Alerta de seguridad informática	**8FFR-00076-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**02 de Octubre de 2019**
Última revisión	**02 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[://]socialbits[.]mx/damp/imagenes/comun2008/banca-en-linea-personas[.]html

Dominio socialbits.mx

bits sociales / mx / Subdominios

tipo de registro	TTL	valor		
UNA	14400	68.70.164.3		
NS	86400	ns2-floki.hosting-mexico.net	Zonas en el servidor DNS	68.70.164.4
NS	86400	ns1-floki.hosting-mexico.net	Zonas en el servidor DNS	68.70.164.3
MX	14400	0 socialbits.mx		
TXT	14400	v = spf1 + a + mx + ip4: 68.70.164.3 ~ todos		
SOA	86400			

Mname	ns1-floki.hosting-mexico.net
Rname	notificaciones.hosting-mexico.net
Número de serie	2019053003
Actualizar	3600
Procesar de nuevo	1800
Expirar	1209600
TTL mínimo	86400

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso

IP´s

68[.]70[.]164[.]3

Dirección IP << 68.70.164.3 >>

Inicio de bloque	68.70.164.0
Fin del bloque	68.70.164.63
Tamaño de bloque	64 Dominios en bloque
Nombre del bloque	AZOGUE
Número AS	22458
Bloque padre	68.70.160.0 - 68.70.175.255
Organización	QuickSilver Associates
Ciudad	Chicago
Región / Estado	Illinois
País	Estados Unidos, Estados Unidos
Reg. fecha	18/11/2011
Nombre del anfitrión	floki.hosting-mexico.net
Dominios	1 socialbits.mx

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Naperville, Illinois, Estados Unidos

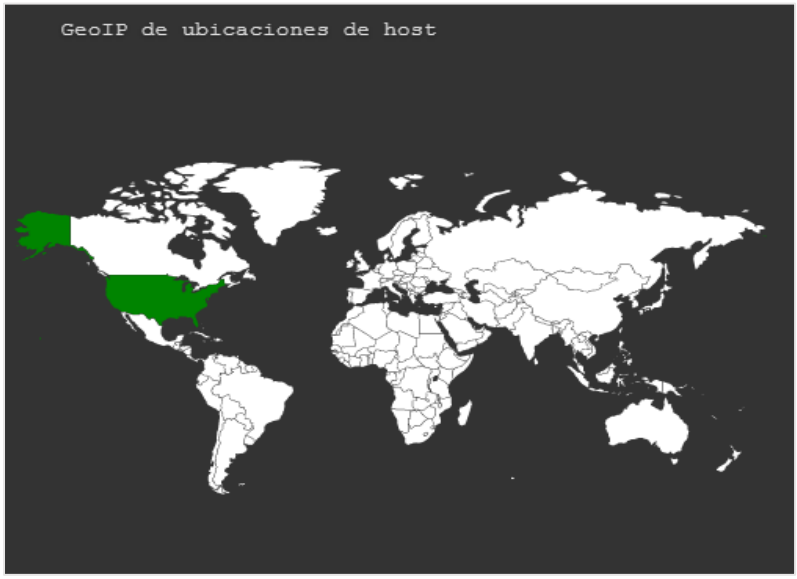
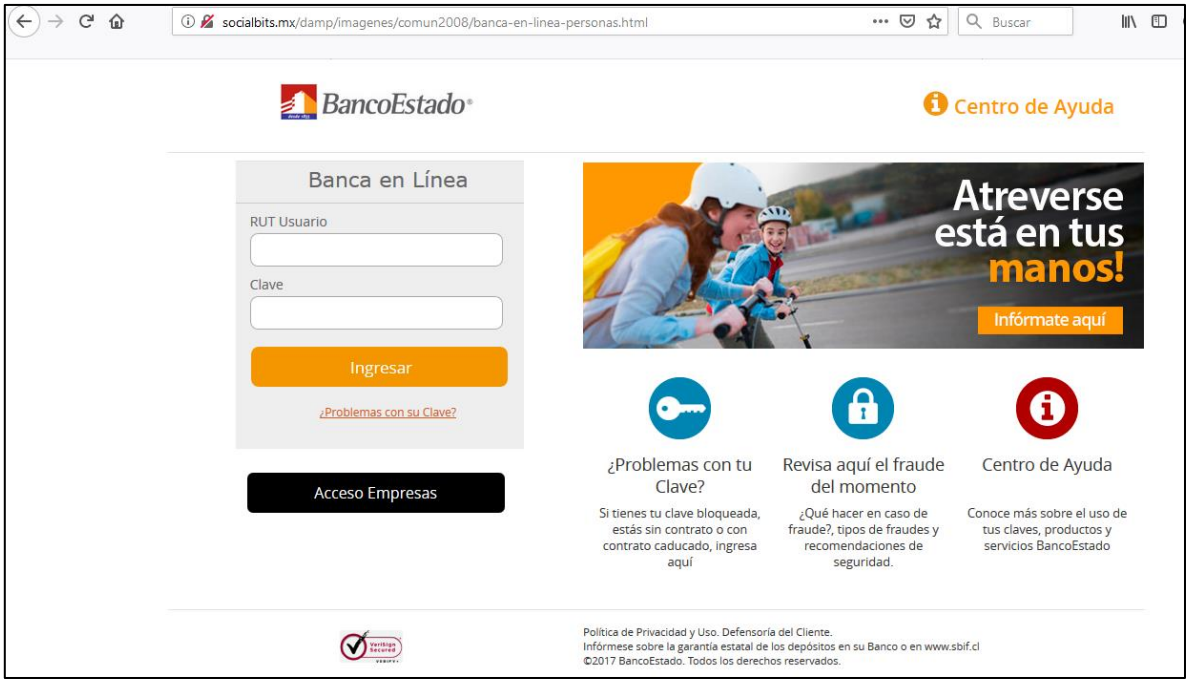


Imagen del sitio



Whois

```
soc@ITQ-ivps2:~$ whois socialbits.mx

Domain Name:        socialbits.mx

Created On:         2019-03-03
Expiration Date:    2020-03-03
Last Updated On:    2019-04-19
Registrar:          Hosting-Mexico
URL:                http://www.hosting-mexico.net

Registrant:
   Name:            Ivan Francisco Castillo Abarca
   City:            TUXPAN
   State:           Veracruz
   Country:         Mexico

Administrative Contact:
   Name:            Ivan Francisco Castillo Abarca
   City:            TUXPAN
   State:           Veracruz
   Country:         Mexico

Technical Contact:
   Name:            Ivan Francisco Castillo Abarca
   City:            TUXPAN
   State:           Veracruz
   Country:         Mexico

Billing Contact:
   Name:            Ivan Francisco Castillo Abarca
   City:            TUXPAN
   State:           Veracruz
   Country:         Mexico

Name Servers:
   DNS:             ns1-floki.hosting-mexico.net
   DNS:             ns2-floki.hosting-mexico.net

DNSSEC DS Records:
```

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: 2019.10.02 18:48:05 -03'00'