Alerta de seguridad informática	**8FFR-00065-001**
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 internacional**, 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[://]aumts.com/modules/chile/www[.]bancointernacional[.]cl/

IP´s
162[.]241[.]252[.]218

Localización
Provo, Utah, Estados Unidos

Ejemplo de Imagen del sitio

Whois

```
soc@kali:~$ whois -h whois.bluehost.com aumts.com
Domain Name: AUMTS.COM
Registry Domain ID: 2347896600_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.bluehost.com
Registrar URL: http://www.bluehost.com/
Updated Date: 2018-12-29T12:08:43Z
Creation Date: 2018-12-29T12:08:42Z
Registrar Registration Expiration Date: 2019-12-29T12:08:42Z
Registrar: FastDomain Inc.
Registrar IANA ID: 1154
Registrar Abuse Contact Email: support@bluehost.com
Registrar Abuse Contact Phone: +1.8017659400
Reseller: BlueHost.Com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Registrant Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Registrant Street: 10 CORPORATE DR, STE 300
Registrant City: BURLINGTON
Registrant State/Province: MASSACHUSETTS
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8017659400
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: WHOIS@BLUEHOST.COM
Registry Admin ID:
Admin Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Admin Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Admin Street: 10 CORPORATE DR, STE 300
Admin City: BURLINGTON
Admin State/Province: MASSACHUSETTS
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8017659400
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: WHOIS@BLUEHOST.COM
Registry Tech ID:
Tech Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Tech Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Tech Street: 10 CORPORATE DR, STE 300
Tech City: BURLINGTON
Tech State/Province: MASSACHUSETTS
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8017659400
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: WHOIS@BLUEHOST.COM
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.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: 2019.09.17 08:42:08 -03'00'