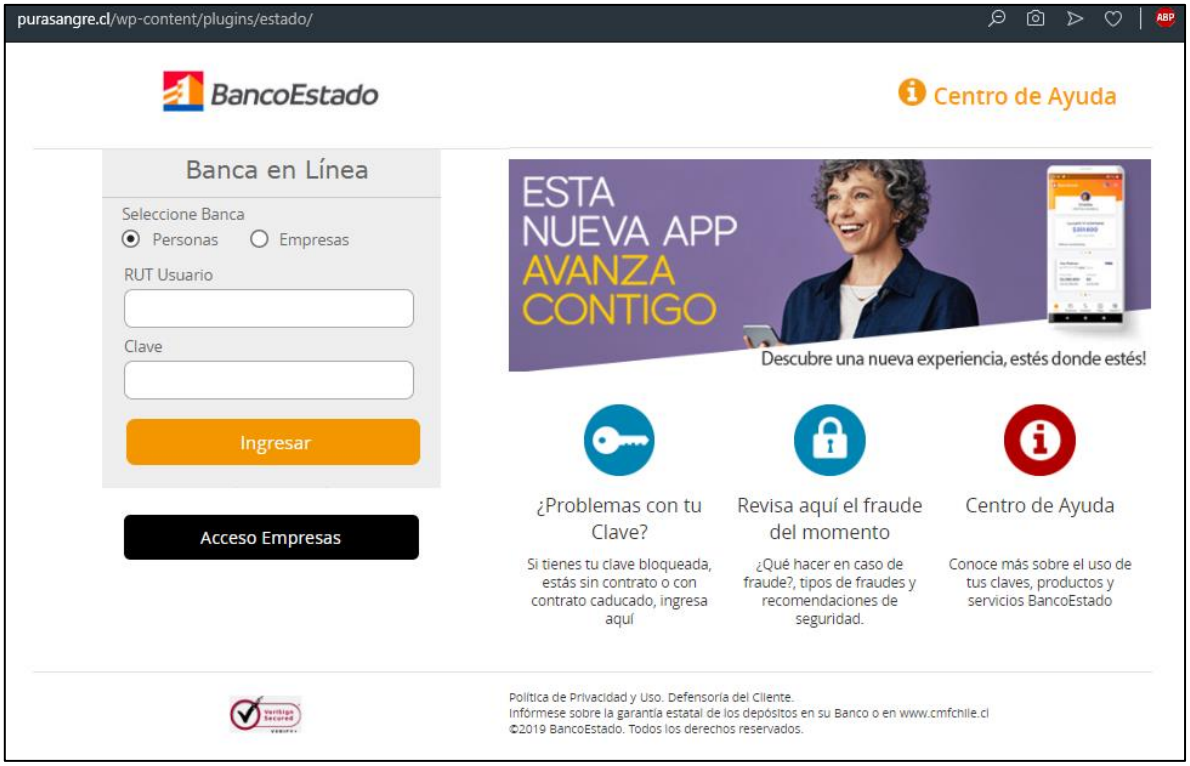
IP´s
190[.]107[.]177[.]232

Domain purasangre.cl is located on IP address << 190.107.177.232 >>	
Block start	190.107.176.0
End of block	190.107.179.255
Block size	1024 Domains in block
Block name	
AS number	265831
Parent block	190.0.0.0 - 190.255.255.255
Organization	SOC. COMERCIAL WIRENET CHILE LTDA.
City	Santiago
Region/State	Region Metropolitana de Santiago
Country	CL , Chile
Reg. date	2012-05-30
Host name	srv02.cphost.cl
Domains	1 purasangre.cl

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

Localización
Santiago, Region Metropolitana de Santiago

Imagen del sitio



Whois

```
soc@ITQ-ivps3:~$ whois purasangre.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: purasangre.cl
Registrant name: indutec eirl
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2019-04-24 17:49:24 CLST
Expiration date: 2021-04-24 17:49:24 CLST
Name server: ns1.cpanelhost.cl
Name server: ns2.cpanelhost.cl

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

```
soc@ITQ-ivps3:~$ whois permisovalido.ga

   Domain name:
      PERMISOVALIDO.GA

   Organisation:
      Gabon TLD B.V.
      My GA administrator
      P.O. Box 11774
      1001 GT  Amsterdam
      Netherlands
      Phone: +31 20 5315725
      Fax: +31 20 5315721
      E-mail: abuse: abuse@freenom.com, copyright infringement: copyright@freenom.com

   Domain Nameservers:
      NS01.FREENOM.COM
      NS02.FREENOM.COM
      NS03.FREENOM.COM
      NS04.FREENOM.COM


   Your selected domain name is a Free Domain. That means that,
   according to the terms and conditions of Free Domain domain names
   the registrant is Gabon TLD B.V.

   Due to restrictions in My GA 's Privacy Statement personal information
   about the user of the domain name cannot be released.

   ABUSE OF A DOMAIN NAME
   If you want to report abuse of this domain name, please send a
   detailed email with your complaint to abuse@freenom.com.
   In most cases My GA responds to abuse complaints within one business day.

   COPYRIGHT INFRINGEMENT
   If you want to report a case of copyright infringement, please send
   an email to copyright@freenom.com, and include the full name and address of
   your organization. Within 5 business days copyright infringement notices
   will be investigated.

   Record maintained by: My GA Domain Registry
```

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: 2019.10.22 18:07:04 -03'00'