Alerta de Seguridad Informática (8FPH-00042-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 12 de Julio de 2019 | Última revisión 12 de Julio 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 identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco de Chile. El correo trata de persuadir a los clientes indicándoles que tiene un premio de $500.0000 mil pesos en su línea de crédito, para que lo gaste en lo que desee. Para reclamar el premio el usuario debe actualizar sus datos. Al hacerlo, también participará de un sorteo de 30 ipads mini y 20 televisores 4k. Se indica en el correo que los días 15 de cada mes será publicado el sorteo en el sitio web y además serán notificados vía telefónica. Una vez que el usuario supuestamente actualiza sus datos a través del enlace, es redirigido a un sitio semejante al de Banco Chile.

> “Estos casos de phishing 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 phishing, 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”

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- http[:]//www[.]portalbanca.ns3[.]name
- http[:]//www[.]webportal.dns04[.]com
- http[:]//www[.]portalbanca1.ddns[.]info
- http[:]//www[.]portalclientes1.ns02[.]us
- http[:]//www[.]portalbanca4.port25[.]biz
- http[:]//www[.]portalclientes1.ns02[.]us
- http[:]//www[.]portalbanca.ns3[.]name
- http[:]//www[.]clientesportal.ddns[.]info
- https[:]//view-contenido[.]website
- https[:]//www[.]portalwebsite[.]site/portal/bancochile/wps/wcm/connect/Personas/Portal/public/cliente
- https[:]//view-contenido[.]website

Smtp Host

- [64[.]44[.]34[.]112]
- [64[.]44[.]34[.]102]
- choff002[.]manage-smtpbz[.]pro
- choff003[.]manage-smtpbz[.]pro
- choff001[.]manage-smtpbz[.]pro
- [64[.]44[.]34[.]11]
- [64[.]44[.]34[.]10]
- [64[.]44[.]34[.]111]

Sender

admin@agroindustrial[.]net
enviodigital@mailer-promociones[.]com
admin@centaurodelasvilcas[.]com
admin@tradicionesverdes[.]com
contactos@eeccvirtual[.]com
newsletter@mail-promociones[.]com

Subject:

Banco de Chile tiene un abono de $ 500.000 al instante
Banco de Chile tiene un abono de $ 500.000 apruebalo ya
Banco de Chile tiene un abono para ti de $ 500.000
Banco de Chile te obsequia $ 500.000 aprovechalos

