Alerta de seguridad informática	**8FFR-00063-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**17 de Septiembre de 2019**
Última revisión	**17 de Septiembre 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.

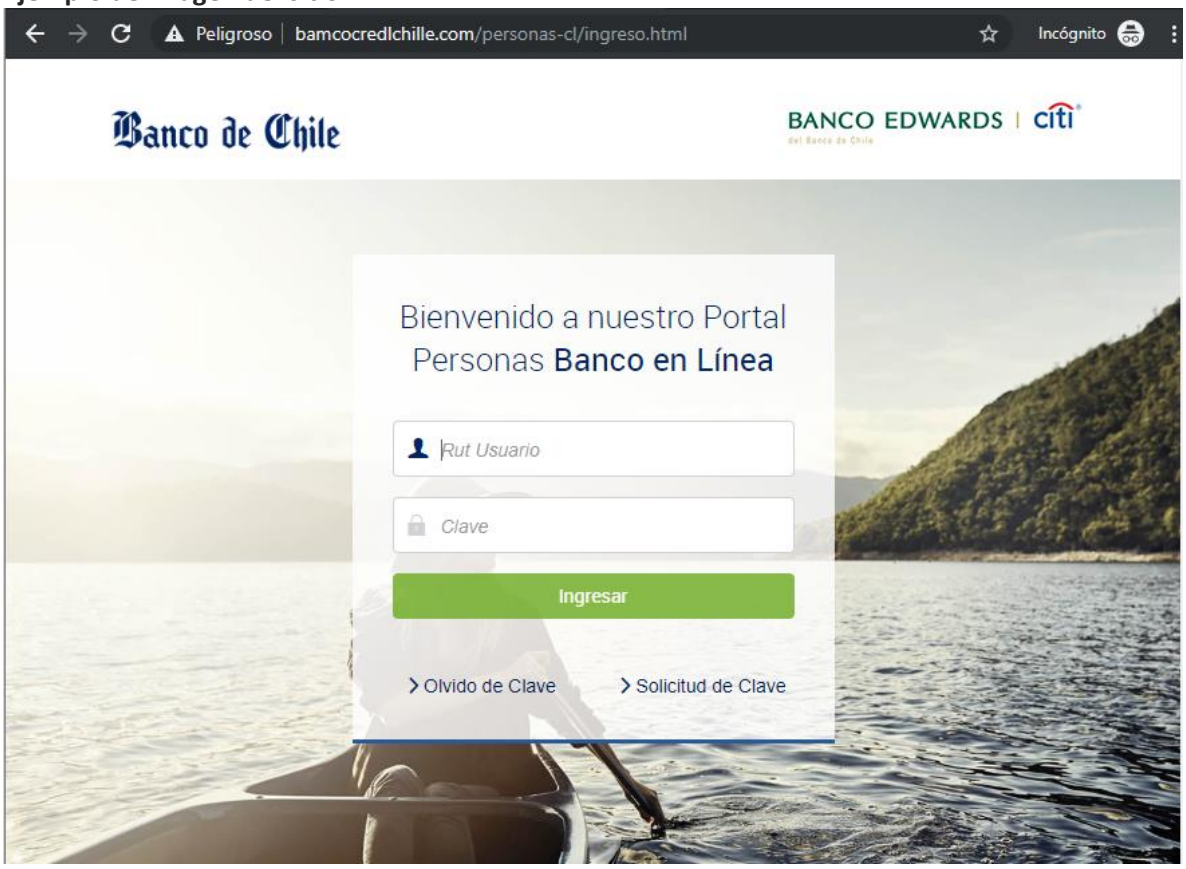
Indicadores de Compromisos

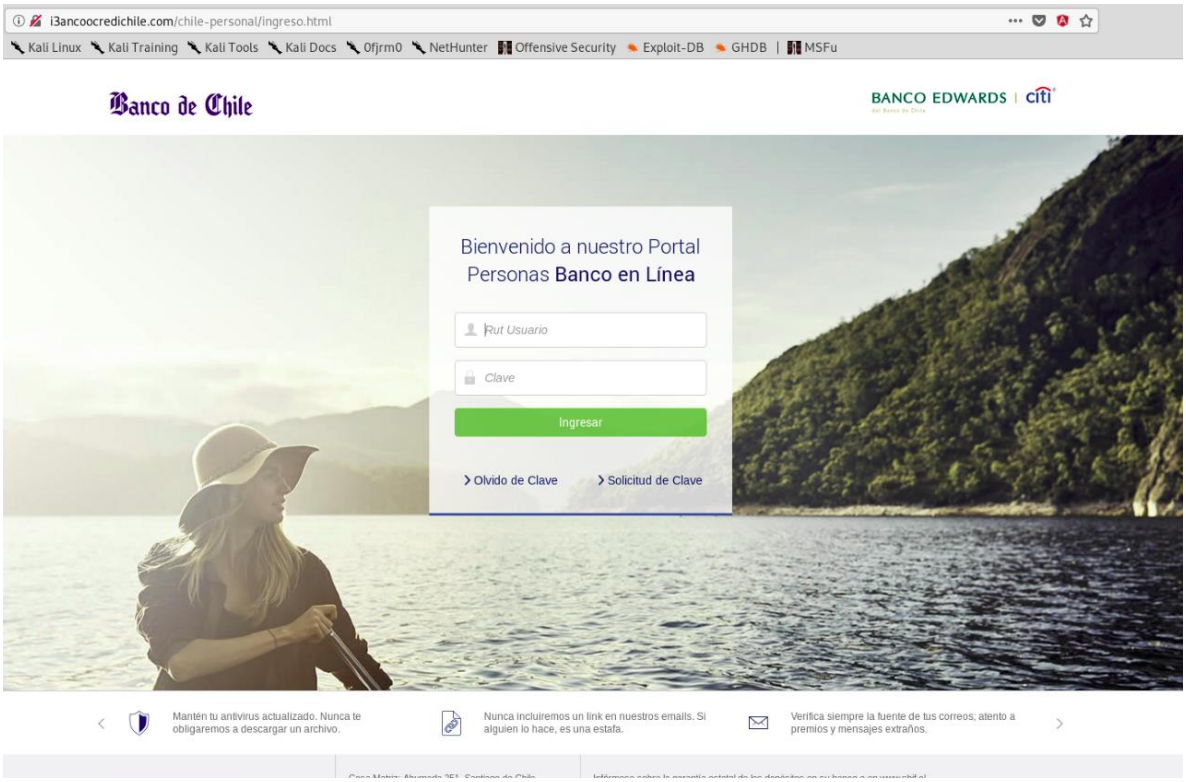
URL´s
http[://]bamcocredlchille[.]com/personas-cl/ingreso[.]html
