Alerta de Seguridad Informática (8FPH-00050-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 25 de Julio de 2019 | Última revisión 25 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), gracias a la colaboración de un usuario de redes sociales, han identificado una campaña de phishing a través de un correo electrónico que intenta engañar a los usuarios de Apple. El asunto del correo informa sobre el “límite de la cuenta”, pero también apunta a un documento adjunto que informa sobre la intrusión en la cuenta del usuario –temas que no están vinculados- y por ende, la compañía solicita confirmar la identidad del afectado.

El mensaje interno, por su parte, habla específicamente del vencimiento de la membresía del servicio y por eso se habría bloqueado la cuenta, por lo que solicita actualizar los datos a través del enlace que se ofrece en el correo, el cual redirecciona a la persona a un sitio semejante al de Apple, para que entregue sus credenciales.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- http[:]//x[.]co/6nvfO
- https[:]//recibo-seguridad[.]creationwithdrawal[.]com/session

Subject:

- Recordatorio: [Notificación de cuenta] [factura de límite de cuenta] [información de límite de cuenta] [límite de verificación de cuenta] información de límite de su cuenta. #8470100231

Adjunto:

Archivo : documento-intl-actvd#18234233333.dot

MD5 : f4e090e9cf8e4ec5334a5ca64175374f

SHA-256 : 47d94a90efb1f2a362f307ecc825c9dccc799a0ce65009effd1c8c5fe8b78eb0

Imagen Phishing Correo

De: Soporte iCloud
Enviado: miércoles, 24 de julio 15:52
Asunto: Recordatorio: [Notificación de cuenta] [factura de límite de cuenta] [información de límite de cuenta] [límite de verificación de cuenta] información de límite de su cuenta. #8470100231
Para:

attachment for details - Información de la cuenta, alguien ha ingresado a su cuenta, por favor confirme su cuenta. - 24/07/2019

Imagen Documento Adjunto

Estimado Cliente,

Su membresía ha llegado a la fecha de vencimiento aunque el recordatorio fue enviado por correo electrónico

Por lo tanto, bloquearemos inmediatamente su ID de aplicación temporalmente por razones de seguridad.

Para garantizar la confidencialidad de sus datos, debe completer

su renovación de detalle. Actualice su ID de Apple para iniciar sesión de nuevo, como de costumbre
haciendo clic en el siguiente enlace tan pronto como reciba este correo electrónico.

Actualizar detalles asociados con su ID>

Si no recibimos su información en 24 horas, su cuenta será desactivada

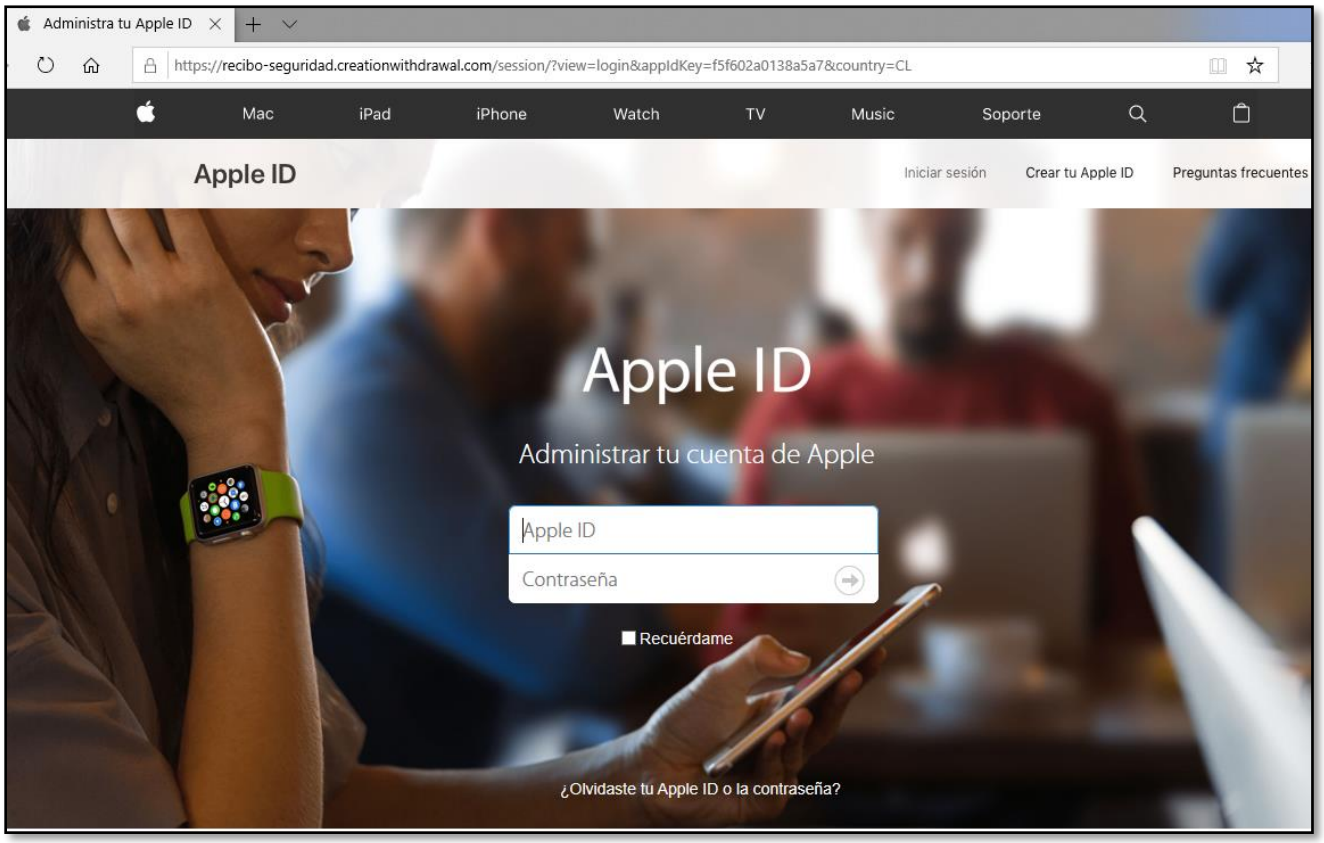
Gracias

Sinceramente,

Equipo soporte Apple

Apple ID | Soporte | Términos de Uso
Copyright © 2019 Apple Todos los derechos reservados

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

Contactos

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

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.07.25
18:07:25 -04'00'