Alerta de seguridad informática	8FPH23-00859-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de julio de 2023
Última revisión	25 de julio de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente:

"Tienes puntos acumulados disponibles para canjear que están muy cerca de expirar. Los clientes de Itaú tienen el doble de puntos, entre otras ventajas.
Accede a continuación y c anjea ahora mismo. Al realizar una compra con una tarjeta Itaú o al usar tu token en nuestros canales digitales, ganarás puntos en Livelo."

De abrir el enlace, la persona es dirigida a un sitio falso semejante a los de Banco Itaú, donde se expone al robo de su usuario y contraseña (credenciales).

IoC Correo Electrónico

Antes de evaluar la aplicación de acciones, tenga presente las advertencias de gestión de los IoC. Los IoC de este informe pueden ser obtenidos directamente desde nuestro repositorio. De forma preventiva, sugerimos aplicar las siguientes recomendaciones de ciberseguridad.

URL redirección:

http://ec2-52-67-192-115.sa-east-1.compute.amazonaws[.]com/?hash=bXJvc3NlbGRAaW50ZXJpb3IuZ292LmNs

URL sitio falso:

https://itau.beneficios-puntos-iupp[.]com/portal/

Dirección IP del sitio falso:

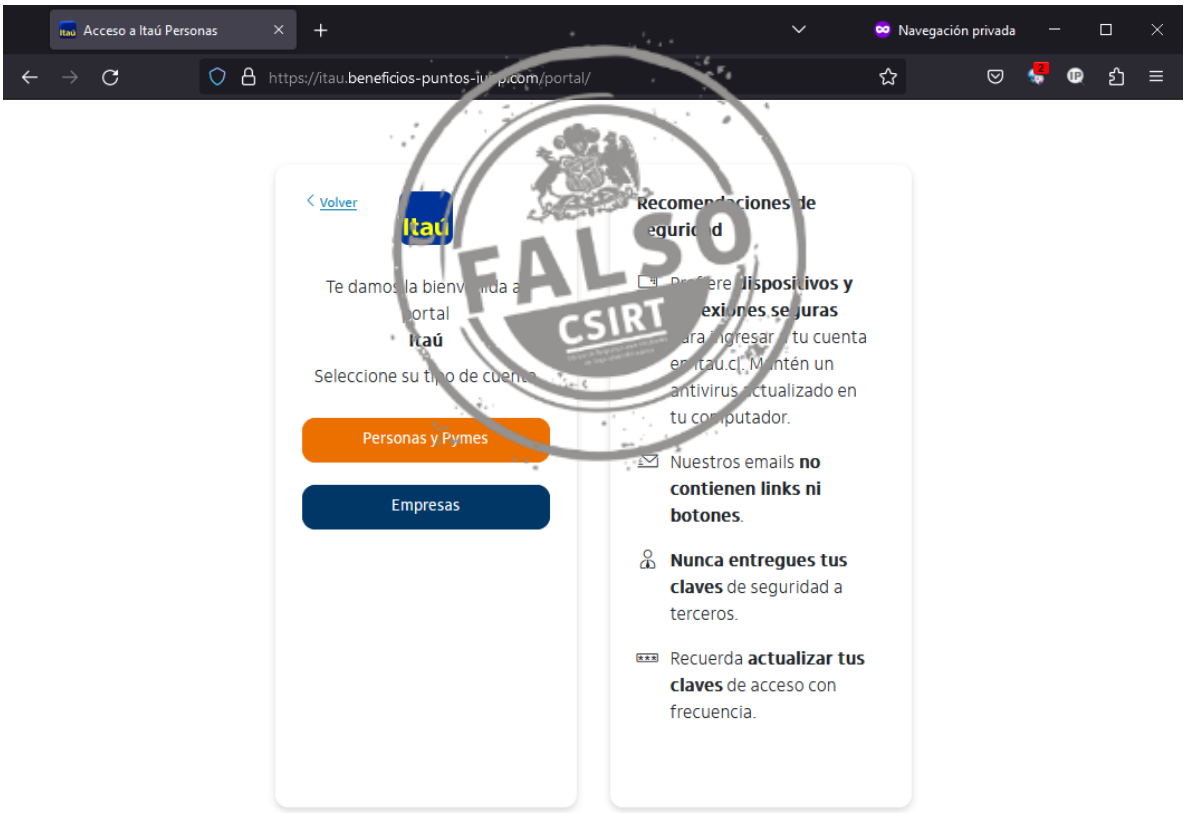
[104.21.13.94]

Datos del remitente:

Asunto	Correo de Salida	SMTP Host
☑ FW_ Itau _ Ultimos dias para canjear tus puntos - (6434)	itau-beneficios@afesuave.com	[139.162.194.142]

Imagen del mensaje

Imagen del sitio



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.25 11:56:00 -04'00'