Alerta de seguridad informática	**8FFR-00048-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**07 de Septiembre de 2019**
Última revisión	**07 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 del **bancobci.cl,** 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.

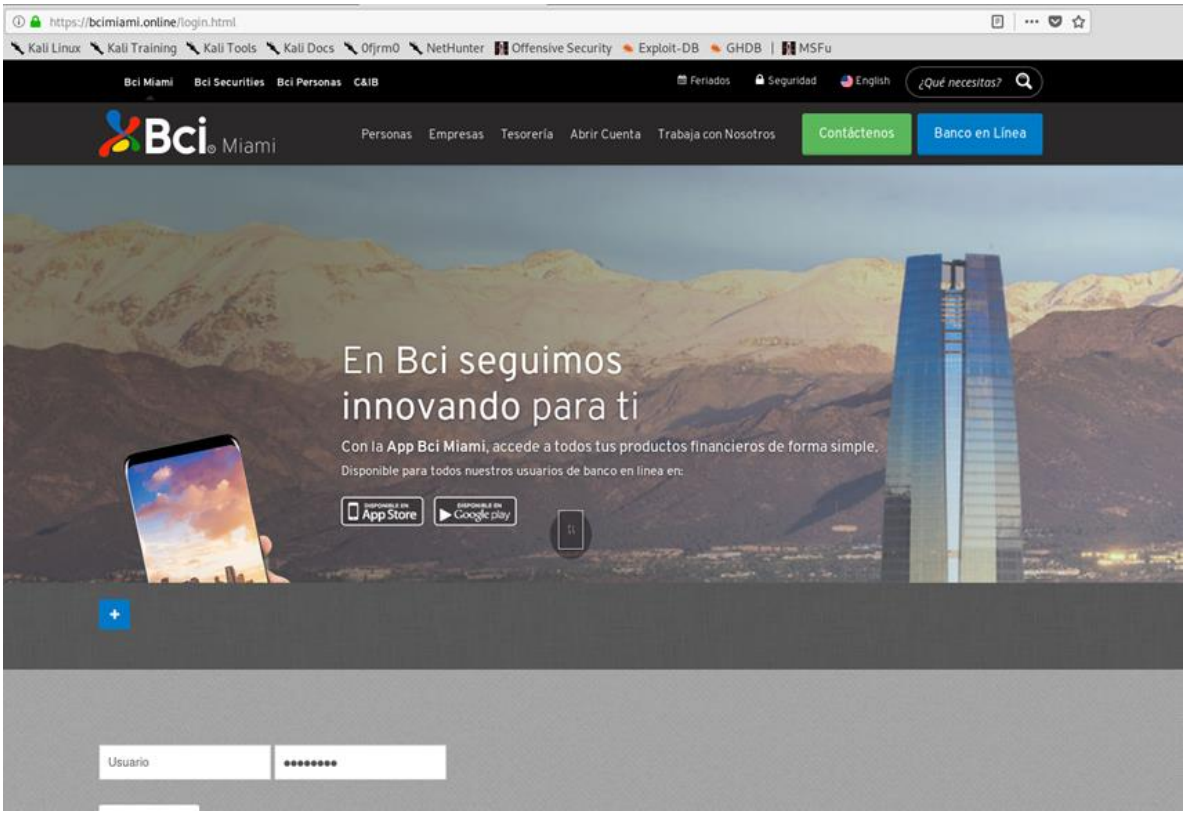
Indicadores de Compromisos

URL´s
https[://]bcimiami[.]online/

IP´s
194[.]5[.]156[.]92

Localización
Amsterdam, Noord-Holland, Holanda

Ejemplo de Imagen del sitio



Whois

```
Domain Name: BCIMIAMI.ONLINE
Registry Domain ID: D123037501-CNIC
Registrar WHOIS Server: whois.hostinger.com
Registrar URL:
Updated Date: 2019-09-03T11:23:53.0Z
Creation Date: 2019-09-03T11:23:52.0Z
Registry Expiry Date: 2020-09-03T23:59:59.0Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibi
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: GDPR Masked
Registrant State/Province: GDPR Masked
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identifi
Admin Email: Please query the RDDS service of the Registrar of Record identified in
Tech Email: Please query the RDDS service of the Registrar of Record identified in
Name Server: NS4.HOSTINGER.FR
Name Server: NS3.HOSTINGER.FR
Name Server: NS2.HOSTINGER.FR
Name Server: NS1.HOSTINGER.FR
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: 2019.09.07 22:27:41 -04'00'