

Alerta de seguridad informática	8FFR-00026-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Agosto de 2019
Última revisión	23 de Agosto de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC 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 134 portales fraudulentos asociados a una IP que suplantan el sitio web oficial del **bancochile.cl** los que podrían 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

avance-cupo-de-tarjeta-web[.]gq
avance-linea-credito-web[.]gq
aumento-avance-web[.]cf
www-consulta-web-aumento-cupo[.]cf
login-avance-cupo-linea-credito[.]gq
www-avance-de-tarjeta-credito-bchile[.]gq
login-aumento-avance-web[.]cf
www-consulta-web-aumento[.]cf
portal-servicios-aumento-cupo[.]cf
avance-compras-online-web[.]gq
www[.]www-web-servicio-de-avance[.]cf
www-web-servicio-de-avance[.]cf
www-avance-de-tarjeta-credito-bchile[.]cf
www[.]www-consulta-online-de-avances[.]cf
www[.]avance-compras-online-web[.]gq
aumento-cupo-solicitud-virtual[.]cf
avance-compras-online-web[.]cf
web-cupo-de-avance-travel[.]cf
www-consulta-online-de-avances[.]cf
portal-de-avance-confirmacion[.]cf
web-aumento-de-avance-travel[.]cf
www-web-aumento-cupo-de-tarjeta[.]cf
web-cupo-de-avance-ssl[.]cf
consulta-online-de-avance[.]cf
www-consulta-online-de-avances[.]gq
portal-servicios-aumento-cupo[.]gq
www-web-servicio-de-avance[.]gq
www-consulta-web-aumento[.]gq
aumento-cupo-verificacion-web[.]gq
consulta-online-de-avance[.]gq
www-consulta-web-de-avance[.]gq
solicitud-avance-online[.]cf
web-cupo-de-avance-ssl[.]gq
web-aumento-de-avance-compras-online[.]gq
www-consulta-web-avances[.]gq
www[.]portal-servicios-aumento-cupo[.]cf
www-consulta-web-avances[.]cf
www-consulta-web-de-avance[.]cf
portal-de-avance-confirmacion[.]gq
www[.]portal-servicios-aumento-cupo[.]gq
www[.]www-web-servicio-de-avance[.]gq

www[.]www-avance-de-tarjeta-credito-bchile[.]cf
www-web-aumento-cupo-de-tarjeta[.]gq
www[.]www-avance-de-tarjeta-credito-bchile[.]gq
www[.]www-web-aumento-cupo-de-tarjeta[.]cf
www[.]www-web-aumento-cupo-de-tarjeta[.]gq
www[.]solicitud-avance-online[.]gq
web-aumento-de-avance-compras-online[.]cf
www[.]web-aumento-de-avance-compras-online[.]cf
www[.]avance-compras-online-web[.]cf
web-aumento-de-avance-travel[.]gq
www[.]web-aumento-de-avance-travel[.]cf
www[.]web-aumento-de-avance-travel[.]gq
www[.]web-cupo-de-avance-travel[.]cf
www[.]web-cupo-de-avance-ssl[.]gq
www[.]web-cupo-de-avance-travel[.]gq
web-cupo-de-avance-travel[.]gq
www-consulta-web-aumento-cupo[.]gq
www[.]www-consulta-web-aumento-cupo[.]gq
www-web-aumento-cupo-consulta[.]gq
www[.]www-consulta-web-aumento-cupo[.]cf
www[.]www-consulta-web-aumento[.]cf
aumento-avance-web[.]gq
www[.]www-consulta-web-avances[.]gq
www[.]www-consulta-web-avances[.]cf
www[.]www-consulta-web-aumento[.]gq
www[.]www-consulta-web-de-avance[.]cf
login-aumento-avance-web[.]gq
aumento-avance-web-bchile[.]cf
aumento-avance-verificacion-web[.]gq
aumento-cupo-verificacion-web[.]cf
aumento-avance-web-bchile[.]gq
aumento-avance-verificacion-web[.]cf
aumento-cupo-solicitud-virtual[.]gq
www[.]aumento-solicitu-de-cupo[.]gq
www[.]portal-de-avance-confirmacion[.]gq
www[.]portal-de-avance-confirmacion[.]cf
www[.]consulta-online-de-avance[.]cf
www[.]consulta-online-de-avance[.]gq
www[.]solicitud-avance-online[.]cf
www[.]aumento-cupo-solicitud-virtual[.]cf
www[.]aumento-cupo-solicitud-virtual[.]gq
www[.]aumento-avance-web-bchile[.]cf
www[.]aumento-avance-web-bchile[.]gq
www[.]login-aumento-avance-web[.]cf
www[.]login-aumento-avance-web[.]gq

