Alerta de seguridad informática	8FFR-00149-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Diciembre de 2019
Última revisión	13 de Diciembre 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 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

URL Sitio Clonado:
https[://]www[.]login-bcochile[.]cl/

Domain www.login-bcochile.cl

www / login-bcochile / cl / Subdomains

record type	TTL	value	
CNAME	14400	login-bcochile.cl	162.241.60.177

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

Certificados

Basic Information

Subject DN	OU=Domain Control Validated, OU=PositiveSSL, CN=login-bcochile.cl
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	114673073075157451498813476547628401774
Validity	2019-12-10 00:00:00 to 2020-12-09 23:59:59 (365 days, 23:59:59)
Names	login-bcochile.cl www.login-bcochile.cl

Fingerprint

SHA-256	6333a9340aaa3f9b2d9c48c39a133ab03bd9c87945f589ba193da908f3ed54fd
SHA-1	9ed4d0a88f82919b36534effb5dbff6f4b04e29f
MD5	7bf0ede3aac5172a3779a5902b478476

Public Key

Key Type	2048-bit RSA, e = 65,537 ✔ STRONG
Modulus	b7:21:2c:cf:bb:2b:ad:50:89:de:23:be:73:c1:6d:99:d3:9a:03:13:
SPKI SHA-256	c610f5335c7f1dbe360546e563d5c04da07edfa998b5ab5b955febd679779b9b

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

IP

162.241.60.177

Domain www.login-bcochile.cl is located on IP address << 162.241.60.177 >>

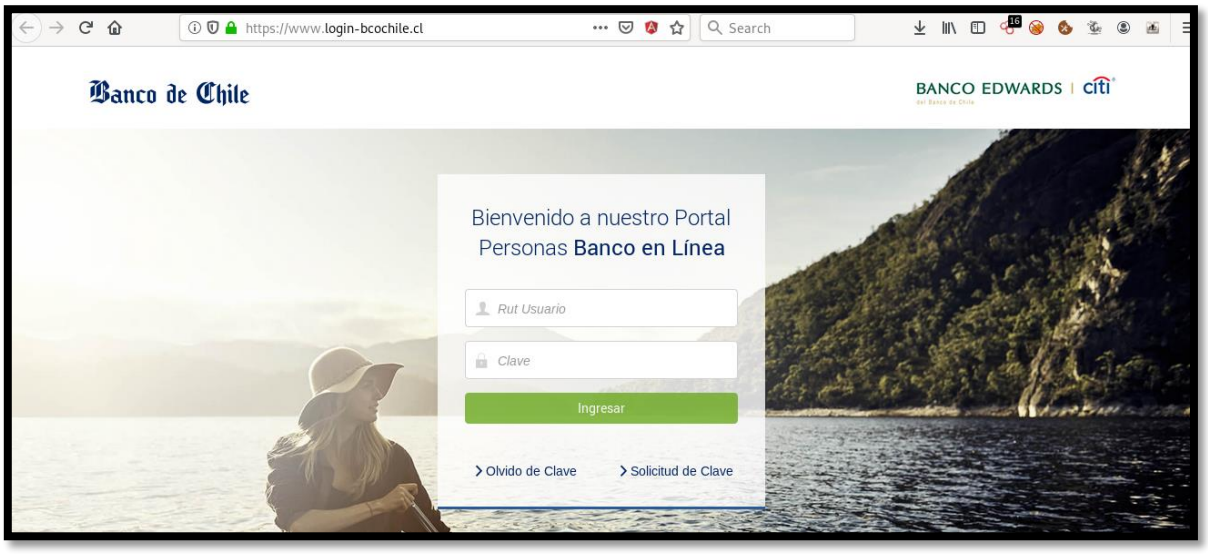
Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	162-241-60-177.unifiedlayer.com
Domain count	>= 2 Servers around
Domains	1 ccvvstore.xyz 2 www.login-bcochile.cl

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

Localización

Provo, Utah, Estados Unidos

Imagen del sitio



Whois

```
Domain name: login-bcochile.cl
Registrant name: vicente pizarro
Registrant organisation: N/A
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar URL: https://www.publicdomainregistry.com
Creation date: 2019-12-10 09:05:32 CLST
Expiration date: 2020-12-10 09:05:32 CLST
Name server: ns16.hostgator.cl
Name server: ns17.hostgator.cl
```

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: 2019.12.13 19:51:27 -03'00'