Alerta de seguridad informática	8FFR20-00209-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de febrero de 2020
Última revisión	07 de febrero 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 Compromisos

URL

www[.]gorbanjara[.]in/portal/imagenes/comun2008/banca-en-linea-personas[.]html

Domain www.gorbanjara.in

www / gorbanjara / in / Subdomains

record type	TTL	value	
A	14400	208.113.213.229	

Ilustración 1 Dominio donde se aloja URL del Banco Estado falso y DNS que utiliza

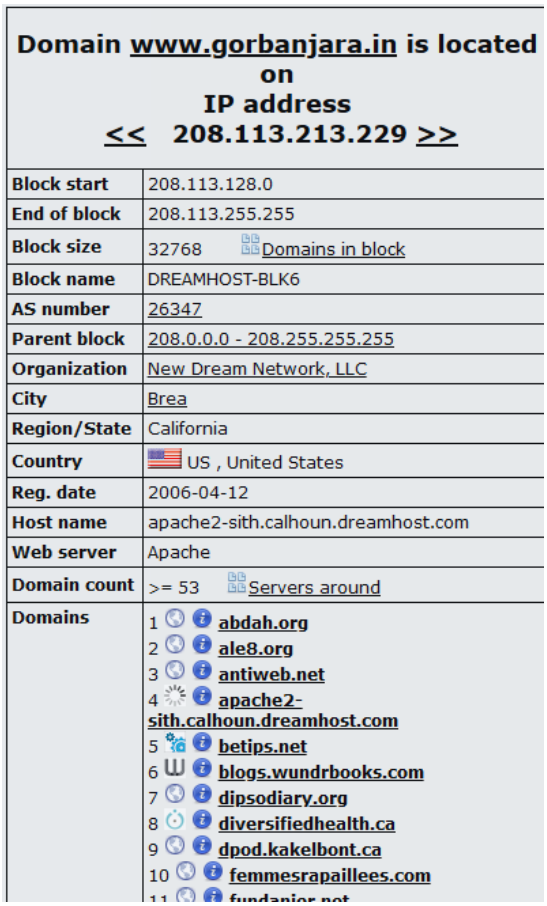
Certificados

Subject DN	CN=gorbanjara.in
Issuer DN	CN=gorbanjara.in
Serial	10176125100639426908
Validity	2017-05-19 04:42:55 **to** 2027-05-17 04:42:55 (3650 days, 0:00:00)

Ilustración 2 Certificado utilizado en URL del sitio falso del Banco Estado.

IP

208[.]113[.]213[.]229



Domain www.gorbanjara.in is located on IP address << 208.113.213.229 >>

Block start	208.113.128.0
End of block	208.113.255.255
Block size	32768 Domains in block
Block name	DREAMHOST-BLK6
AS number	26347
Parent block	208.0.0.0 - 208.255.255.255
Organization	New Dream Network, LLC
City	Brea
Region/State	California
Country	US , United States
Reg. date	2006-04-12
Host name	apache2-sith.calhoun.dreamhost.com
Web server	Apache
Domain count	>= 53 Servers around
Domains	1 abdah.org 2 ale8.org 3 antiweb.net 4 apache2-sith.calhoun.dreamhost.com 5 betips.net 6 blogs.wundrbooks.com 7 dipsodiary.org 8 diversifiedhealth.ca 9 dpod.kakelbont.ca 10 femmesrapaillees.com 11 fundanior.net

Ilustración 3 Ip de origen donde se aloja sitio falso del Banco Estado.