Imagen Phishing correo

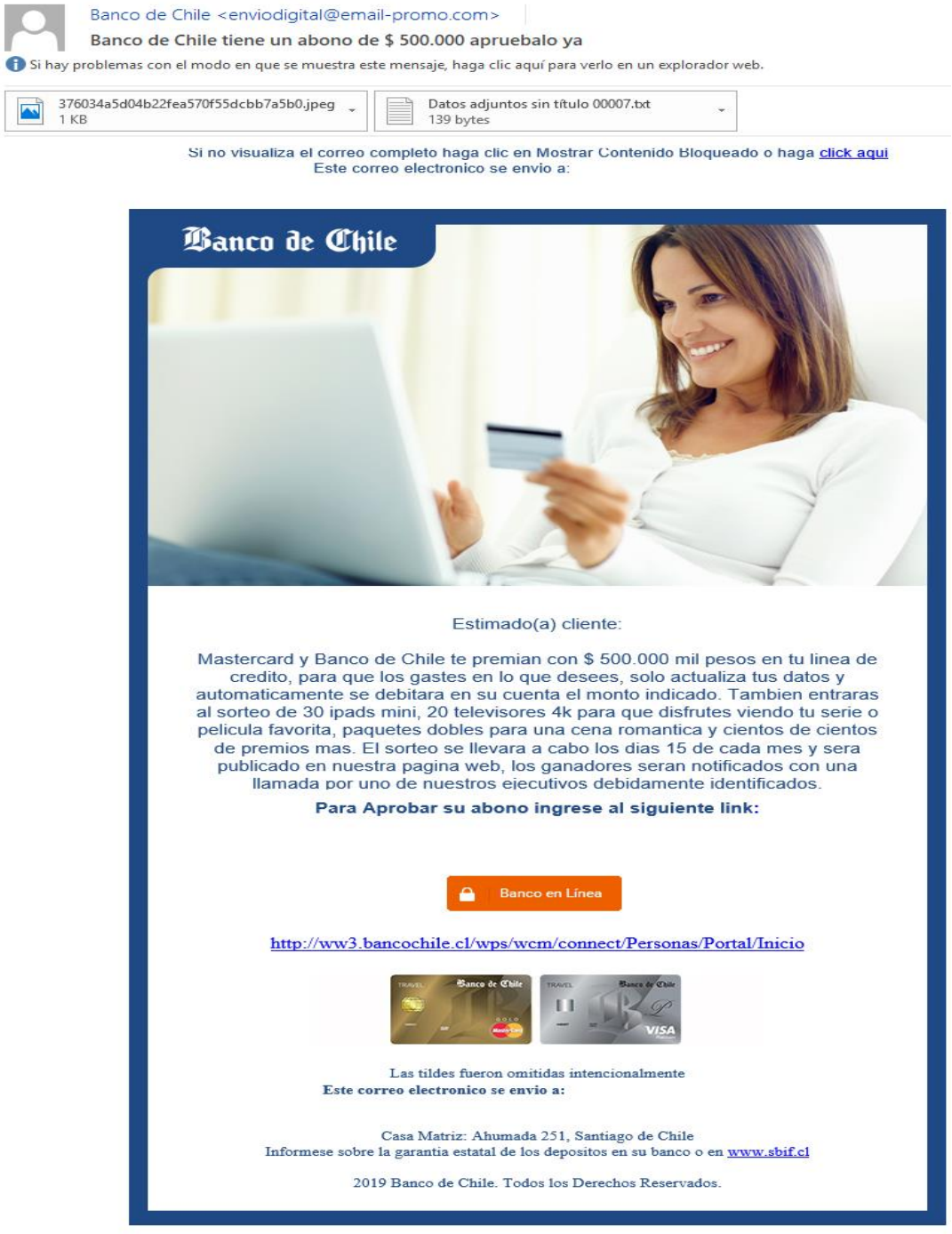
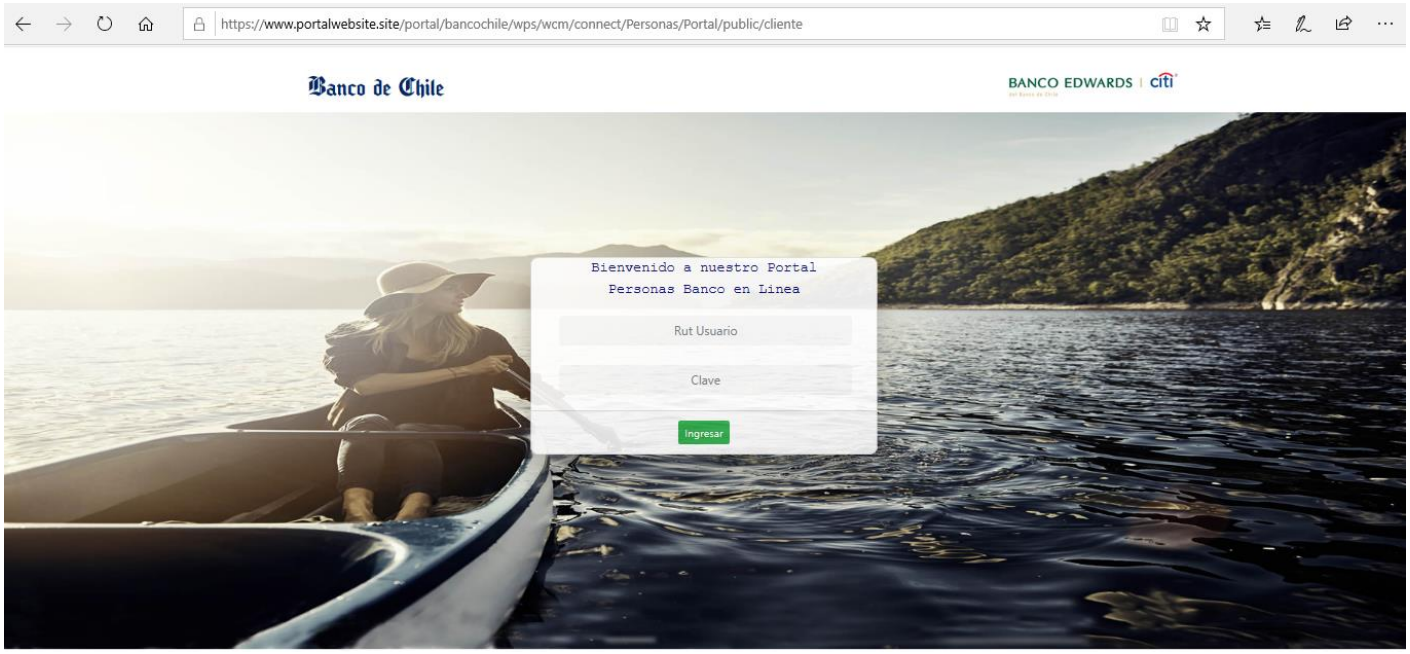


Imagen Sitio Web



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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
- Visualizar los sitios web que se ingresen que sean los oficiales

Contactos

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