Alerta de seguridad informática	8FPH23-00861-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de julio de 2023
Última revisión	26 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:

"See attachment."

De abrir el enlace, la persona es dirigida a un sitio falso semejante a un inicio de sesión de correo electrónico, 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:

```
https://bql0epapf-xn--luuaryqv-xn----c1ac4bxc-xn----p1ai.translate.goog/6ruocAit/0PIl7/e8Pyg?YzI5akxXTnphWEowUUdsdWRHVnlhVzl5TG1kdllpNWpiQT09OjBZclE2+&_x_tr_sch=http&_x_tr_sl=CFEFhLRr&_x_tr_tl=txSzTXAb
```

URL sitio falso:

```
https://hty1iiu-web-app.translate[.]goog/host:-web.interior.gob.cl:0264?_x_tr_sl=wsvfGdH&_x_tr_tl=XDXWjXGI&_x_tr_hist=true
```

Dirección IP del sitio falso:

[74.125.201.132]

Datos del remitente:

Asunto	Correo de Salida	SMTP Host
[Do Not Reply]_soc-test@csirt.gob.cl: Automated Request [05/07/2023 00:28:44 AM]	info@haraslaesperanza.com.ar	[190.7.29.21]

Imagen del mensaje

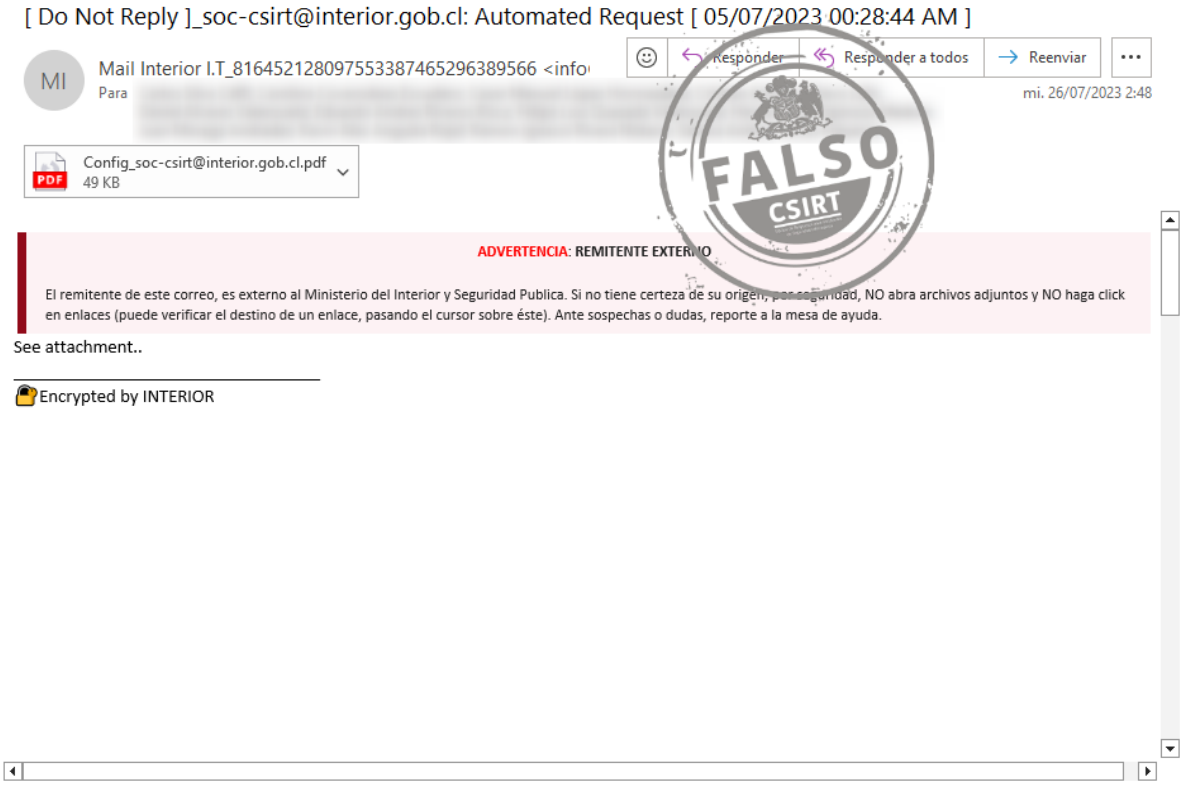
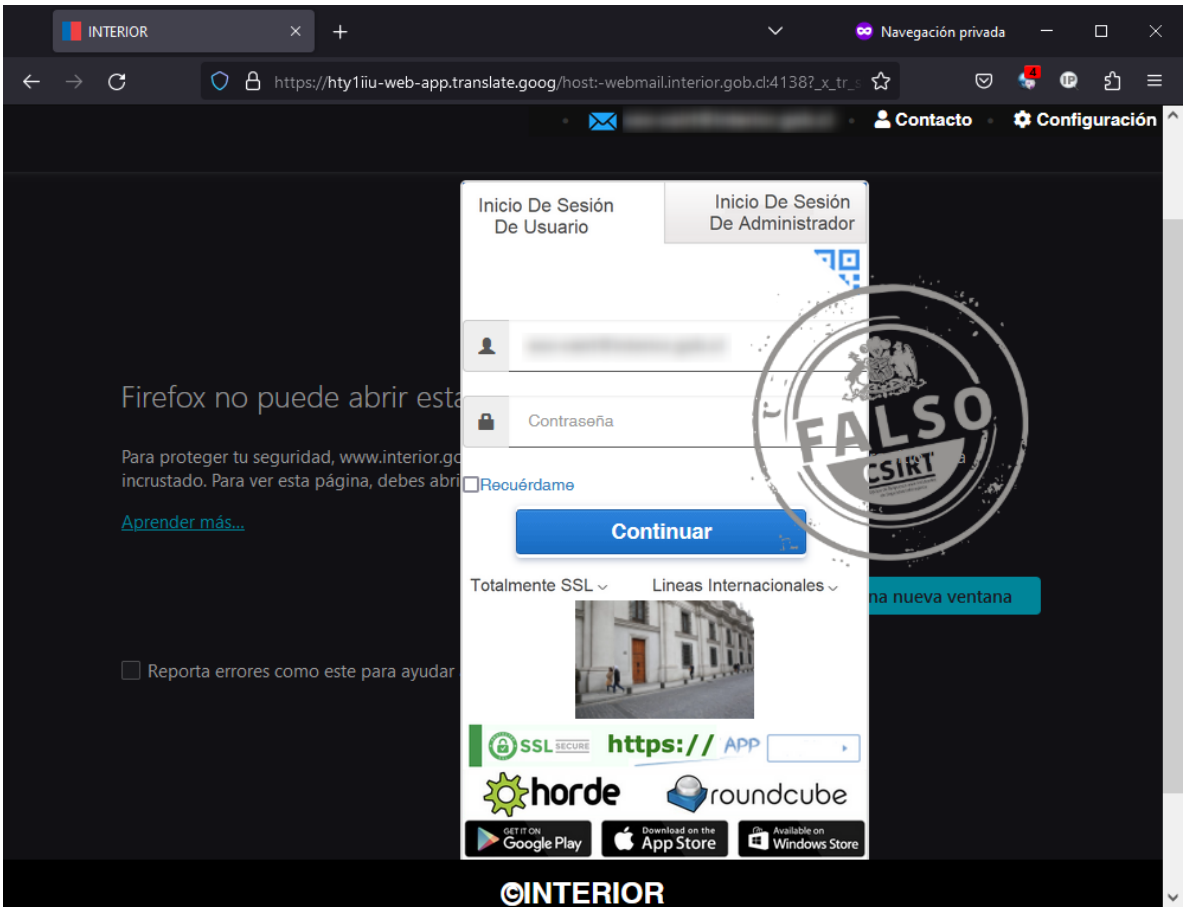


Imagen del sitio



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.26 10:57:01 -04'00'