Alerta de seguridad informática	**8FFR-00067-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**23 de Septiembre de 2019**
Última revisión	**23 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 dos sitios fraudulentos asociados a IP's que suplantan la web oficial de Banco ESTADO, lo 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

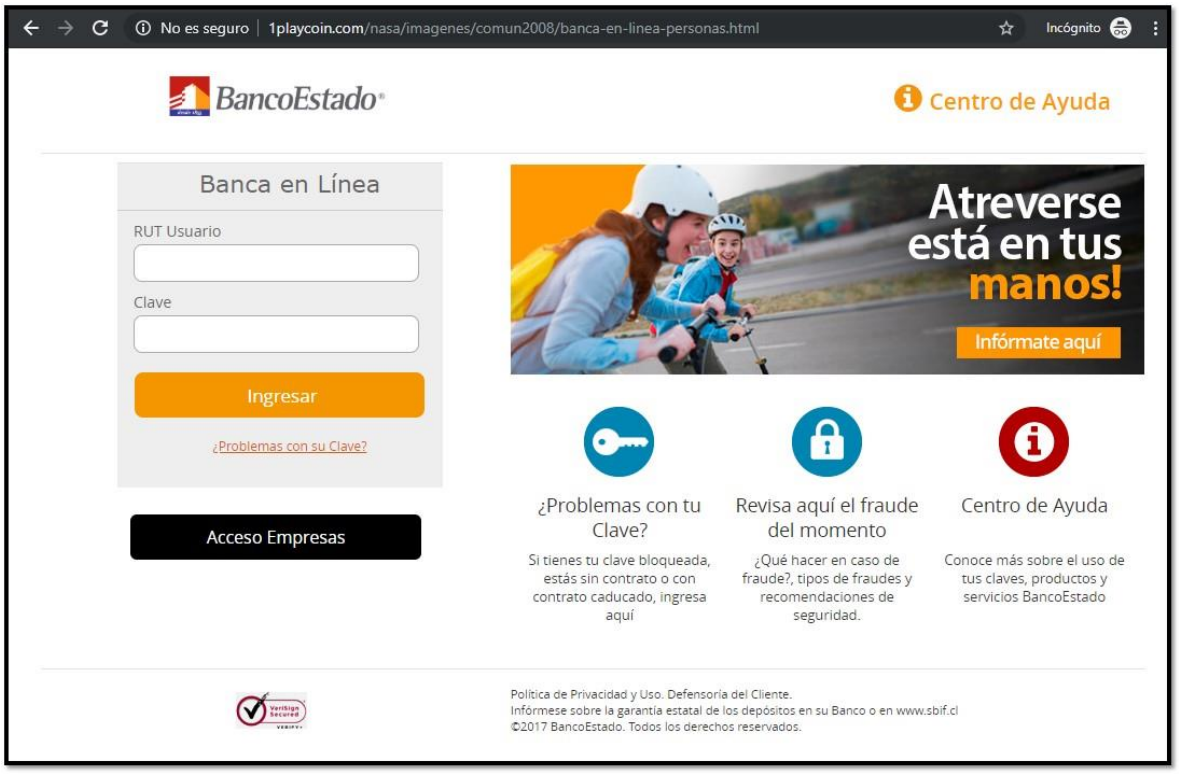
URL´s
http[://]1playcoin[.]com/nasa/imagenes/comun2008/banca-en-linea-personas[.]html
Spanet[.]site/sql/beneficios/consultoriomedico[.]online/sql/beneficios/

Ambas direcciones redirigen a la siguiente URL:
http[://]1playcoin[.]com/nasa/imagenes/comun2008/banca-en-linea-personas[.]html

IP´s
198[.]37[.]123[.]235

Localización
La Jolla, California, Estados Unidos

Ejemplo de Imagen del sitio



Whois

```
Domain Name: lplaycoin.com
Registry Domain ID: 2432469881_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-09-12T07:00:00Z
Creation Date: 2019-09-12T07:00:00Z
Registrar Registration Expiration Date: 2020-09-12T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: romero fajardo
Registrant Organization:
Registrant Street: Argomedo Ndeg 588
Registrant City: santiago
Registrant State/Province: santiago
Registrant Postal Code: 0056
Registrant Country: CL
Registrant Phone: +56.935949583
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: romero.gajardo88@gmail.com
Registry Admin ID:
Admin Name: romero fajardo
Admin Organization:
Admin Street: Argomedo Ndeg 588
Admin City: santiago
Admin State/Province: santiago
Admin Postal Code: 0056
Admin Country: CL
Admin Phone: +56.935949583
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: romero.gajardo88@gmail.com
Registry Tech ID:
Tech Name: romero fajardo
Tech Organization:
Tech Street: Argomedo Ndeg 588
Tech City: santiago
Tech State/Province: santiago
Tech Postal Code: 0056
Tech Country: CL
Tech Phone: +56.935949583
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: romero.gajardo88@gmail.com
Name Server: DNS69.SERVIDORESPH.COM
Name Server: DNS70.SERVIDORESPH.COM
DNSSEC: unsigned
```

```
soc@kali:~$ whois -h whois.namesilo.com lplaycoin.com
Domain Name: lplaycoin.com
Registry Domain ID: 2432469881_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-09-12T07:00:00Z
Creation Date: 2019-09-12T07:00:00Z
Registrar Registration Expiration Date: 2020-09-12T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: romero fajardo
Registrant Organization:
Registrant Street: Argomedo Ndeg 588
Registrant City: santiago
Registrant State/Province: santiago
Registrant Postal Code: 0056
Registrant Country: CL
Registrant Phone: +56.935949583
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: romero.gajardo88@gmail.com
Registry Admin ID:
Admin Name: romero fajardo
Admin Organization:
Admin Street: Argomedo Ndeg 588
Admin City: santiago
Admin State/Province: santiago
Admin Postal Code: 0056
Admin Country: CL
Admin Phone: +56.935949583
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: romero.gajardo88@gmail.com
Registry Tech ID:
Tech Name: romero fajardo
Tech Organization:
Tech Street: Argomedo Ndeg 588
Tech City: santiago
Tech State/Province: santiago
Tech Postal Code: 0056
Tech Country: CL
Tech Phone: +56.935949583
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: romero.gajardo88@gmail.com
Name Server: DNS69.SERVIDORESPH.COM
Name Server: DNS70.SERVIDORESPH.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: 2019.09.23 23:28:45 -03'00'