Alerta de seguridad informática	**8FFR-00030-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**27 de Agosto de 2019**
Última revisión	**27 de Agosto 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 **bancochile.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

http[://]www[.]personas-bancodechile[.]alertasviabcpe[.]com/persona/login/

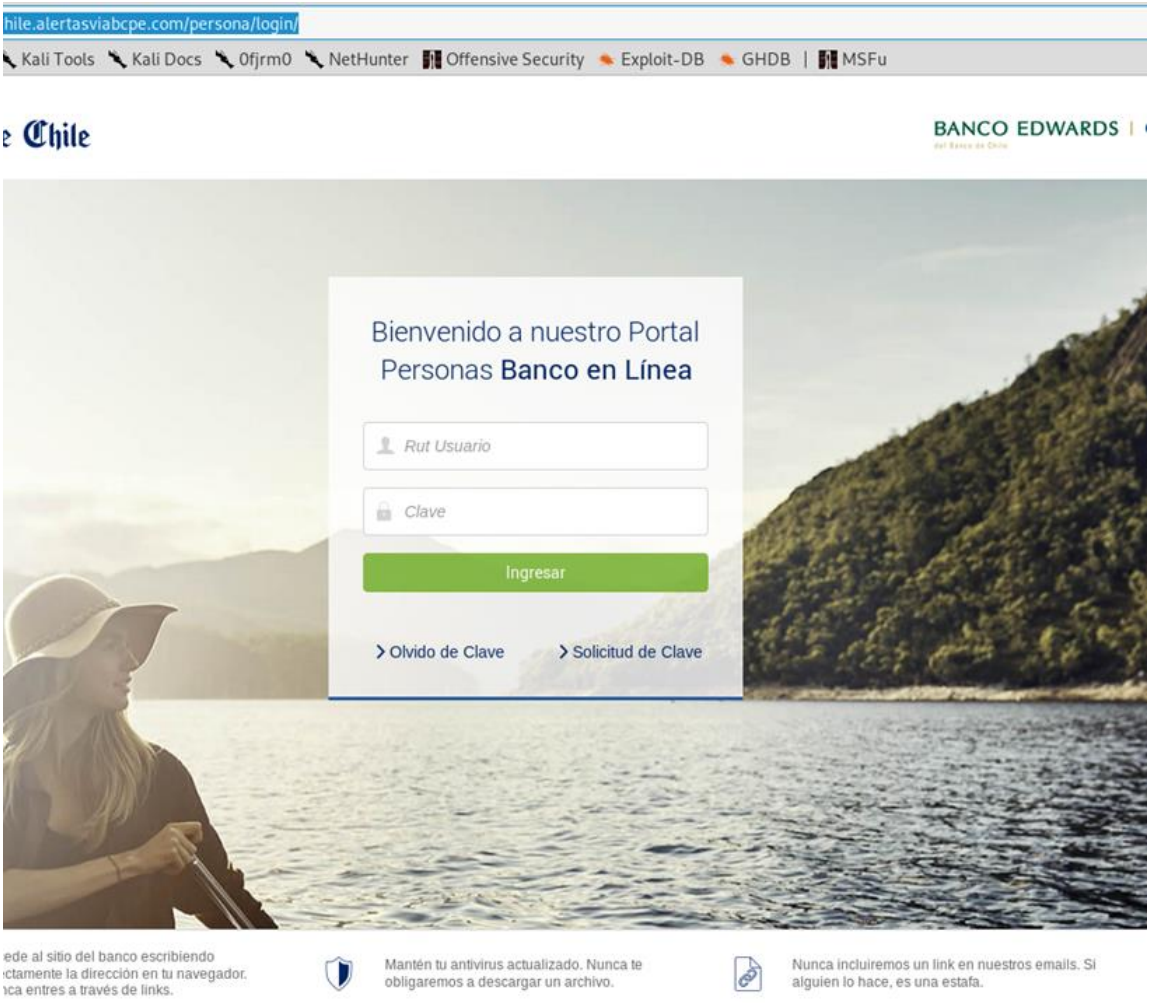
IP´s

186[.]64[.]117[.]225

Localización

Lima, Perú

Ejemplo de Imagen del sitio



Whois

```
Domain Name: ALERTASVIABCPE.COM
Registry Domain ID: 2426416561_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-08-24T17:22:03Z
Creation Date: 2019-08-24T17:22:02Z
Registrar Registration Expiration Date: 2020-08-24T17:22:02Z
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: Marcos Prieto Garcia
Registrant Organization:
Registrant Street: Los Proceres 5523
Registrant City: lima
Registrant State/Province: lima
Registrant Postal Code: 15081
Registrant Country: PE
Registrant Phone: +51.972453675
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: nonedegar@dot-mail.top
Registry Admin ID: Not Available From Registry
Admin Name: Marcos Prieto Garcia
Admin Organization:
Admin Street: Los Proceres 5523
Admin City: lima
Admin State/Province: lima
Admin Postal Code: 15081
Admin Country: PE
Admin Phone: +51.972453675
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: nonedegar@dot-mail.top
Registry Tech ID: Not Available From Registry
Tech Name: Marcos Prieto Garcia
Tech Organization:
Tech Street: Los Proceres 5523
Tech City: lima
Tech State/Province: lima
Tech Postal Code: 15081
Tech Country: PE
Tech Phone: +51.972453675
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: nonedegar@dot-mail.top
Name Server: ns1.dnshosty.net
Name Server: ns2.dnshosty.net
Name Server: ns3.dnshosty.net
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: 2019.08.27
17:32:04 -04'00'