Alerta de seguridad cibernética	8FPH20-00251-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020

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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene de la Compañía de Apple.

El atacante intenta persuadir a la persona para utilizar un enlace malicioso en el cuerpo del correo.

El mensaje del correo informa que se ha detectado un problema con la cuenta, motivo por el cual Apple ha bloqueado la cuenta.

Al seleccionar el enlace para supuestamente evitar la suspensión es dirigido a un sitio falso de Apple, donde se expone al robo de sus credenciales.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromiso

Urls Redirecciones:

Urls sitio falso:
hxxps://limiteced.access.akojagia[.]com/account/?view=login&appIdKey=53bdcc7a4a47bd9&country=CL

Smtp Host
[]

Sender
email.notifications-customer.mails.id-1635665923@cintaole.com

Asunto
Alerta: Información sobre tu servicio - Consulta el estado de tu cuenta.

Otros antecedentes

URL Body SHA-256

afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e

Certificado Digital

Fecha Valido	:	22-06-2020
Fecha Termino	:	21-09-2020
Emitido	:	Cpanel, Inc. Certification Authority

Datos Alojamiento

IP	:	162.241.117.207
Número de sistema autónomo (AS)	:	AS 46606
Etiqueta del sistema autónomo	:	Unified Layer
País	:	Estados Unidos
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	limiteced.access.akojagia[.]com
Estado del dominio	:	clientTransferProhibited
Creado	:	12 de Diciembre del 2019
Expira	:	12 de Diciembre del 2020
Información del registrador	:	Google LLC
ID IANA	:	895
Correo electrónico	:	registrar-abuse@google.com
Servidores de nombres	:	ns-cloud-b1.googledomains.com ns-cloud-b2.googledomains.com ns-cloud-b3.googledomains.com ns-cloud-b4.googledomains.com

Imagen del mensaje

Estimado Cliente,

Recientemente hemos detectado un problema con su cuenta. No podemos verificar la información que proporcionó. Como resultado, su ID de Apple se ha bloqueado por motivos de seguridad.

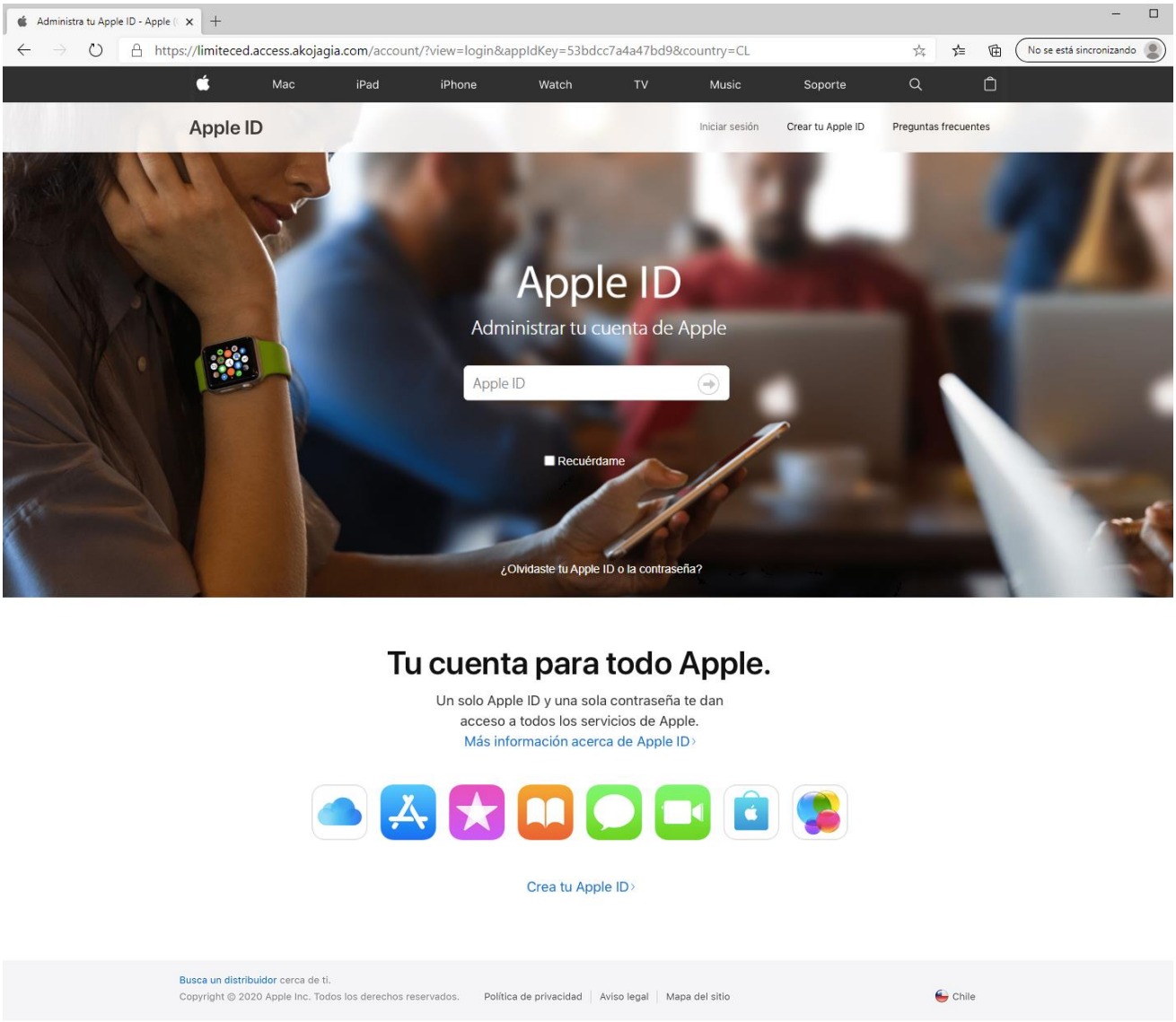
Pedimos disculpas por cualquier inconveniente, pero tenga en cuenta que se necesita algo de tiempo para proteger de manera segura su cuenta y su información.

Para evitar la suspensión de su servicio (dentro de 24 horas), actualice la información de su cuenta:

Verificar Cuenta >

Gracias,
Apple

Imagen del sitio


Administra tu Apple ID - Apple
https://limiteced.access.akojagia.com/account/?view=login&appIdKey=53bdcc7a4a47bd9&country=CL
No se está sincronizando
Mac
iPad
iPhone
Watch
TV
Music
Soporte
Apple ID
Iniciar sesión
Crear tu Apple ID
Preguntas frecuentes
Apple ID
Administrar tu cuenta de Apple
Apple ID
Recuérdame
¿Olvidaste tu Apple ID o la contraseña?
Tu cuenta para todo Apple.
Un solo Apple ID y una sola contraseña te dan acceso a todos los servicios de Apple.
Más información acerca de Apple ID›
Crea tu Apple ID›
Busca un distribuidor cerca de ti.
Copyright © 2020 Apple Inc. Todos los derechos reservados.
Política de privacidad
Aviso legal
Mapa del sitio
Chile

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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 sean los oficiales.