# Alerta de Seguridad Informática (8FPH-00017-001)

## Nivel de Riesgo: Alto

## Tipo: Phishing

Fecha de lanzamiento Original: 08 de Mayo de 2019 | Última revisión 08 de Mayo 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 busca engañar a los usuarios de Apple, requiriendo de ellos la actualización de su información, de lo contrario podría ser suspendida su cuenta en un plazo de 48 horas.

### Indicadores de compromisos

**Url's:**

http[:]//www.varans[.]lv/old/documents//milleradarbnica.html
http[:]//masterlifetravel[.]com/fr/applesx0/home/

**Smtp Host**

163.172.75.15

**From:**

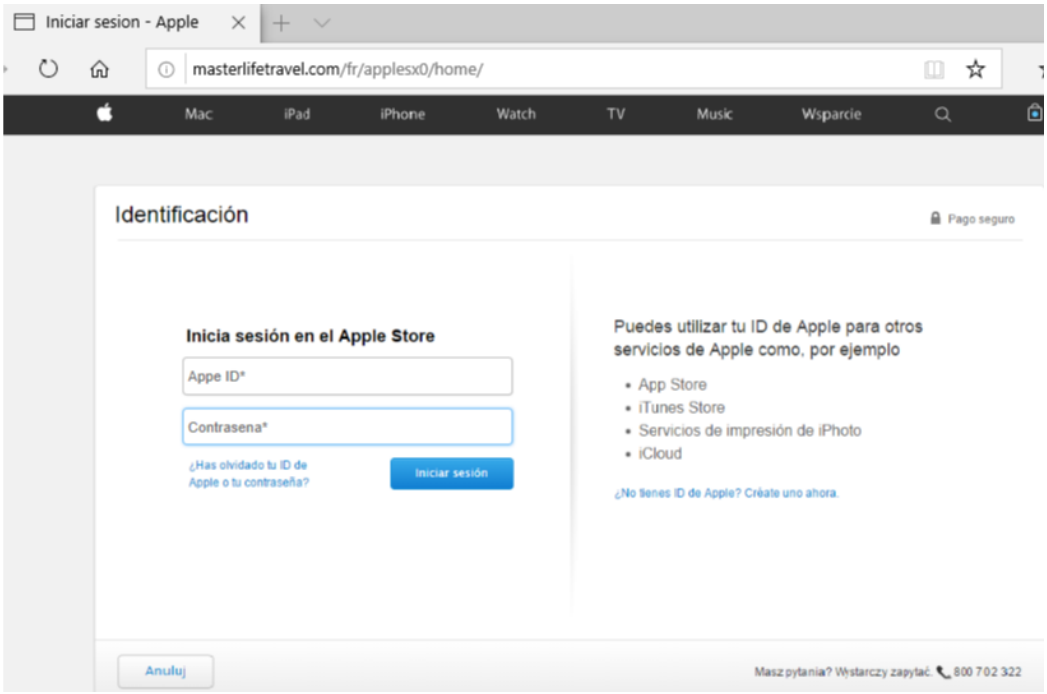
Apple <postmaster@netins.net>

**Subject:**

cuenta de Apple suspendida

## Imágenes


Apple <postmaster@netins.net>
cuenta de Apple suspendida
Apple
Queridos clientes,
Alguna información de su cuenta parece estar incorrecta o falta, actualice su información en un plazo de 48 horas.
Si esto no se hace, nos veremos obligados a suspender su cuenta
actualiza tu información aquí
@2019 Apple.Todos los derechos reservados.


Iniciar sesion - Apple
masterlifetravel.com/fr/applesx0/home/
Mac
iPad
iPhone
Watch
TV
Music
Wsparcie
Identificación
Pago seguro
Inicia sesión en el Apple Store
Appe ID*
Contrasena*
¿Has olvidado tu ID de Apple o tu contraseña?
Iniciar sesión
Puedes utilizar tu ID de Apple para otros servicios de Apple como, por ejemplo
App Store
iTunes Store
Servicios de impresión de iPhoto
iCloud
¿No tienes ID de Apple? Créate uno ahora.
Anuluj
Masz pytania? Wystarczy zapytać: 800 702 322

## 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

## Contactos

https://www.csirt.gov.cl
+(562) 2486 3850
https://www.linkedin.com/company/csirt-gob
@CSIRTGOB