http[://]li3ancocredichille[.]com/chile-personal/ingreso[.]html
http[://]i3ancoocredichile[.]com/chile-personal/ingreso[.]html
http[://]il3ancocredlchile[.]com/chile-personal/ingreso[.]html
http[://]www[.]wwv-l3ancacredichille-cl[.]htlps-wwv-cmr-cl[.]com/personas-cl/ingreso[.]html

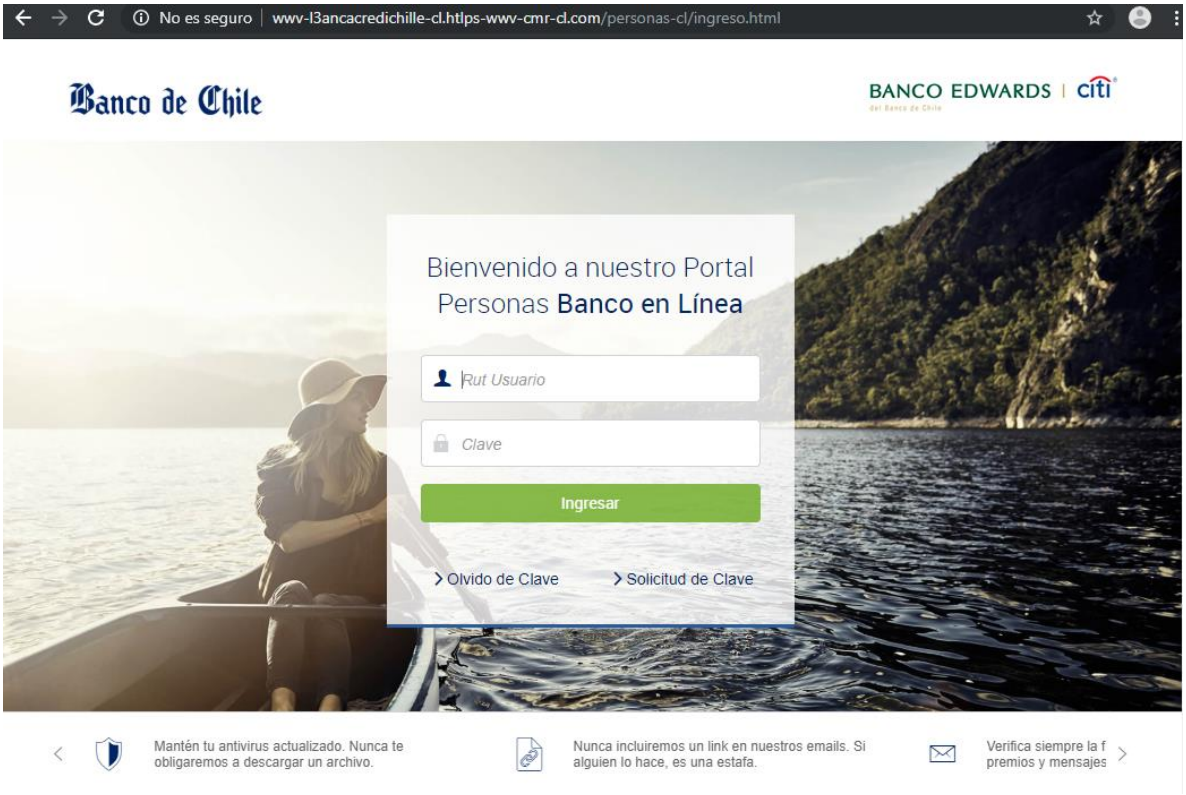
IP´s
162[.]241[.]60[.]14
108[.]167[.]192[.]244
162[.]241[.]60[.]15

