Alerta de seguridad informática	**8FFR-00084-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**09 de Octubre de 2019**
Última revisión	**09 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 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[.]webportal[.]live/consulting/bancochile//wcm/connect/Personas/Portal/2w7ddyl4ar/u1ax4_persona/login_ju3o/index/loginkd0j/

Domain www.webportal.live			
www / webportal / live / Subdomains			
record type	TTL	value	
CNAME	14400	webportal.live	45.95.168.70

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

IP´s

45[.]95[.]168[.]70

Domain www.webportal.live is located on IP address << 45.95.168.70 >>	
Block start	45.95.168.0
End of block	45.95.171.255
Block size	1024 Domains in block
Block name	HR-MAXKO-20190710
AS number	42864
Parent block	45.80.0.0 - 45.95.255.255
Organization	ORG-MJ181-RIPE
City	-
Country	
Reg. date	2019-07-10
Host name	server.maxko-hosting.com
Domains	1 www.webportal.live

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

Localización

Sisak, Sisacko-moslavacka zupanija, Croacia

Certificados

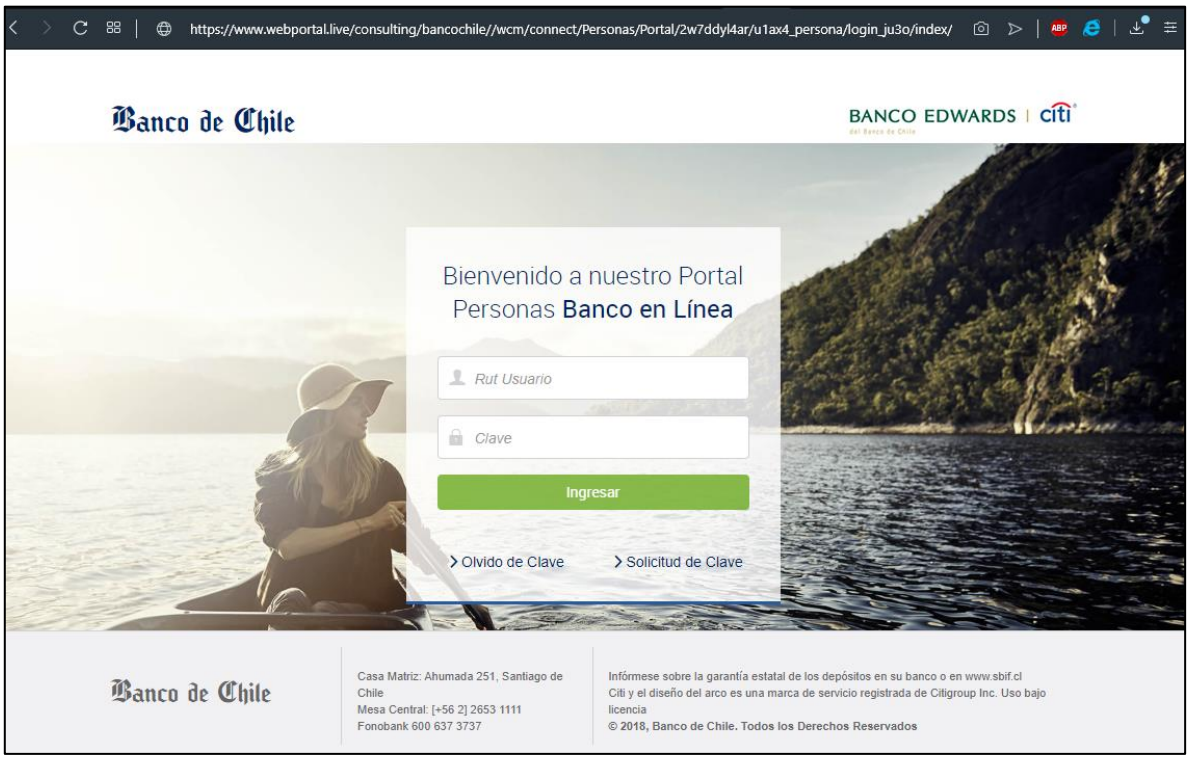
Criteria | Identity = 'www.webportal.live'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1944702516	2019-10-01	2019-10-01	2019-12-30	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1944702430	2019-10-01	2019-10-01	2019-12-30	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1814084942	2019-08-27	2019-08-27	2019-11-25	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1814084381	2019-08-27	2019-08-27	2019-11-25	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1825384737	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1772110610	2019-08-14	2019-08-14	2019-11-12	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1823137465	2019-08-13	2019-08-13	2019-11-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1768711243	2019-08-13	2019-08-13	2019-11-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1497401377	2019-05-22	2019-05-22	2019-08-20	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1497401057	2019-05-22	2019-05-22	2019-08-20	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1416695554	2019-04-25	2019-04-25	2019-07-24	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1416693247	2019-04-25	2019-04-25	2019-07-24	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1382462385	2019-04-12	2019-04-12	2019-07-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1379328251	2019-04-12	2019-04-12	2019-07-11	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 3 Certificado Utilizado en Url del sitio Falso del Banco Chile

Imagen del sitio



Whois

```
soc@ITQ-ivps2:~$ whois webportal.live
Domain Name: webportal.live
Registry Domain ID: cc3f57b8113940e7978acfd16cdeda2a-DONUTS
Registrar WHOIS Server: dynadot.com/whois
Registrar URL: http://dynadot.com
Updated Date: 2019-10-01T12:48:21Z
Creation Date: 2019-04-10T01:06:03Z
Registry Expiry Date: 2020-04-10T01:06:03Z
Registrar: Dynadot, LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: California
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: ns1.maxko-hosting.com
Name Server: ns2.maxko-hosting.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: 2019.10.09 09:20:53 -03'00'