Localización

USA, Brea, California

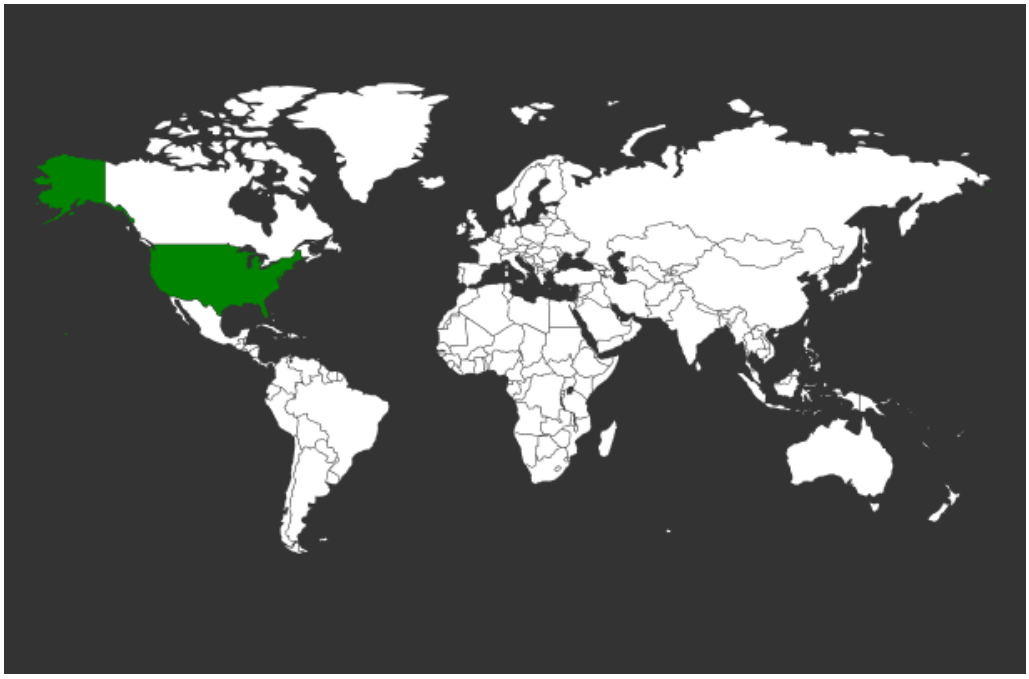
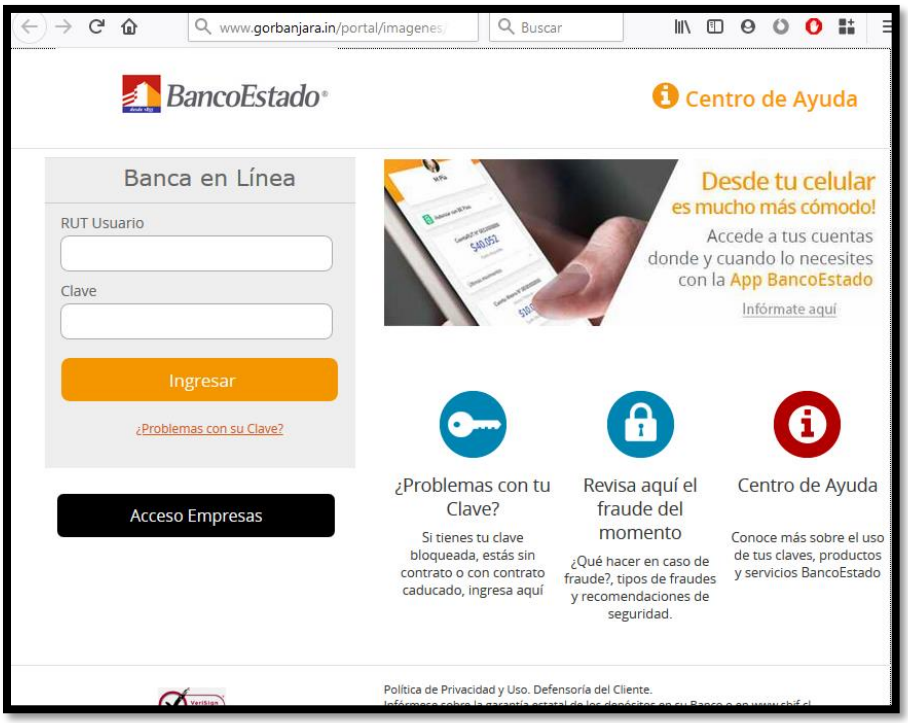


Imagen del sitio



Whois

```
Domain Name: gorbanjara.in
Registry Domain ID: D9231362-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2019-03-11T12:45:21Z
Creation Date: 2015-02-21T16:07:52Z
Registry Expiry Date: 2021-02-21T16:07:52Z
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#clientTransferProhibited
Domain Status: renewPeriod http://www.icann.org/epp#renewPeriod
Registry Registrant ID:
Registrant Name:
Registrant Organization: Clearchoice Constructions
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Karnataka
Registrant Postal Code:
Registrant Country: IN
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:
Tech Email: Please contact the Registrar listed above
Name Server: ns2.dreamhost.com
Name Server: ns4.dreamhost.com
Name Server: ns1.dreamhost.com
Name Server: ns3.dreamhost.com
DNSSEC: unsigned
```

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: 2020.02.07 11:50:31 -03'00'