Alerta de Seguridad Informática (8FPH-00030-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 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 26 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.

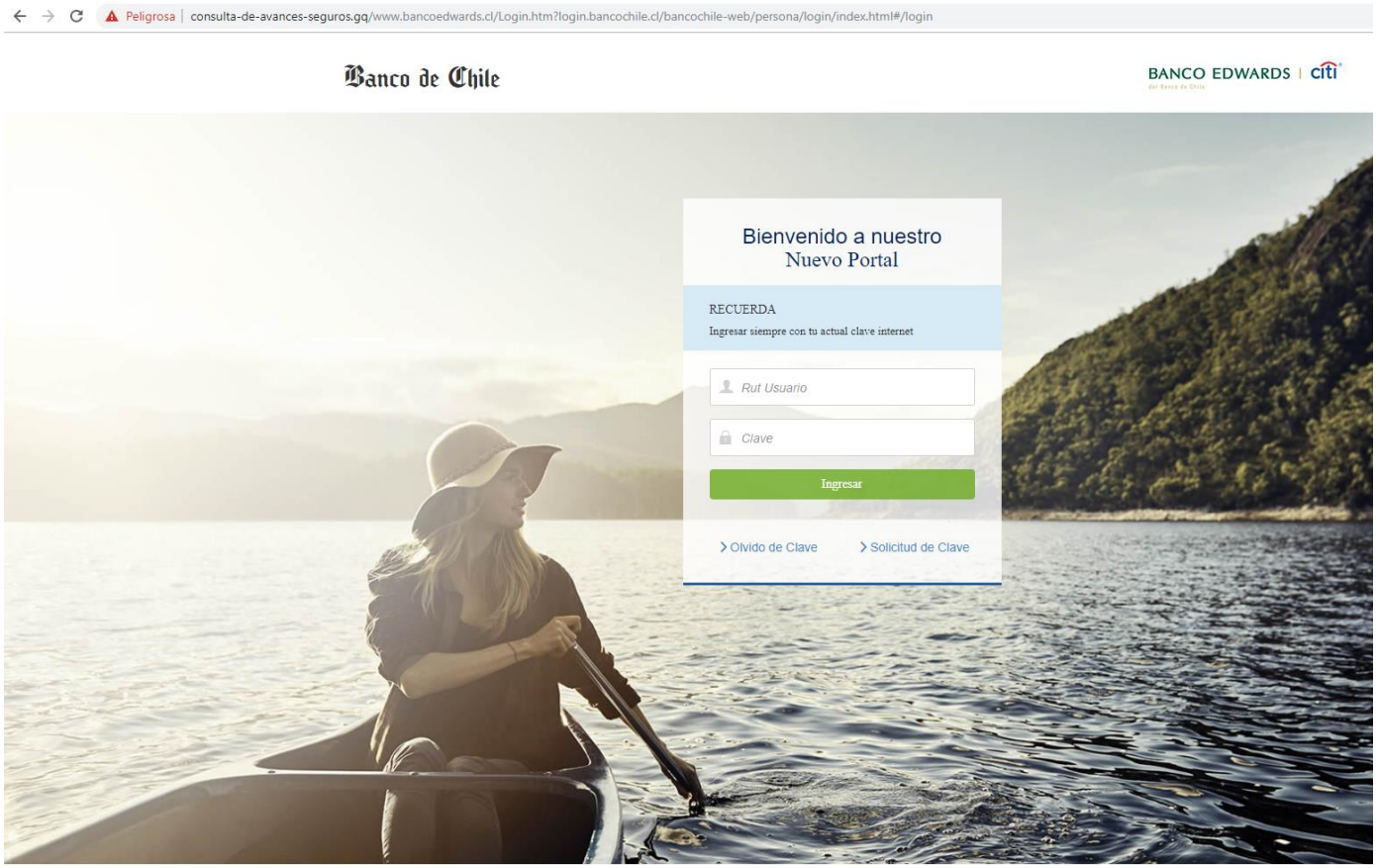
Indicadores de compromisos

IP: 178.159.36.74

Url's:

acceso-avance-en-linea-seguro-cl[.]gq
activacion-avances-web-segura[.]gq
avances-promo-en-linea-seguros-cl[.]gq
avances-seguros-en-bchile-web[.]gq
consulta-avances-bchile-edwards-web[.]gq
consulta-de-avances-seguros[.]gq
consulta-web-avances-cl[.]gq
credito-de-avances-web-personas[.]gq
ingreso-balance-cupo-online[.]gq
ingreso-personas-credito-web[.]gq
ingreso-seguro-avances-web[.]gq
ingreso-web-cupo-credito-consumo-cl[.]gq
personas-avances-seguro-web-cl[.]gq
personas-balance-web-cl[.]gq
portal-avances-bchile-wen-segura-cl[.]gq
portal-edwards-avances-en-linea-cl[.]gq
login-avances-bchile-reporte-web[.]gq
promo-prima-avances-online-cl[.]gq
registro-de-avances-online[.]gq
servicios-de-avance-cupo-online[.]gq
soporte-avances-en-linea-seguros-cl[.]gq
web-avances-consultas[.]gq
web-bchile-avances-rapido-seguro-cl[.]gq
web-consulta-de-avances-cl[.]gq
web-consultas-personas[.]gq
web-edwards-avances-seguro-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