Localización
Provo, Utah, Estados Unidos
Three Lakes, Wisconsin, Estados Unidos

Ejemplo de Imagen del sitio




i3ancoocredichile.com/chile-personal/ingreso.html
Kali Linux Kali Training Kali Tools Kali Docs 0fjrm0 NetHunter Offensive Security Exploit-DB GHDB MSFu
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
Ingresar
Olvido de Clave
Solicitud de Clave
Mantén tu antivirus actualizado. Nunca te obligaremos a descargar un archivo.
Nunca incluiremos un link en nuestros emails. Si alguien lo hace, es una estafa.
Verifica siempre la fuente de tus correos; atento a premios y mensajes extraños.


No es seguro | wwv-l3ancacredichille-cl.htlps-wwv-cmr-cl.com/personas-cl/ingreso.html
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
Ingresar
Olvido de Clave
Solicitud de Clave
Mantén tu antivirus actualizado. Nunca te obligaremos a descargar un archivo.
Nunca incluiremos un link en nuestros emails. Si alguien lo hace, es una estafa.
Verifica siempre la f
premios y mensajes

Whois

```
soc@kali:~$ whois -h whois.PublicDomainRegistry.com bamcocredlchille.com
Domain Name: BAMCOCREDLCHILLE.COM
Registry Domain ID: 2429247282_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-09-02T13:31:09Z
Creation Date: 2019-09-02T13:31:08Z
Registrar Registration Expiration Date: 2020-09-02T13:31:08Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: jairo tafur
Registrant Organization:
Registrant Street: las condes, 2328 macul
Registrant City: Macul
Registrant State/Province: RM
Registrant Postal Code: 7180000
Registrant Country: CL
Registrant Phone: +56.983772888
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: samuelpasajes@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: jairo tafur
Admin Organization:
Admin Street: las condes, 2328 macul
Admin City: Macul
Admin State/Province: RM
Admin Postal Code: 7180000
Admin Country: CL
Admin Phone: +56.983772888
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: samuelpasajes@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: jairo tafur
Tech Organization:
Tech Street: las condes, 2328 macul
Tech City: Macul
Tech State/Province: RM
Tech Postal Code: 7180000
Tech Country: CL
Tech Phone: +56.983772888
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: samuelpasajes@gmail.com
Name Server: ns14.hostgator.cl
Name Server: ns15.hostgator.cl
DNSSEC: Unsigned
```

```
soc@kali:~$ whois -h whois.PublicDomainRegistry.com il3ancocredlchile.com
Domain Name: IL3ANCOCREDLCHILE.COM
Registry Domain ID: 2431753937_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-09-10T12:29:16Z
Creation Date: 2019-09-10T12:29:15Z
Registrar Registration Expiration Date: 2020-09-10T12:29:15Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: jairo tafur
Registrant Organization:
Registrant Street: las condes, 2328 macul
Registrant City: Macul
Registrant State/Province: RM
Registrant Postal Code: 7180000
Registrant Country: CL
Registrant Phone: +56.983772888
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: samuelpasajes@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: jairo tafur
Admin Organization:
Admin Street: las condes, 2328 macul
Admin City: Macul
Admin State/Province: RM
Admin Postal Code: 7180000
Admin Country: CL
Admin Phone: +56.983772888
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: samuelpasajes@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: jairo tafur
Tech Organization:
Tech Street: las condes, 2328 macul
Tech City: Macul
Tech State/Province: RM
Tech Postal Code: 7180000
Tech Country: CL
Tech Phone: +56.983772888
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: samuelpasajes@gmail.com
Name Server: ns10.hostgator.cl
Name Server: ns11.hostgator.cl
DNSSEC: Unsigned
```

```
Domain Name: HTLPS-WWV-CMR-CL.COM
Registry Domain ID: 2414128928_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-07-18T13:56:00Z
Creation Date: 2019-07-18T13:55:59Z
Registrar Registration Expiration Date: 2020-07-18T13:55:59Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: jairo tafur
Registrant Organization:
Registrant Street: los arboles, 4348 macul
Registrant City: Macul
Registrant State/Province: RM
Registrant Postal Code: 7180000
Registrant Country: CL
Registrant Phone: +56.938499944
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pasajesyonn@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: jairo tafur
Admin Organization:
Admin Street: los arboles, 4348 macul
Admin City: Macul
Admin State/Province: RM
Admin Postal Code: 7180000
Admin Country: CL
Admin Phone: +56.938499944
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pasajesyonn@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: jairo tafur
Tech Organization:
Tech Street: los arboles, 4348 macul
Tech City: Macul
Tech State/Province: RM
Tech Postal Code: 7180000
Tech Country: CL
Tech Phone: +56.938499944
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pasajesyonn@gmail.com
Name Server: ns14.hostgator.cl
Name Server: ns15.hostgator.cl
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: 2019.09.17 08:27:35 -03'00'