Alerta de seguridad informática	**8FFR-00057-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**13 de Septiembre de 2019**
Última revisión	**13 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 102 portales fraudulentos asociados a una IP que suplantan el sitio web oficial del **Banco de 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 de redirección:
www[.]aumento-cupo-bancochile[.]gq
www[.]bchile-aliados-cupo-de-avance[.]cf
portal-aliados-cupo-de-avance[.]cf
portal-aliados-cupo-de-avance[.]gq
www[.]portal-aliados-cupo-de-avance[.]gq
bchile-aliados-cupo-de-avance[.]cf
www[.]portal-aliados-cupo-de-avance[.]cf
web-aliados-travel-avances[.]cf
site-web-bchile-aliados-avance-cl[.]cf
bchile-aliados-cupo-de-avance[.]gq
www[.]web-aliados-travel-avances[.]cf
www[.]web-aliados-cupo-de-avances[.]gq
web-aliados-cupo-de-avances[.]gq
www[.]site-web-bchile-aliados-avance-cl[.]cf
www[.]web-aliados-cupo-de-avances[.]cf
www[.]bchile-aliados-cupo-de-avance[.]gq
web-aliados-cupo-de-avances[.]cf
site-web-aliados-avance[.]cf
site-web-aliados-avance-cl[.]gq
site-web-bchile-aliados-avance-cl[.]gq
www[.]site-web-aliados-avance-cl[.]gq
www[.]site-web-bchile-aliados-avance-cl[.]gq
www[.]web-aliados-avance-online[.]cf
web-aliados-avance-online[.]gq
www[.]site-web-aliados-avance[.]gq
site-web-aliados-avance[.]gq
www[.]web-aliados-avance-online[.]gq
web-aliados-avance-online[.]cf
www[.]aumento-cupo-consulta-web-aliados[.]cf
aumento-cupo-consulta-web-aliados[.]gq
aumento-cupo-consulta-web-aliados[.]cf
aumento-avance-consulta-web-aliados[.]gq
aumento-avance-consulta-web-aliados[.]cf
www[.]aumento-avance-consulta-web-aliados[.]cf
portal-aumento-cupo-web-aliados[.]gq
www[.]portal-aumento-cupo-web-aliados[.]gq
aumento-cupo-generico-consulta-web-aliados[.]gq
aumento-cupo-generico-consulta-web-aliados[.]cf
avance-servicio-web-personas[.]cf
www[.]aumento-cupo-generico-consulta-web-aliados[.]gq
www[.]aumento-cupo-generico-consulta-web-aliados[.]cf
www[.]avance-servicio-web-personas[.]cf

avance-servicio-web-ssl[.]gq
www[.]avance-servicio-web-ssl[.]gq
www[.]login-avance-servicio-web-cl[.]gq
login-avance-servicio-web-cl[.]gq
www[.]login-avance-servicio-cl[.]gq
login-aumento-cupo-bchile[.]cf
login-aumento-de-avance-bchile[.]gq
www[.]login-aumento-de-avance-bchile[.]gq
www[.]login-aumento-de-avance-bchile[.]cf
login-aumento-de-avance-bchile[.]cf
www[.]login-aumento-cupo-bchile[.]cf
login-avance-servicio-cl[.]gq
login-aumento-cupo-bchile[.]gq
www[.]login-aumento-cupo-bchile[.]gq
www[.]login-bch-avance-de-cupos[.]cf
login-bch-avance-de-cupos[.]gq
login-aumentocupos-destacados[.]cf
www[.]login-bch-avance-de-cupos[.]gq
www[.]login-aumentocupos-destacados[.]cf
aumentocupos-login-portal-bch[.]cf
www[.]login-aumentocupos-destacados[.]gq
aumento-cupo-travel-compras[.]cf
www[.]aumentocupos-login-portal-bch[.]cf
www[.]aumento-cupo-travel-compras[.]cf
login-aumentocupos-destacados[.]gq
aumento-cupo-promociones[.]cf
www[.]aumento-cupo-promociones[.]cf
www[.]aumento-cupo-travel-compras[.]gq
aumento-cupo-travel-compras[.]gq
login-aumento-cupo-banchile[.]gq
login-aumento-cupo-banchile[.]cf
www[.]login-aumento-cupo-banchile[.]gq
www[.]login-aumento-cupo-banchile[.]cf
login-aumento-cupo-bancochile[.]cf
www[.]login-aumento-cupo-bancochile[.]cf
aumento-cupo-bancochile[.]cf
aumento-cupo-bancochile[.]gq
www[.]aumento-cupo-bancochile[.]cf
www[.]site-web-aliados-avance[.]cf
www[.]aumento-avance-consulta-web-aliados[.]gq
www[.]avance-servicio-web-ssl[.]cf
avance-servicio-web-ssl[.]cf
avance-servicio-web[.]cf
www[.]avance-servicio-web[.]cf
www[.]login-avance-servicio-cl[.]cf

login-avance-servicio-cl[.]cf
login-bch-avance-de-cupos[.]cf
www[.]aumento-cupo-promociones[.]gq
aumento-cupo-promociones[.]gq
www[.]aumento-cupo-consulta-web-aliados[.]gq
www[.]avance-servicio-web[.]gq
avance-servicio-web[.]gq
www[.]login-aumento-cupo-bancochile[.]gq
login-aumento-cupo-bancochile[.]gq
aumentocupos-login-portal-bch[.]gq
aumento-beneficios-cupo-web[.]gq
auemnto-de-avance-online[.]cf
avance-diferido-online[.]cf
avance-cupo-beneficios[.]cf
www-login-avance-de-cupo[.]cf

IP´s
178[.]159[.]36[.]236

Localización
Moscú, Moscú, Federación Rusa

Whois

```
domain:       GQ

organisation: GETESA
address:      A.P. 494
address:      Malabo
address:      Equatorial Guinea

contact:      administrative
name:         Jose Antonio Bibang Yembi
organisation: GETESA
address:      A.P. 494
address:      Malabo
address:      Equatorial Guinea
phone:        +240222268239
e-mail:       bibang.yembi@orange-getesa.gq

contact:      technical
name:         Manager ICT
organisation: Equatorial Guinea Domains B.V.
address:      Danzigerkade 23D
address:      1013 AP  Amsterdam
address:      Netherlands
phone:        +31205315726
fax-no:       +31205315721
e-mail:       info@equatorialguineadomains.com

nserver:      A.NS.GQ 185.21.168.65 2a04:1b00:10:0:0:0:0:1
nserver:      B.NS.GQ 185.21.169.65 2a04:1b00:11:0:0:0:0:1
nserver:      C.NS.GQ 185.21.170.65 2a04:1b00:12:0:0:0:0:1
nserver:      D.NS.GQ 185.21.171.65 2a04:1b00:13:0:0:0:0:1

whois:        whois.dominio.gq

status:       ACTIVE
remarks:      Registration information: http://www.dominio.gq

created:      1997-07-10
changed:      2015-12-24
source:       IANA
```

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: 2019.09.13
15:57:45 -03'00'