www[.]aumento-avance-web[.]cf
www[.]aumento-avance-verificacion-web[.]gq
www[.]aumento-cupo-verificacion-web[.]cf
www[.]aumento-cupo-verificacion-web[.]gq
www[.]aumento-avance-verificacion-web[.]cf
www-consulta-de-cupo[.]cf
www[.]www-aumento-cupo-web-segura[.]cf
www-portal-web-de-avances[.]cf
www-web-de-avances[.]cf
www-aumento-cupo-web-segura[.]cf
consulta-avance-en-linea[.]gq
www[.]www-aumento-cupo-web-segura[.]gq
www-aumento-cupo-web-segura[.]gq
personas-validacion-de-avance[.]cf
personas-validacion-de-avance[.]gq
www[.]www-activacion-de-aumento-cupo[.]cf
www-activacion-de-aumento-cupo[.]cf
www[.]www-web-de-aumento-cupo[.]cf
www-activacion-de-aumento-cupo[.]gq
www-web-de-aumento-cupo[.]cf
www[.]www-activacion-de-aumento-cupo[.]gq
www[.]www-web-de-aumento-cupo[.]gq
www-portal-web-de-avances[.]gq
www[.]www-web-de-avances[.]gq
www[.]www-portal-web-de-avances[.]cf
www[.]www-portal-web-de-avances[.]gq
www[.]avance-cupo-de-tarjeta-web[.]cf
www[.]avance-linea-credito-web[.]cf
avance-linea-credito-web[.]cf
consulta-avance-en-linea[.]cf
www[.]validacion-de-avance[.]cf
validacion-de-avance[.]cf
www[.]consulta-avance-en-linea[.]cf
www[.]personas-validacion-de-avance[.]cf
www[.]personas-validacion-de-avance[.]gq
avance-web-de-cupo[.]gq
www-avance-linea-credito-activo[.]gq
avance-web-de-cupo[.]cf
login-verificacion-de-avance[.]cf
www-personas-cupo-de-avance[.]cf
login-cupo-linea-credito-aumento[.]cf
avance-linea-credito-diferido[.]gq
aumento-de-cupo-descuento-online[.]gq
www[.]www-avance-linea-credito-activo[.]gq
avance-de-cupo-promocional[.]gq

www-avance-linea-credito-activo[.]cf
consulta-cupo-aumento-web-autorizado[.]gq
aumento-de-cupo-travel-promociones[.]cf

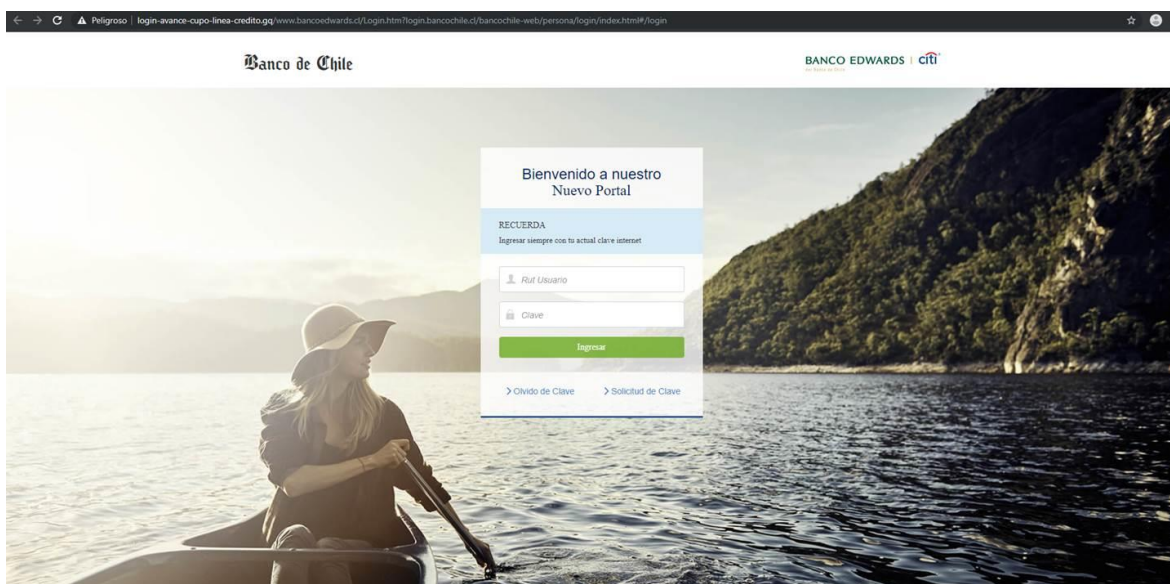
IP's

178.159.36.177

Localización

Federación Rusa, Moscú.

Ejemplo de Imagen del sitio



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