

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



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.google/6ruocAit/0PII7/e8Pyg?YzI5akxXTnphWEowUUdsdWRHVnlhVzI5TG1kdllpNWp  
iQT09OjBZclE2+&_x_tr_sch=http&_x_tr_sl=CFEFhLRr&_x_tr_tl=txSzTXAb
```

URL sitio falso:

```
https://hty1iiu-web-app.translate[.]google/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]

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

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

[Do Not Reply]_soc-csirt@interior.gob.cl: Automated Request [05/07/2023 00:28:44 AM]

MI Mail Interior I.T_816452128097553387465296389566 <info@haraslaesperanza.com.ar>
Para [Redacted] mi. 26/07/2023 2:48

Responder Responder a todos Reenviar

Config_soc-csirt@interior.gob.cl.pdf 49 KB

FALSO CSIRT

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Pública. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.

See attachment..

Encrypted by INTERIOR

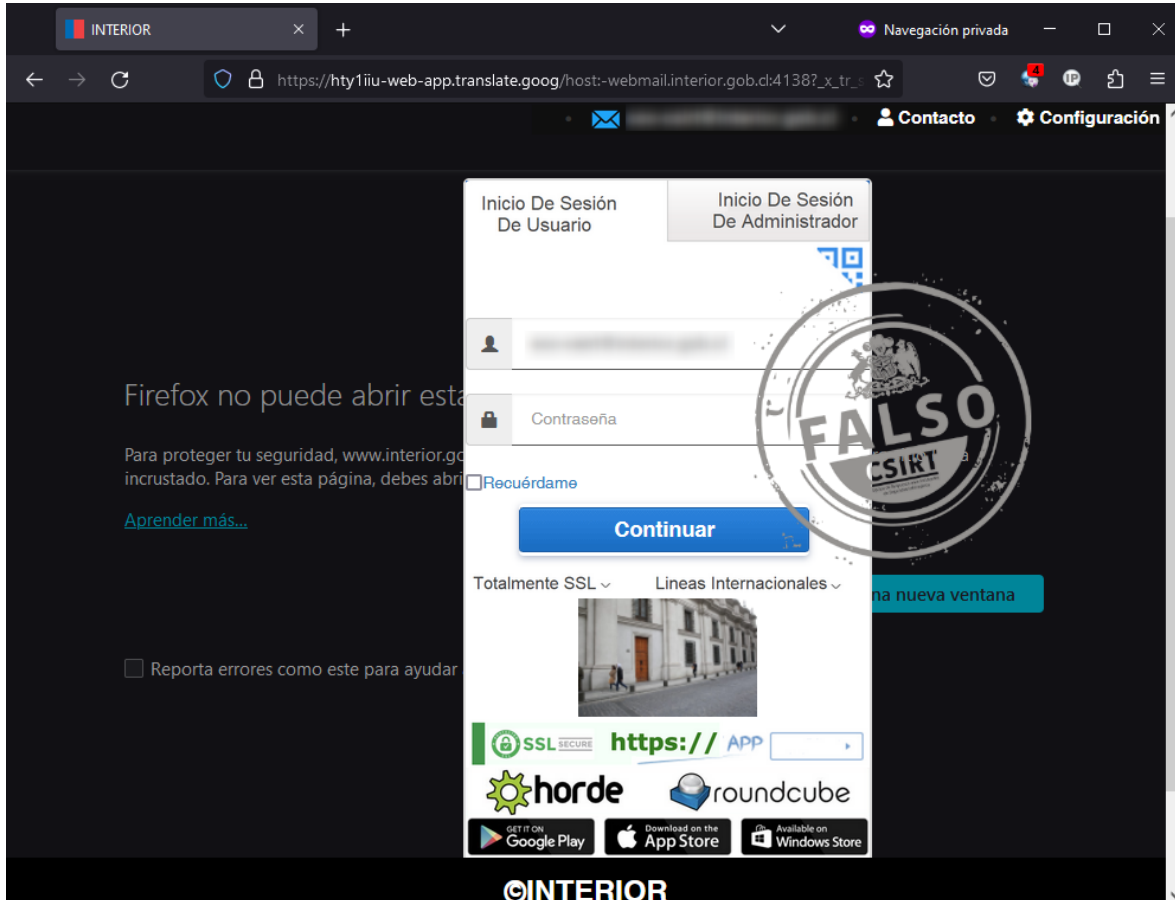
CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Imagen del sitio



CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>