Alerta de seguridad informática	**8FPH-00060-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**09 de Septiembre de 2019**
Última revisión	**09 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 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico dirigido a los usuarios del Banco de Chile. El mensaje del correo intenta persuadir a los usuarios de ingresar a un hipervínculo como parte del procedimiento para sincronizar su digipass. A través del uso de técnicas de ingeniería social, los criminales tratan de engañar a las personas enfatizando la urgencia de realizar este trámite a través de la banca de internet en un plazo máximo de 48 horas tras la recepción del correo, de lo contrario su cuenta sería inhabilitada y obligaría a la persona a realizar el trámite directamente en la sucursal más cercana para solicitar una nueva tarjeta. Si la persona llega a ingresar al hipervínculo señalado, se expone a que el atacante robe sus credenciales desde un sitio semejante al original del Banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

http://wzwpay[.]com/25ca4587b603f944540e48f8fe39fb82
https://bossabons[.]com/lbancobechileportaln

Smtp Host

hwsrv-588407[.]hostwindsdns[.]com [104.168.219.209]
hwsrv-588378[.]hostwindsdns[.]com [104.168.147.77]

From:

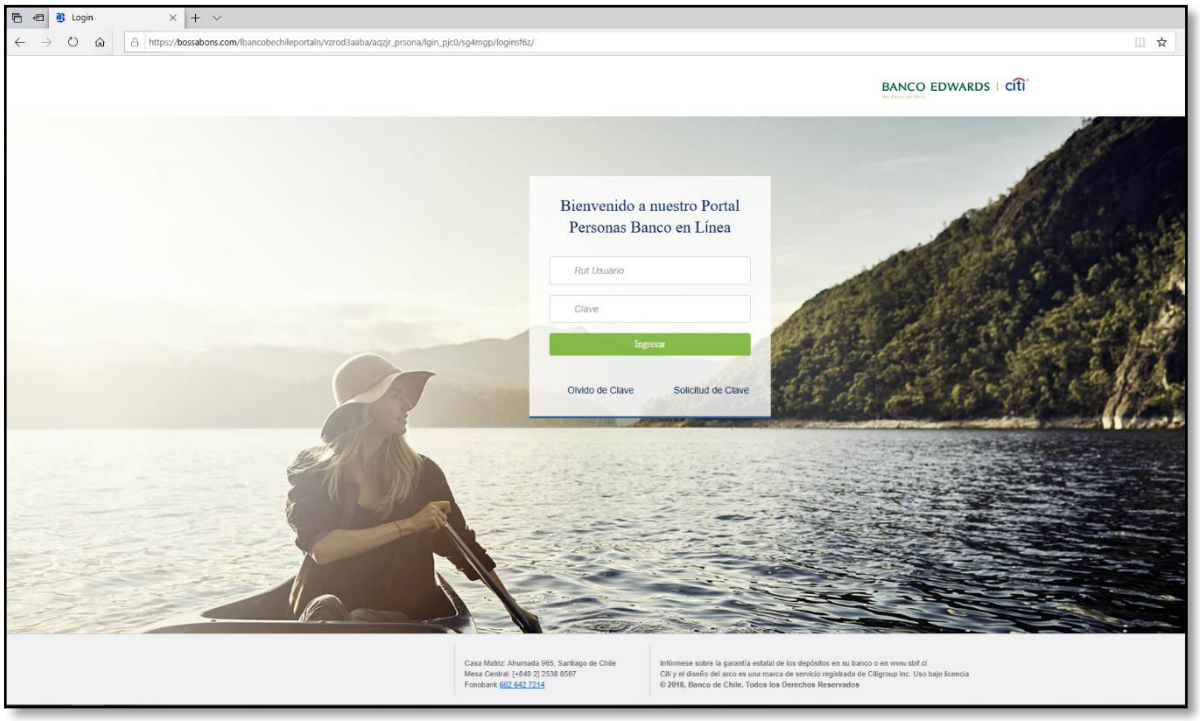
root@hwsrv-588407.hostwindsdns[.]com
root@hwsrv-588378.hostwindsdns[.]com

Subject:

Urgente: Sujeto a bloqueo si no sincroniza su dispositivo
Urgente: Cuenta Bloqueo Temporal

Imagen Phishing Correo

Imagen Sitio Web



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
- Visualizar los sitios web que se ingresen que sean los oficiales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.09 15:04:56 -03'00'