Alerta de Seguridad Informática (8FPH-00036-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 20 de Junio de 2019 | Última revisión 20 de Junio 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 41 dominios de suplantación del Banco Chile que intentan engañar a los clientes utilizando técnicas de phishing. Los delincuentes intentan convencer a sus víctimas a través de correos electrónicos u otro medios para que accedan a los sitios aquí indicados, con la finalidad de que los clientes entreguen sus credenciales de acceso a sus cuentas bancarias.

Indicadores de compromisos

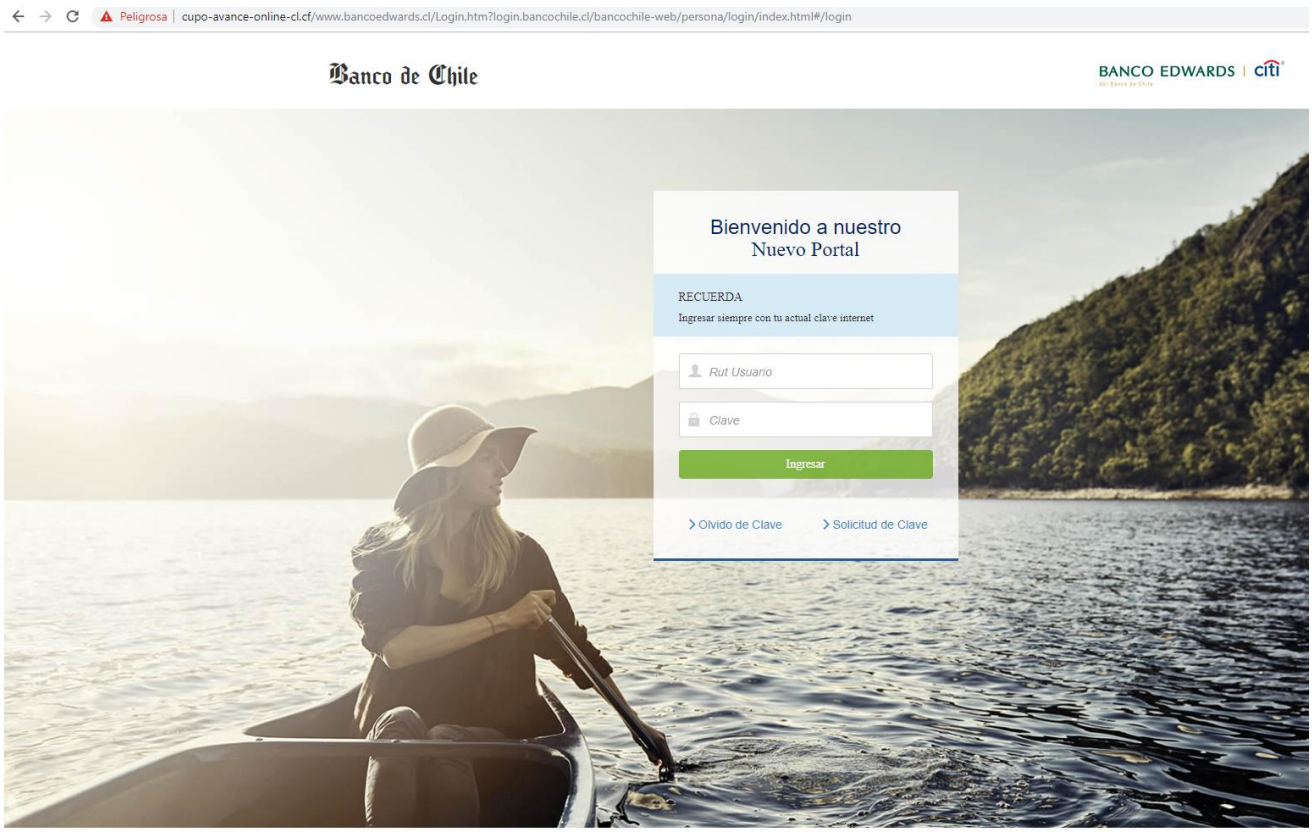
IP: 91.209.70.21

Url's:

aumento-cupo-diferido-cl[.]cf
aumento-cupo-diferido-cl[.]gq
avance-activo-en-cuotas-cl[.]cf
avance-cupo-diferido-cl[.]gq
avance-cupo-diferido-personas-cl[.]cf
avance-cupo-diferido-personas-cl[.]gq
avance-cupo-simulador-web[.]gq
avance-de-aumento-cl[.]cf
avance-de-aumento-cl[.]gq
avance-en-linea-diferido-web-cl[.]cf
avance-en-linea-diferido-web-cl[.]gq
avance-personas-cuotas-diferido-cl[.]cf
avance-personas-cuotas-diferido-cl[.]gq
avances-cuotas-diferido-promo-cl[.]cf
avances-cuotas-diferido-promo-cl[.]gq
avance-web-confirmacion-cl[.]cf
avance-web-confirmacion-cl[.]gq
cupo-avance-credito-en-linea-cl[.]cf
cupo-avance-credito-en-linea-cl[.]gq
cupo-avance-online-cl[.]cf
cupo-avance-online-cl[.]gq
cupo-prestamo-cl[.]cf
cupo-web-avance-cl[.]gq
solicitud-avance-cupo-en-linea-cl[.]gq
web-avance-en-linea-cl[.]cf
web-avance-en-linea-cl[.]gq

www[.]aumento-cupo-diferido-cl[.]cf
www[.]aumento-cupo-diferido-cl[.]gq
www[.]avance-activo-en-cuotas-cl[.]cf
www[.]avance-cupo-diferido-cl[.]cf
www[.]avance-cupo-diferido-personas-cl[.]cf
www[.]avance-cupo-simulador-web[.]gq
www[.]avance-de-aumento-cl[.]gq
www[.]avance-en-linea-diferido-web-cl[.]cf
www[.]avance-en-linea-diferido-web-cl[.]gq
www[.]avances-cuotas-diferido-promo-cl[.]cf
www[.]cupo-avance-online-cl[.]cf
www[.]cupo-avance-online-cl[.]gq
www[.]cupo-prestamo-cl[.]cf
www[.]cupo-web-avance-cl[.]gq
www[.]web-avance-en-linea-cl[.]gq

Imagen de muestra



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob