Alerta de seguridad informática	8FFR-00107-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Noviembre de 2019
Última revisión	11 de Noviembre 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 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

https[://]www[.]login[.]bancochile[.]cl-bancochile-web[.]com-cl[.]nl/39ntqf3xes/l8fol_persona/login_zce8/index/login88oh/

Domain com-cl.nl

com-cl / nl / Subdomains

record type	TTL	value		
A	14400	68.66.224.55		
NS	86400	ns2.a2hosting.com	Zones on DNS server	162.159.24.221
NS	86400	ns4.a2hosting.com	Zones on DNS server	162.159.24.227
NS	86400	ns3.a2hosting.com	Zones on DNS server	162.159.25.82
NS	86400	ns1.a2hosting.com	Zones on DNS server	162.159.25.95
MX	14400	0 com-cl.nl		
TXT	14400	v=spf1 +a +mx +ip4:68.66.224.55 ~all		
SOA	86400	Mname: ns1.a2hosting.com Rname: root.az1-ss28.a2hosting.com Serial number: 2019110804 Refresh: 3600 Retry: 1800 Expire: 1209600 Minimum TTL: 86400		

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

Certificado

Criteria: Identity = 'com-cl.nl'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2075431746	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2075431832	2019-11-05	2019-11-05	2020-02-03	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

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

IP´s

68[.]66[.]224[.]55

Domain com-cl.nl is located on IP address << 68.66.224.55 >>	
Block start	68.66.192.0
End of block	68.66.255.255
Block size	16384 Domains in block
Block name	RSN-4
AS number	55293
Parent block	68.0.0.0 - 68.255.255.255
Organization	RockSolid Network, Inc.
City	Ann Arbor
Region/State	Michigan
Country	US , United States
Reg. date	2009-09-01
Host name	az1-ss28.a2hosting.com
Domains	1 com-cl.nl

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

Localización

Estados Unidos, Ann Arbor

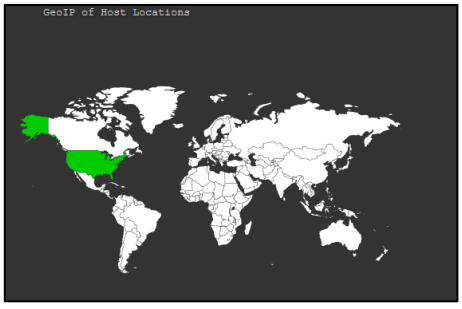
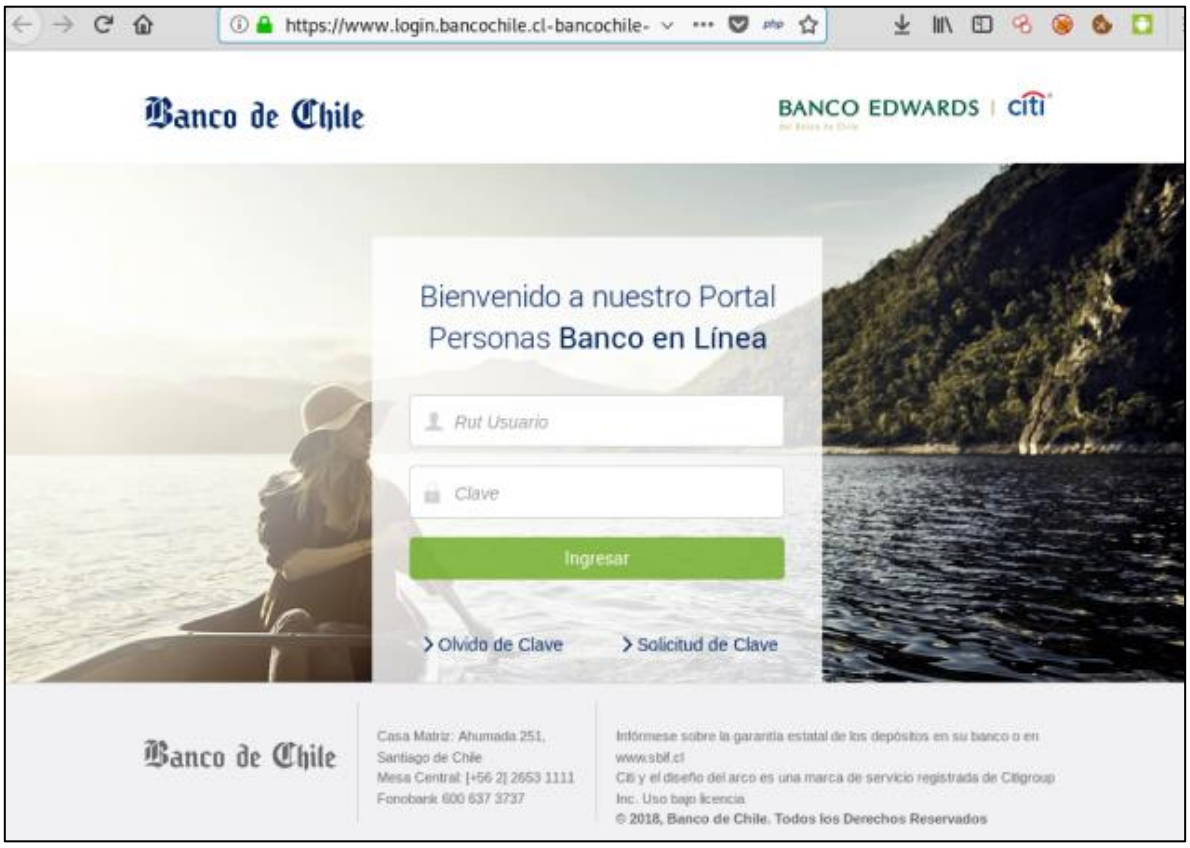


Imagen del sitio



Whois

```
root@gsa:~# whois -I com-cl.nl
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.domain-registry.nl

domain:       NL

organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands

contact:      administrative
name:         Managing Director
organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands
phone:        +31 26 3525500
fax-no:       +31 26 3525505
e-mail:       admin@sidn.nl

contact:      technical
name:         Manager ICT
organisation: SIDN (Stichting Internet  Domeinregistratie Nederland)
address:      P.O. Box 5022
address:      Arnhem  6802 EA
address:      Netherlands
phone:        +31 26 3525500
fax-no:       +31 26 3525550
e-mail:       tech@sidn.nl

nserver:      NS1.DNS.NL 194.0.28.53 2001:678:2c:0:194:0:28:53
nserver:      NS2.DNS.NL 194.146.106.42 2001:67c:1010:10:0:0:0:53
nserver:      NS3.DNS.NL 194.0.25.24 2001:678:20:0:0:0:0:24
nserver:      SNS-PB.ISC.ORG 192.5.4.1 2001:500:2e:0:0:0:0:1
```

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: 2019.11.11 15:49:59 -03'00'