Alerta de seguridad informática	8FFR20-00190-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero 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 de Chile, 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

w2bancodchile[.]eventorut[.]ml/persona/login/

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

Certificados

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco de Chile

IP

192.185.5.44

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

Localización

Houston, Texas, Estados Unidos

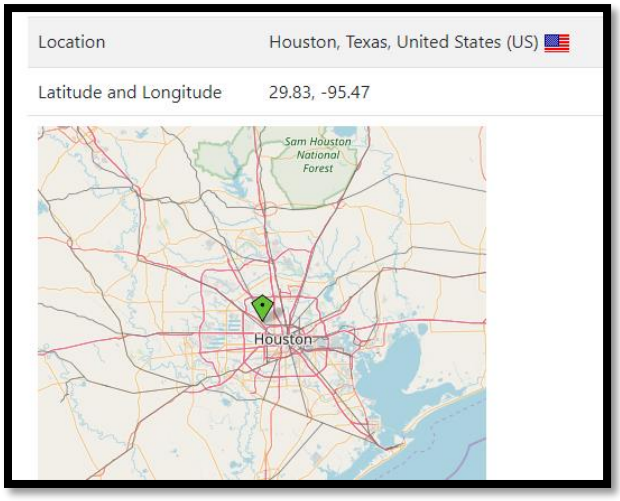
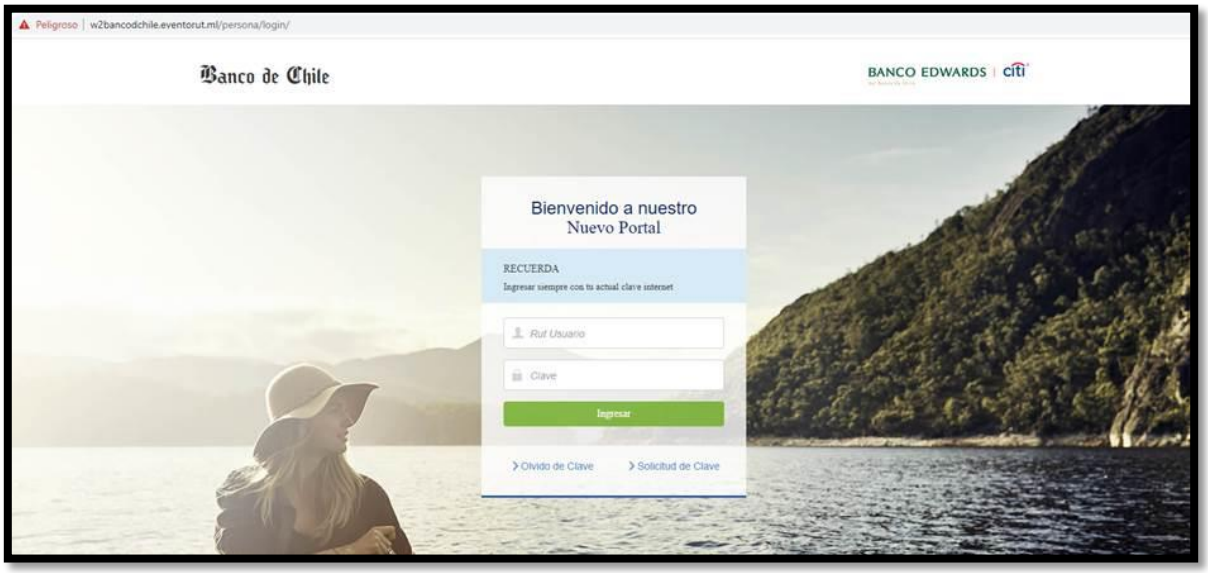


Imagen del sitio



Whois

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.dot.ml

domain:       ML

organisation: Agence des Technologies de l'Information et de la Communication
address:      ACI 2000 Hamdallaye
address:      Bamako BP E 5467
address:      Mali

contact:      administrative
name:         Chef Service Gestion du .ml
organisation: Agence des Technologies de l'Information et de la Communication
address:      ACI 2000 Hamdallaye
address:      Bamako BP E 5467
address:      Mali
phone:        +223 77 28 52 51
fax-no:       +223 20 29 94 13
e-mail:       nkamate@agetic.gouv.ml

contact:      technical
name:         Manager ICT
organisation: Mali Dili B.V.
address:      Keizersgracht 213
address:      1016 DT  Amsterdam
address:      Netherlands
phone:        +31 20 5315726
fax-no:       +31 20 5315721
e-mail:       info@malidili.com

nserver:      A.NS.ML 185.21.168.1 2a04:1b00:0:0:0:0:0:1
nserver:      B.NS.ML 185.21.169.1 2a04:1b00:1:0:0:0:0:1
nserver:      C.NS.ML 185.21.170.1 2a04:1b00:2:0:0:0:0:1
nserver:      D.NS.ML 185.21.171.1 2a04:1b00:3:0:0:0:0:1

whois:        whois.dot.ml

status:       ACTIVE
remarks:      Registration information: http://www.dot.ml

created:      1993-09-29
changed:      2018-04-20
source:       IANA


   Domain name:
      EVENTORUT.ML

   Organisation:
      Freedom Registry, Inc.
      2225 East Bayshore Road #290
      Palo Alto CA 94303
      United States
      Phone: +1 650-681-4172
      Fax: +1 650-681-4173

   Domain Nameservers:
      NS01.FREENOM.COM
```

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: 2020.01.25 12:55:30 -03'00'