

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 cibernética | 8FPH23-00912-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 01 de diciembre de 2023 |
| Última revisión | 01 de diciembre 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, que en esta ocasión suplanta a la empresa colombiana Confipetrol, que cuenta con operaciones en Chile, y además presenta a sus potenciales víctimas un falso inicio de sesión de Microsoft. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente:

“Buenos días, adjunto la aplicación de pago según lo comentado con la administración, con orientación y actualizaciones. Por razones de seguridad, escanee el código QR para verlo”.

El correo electrónico incluye un enlace a un formulario para capturar credenciales de usuarios.

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@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



Indicadores de compromiso

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**.

| | |
|--|------------|
| URL del sitio falso | |
| https://ms-onlinesupport[.]com/165959/common/oauth2.0/login/84633/ | |
| URL de redirección | |
| N/A | |
| IP del sitio falso | |
| 104.21.11.92 | |
| Asuntos del correo electrónico | |
| Factura | |
| Correos de salida | |
| supervisor.tecnico15.enel@confipetrol.com | |
| IP | Comentario |
| 40.107.220.40 | SMTP |

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

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

Imágenes Relacionadas

[EXTERNO] Factura



Jhon Alexander Bello Garzon <supervisor.tecnico15.enel@confipetrol.com>

Para

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.



CORDIAL SALUDO:

Buenos días, adjunto la aplicación de pago según lo comentado con la administración, con orientación y actualizaciones. Por razones de seguridad, escanee el código QR para verlo. Si tiene alguna pregunta, por favor póngase en contacto conmigo.

Cordialmente



Responder Responder a todos Reenviar

viernes 01-12-2023 9:06

Imagen 1: Correo Electrónico

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

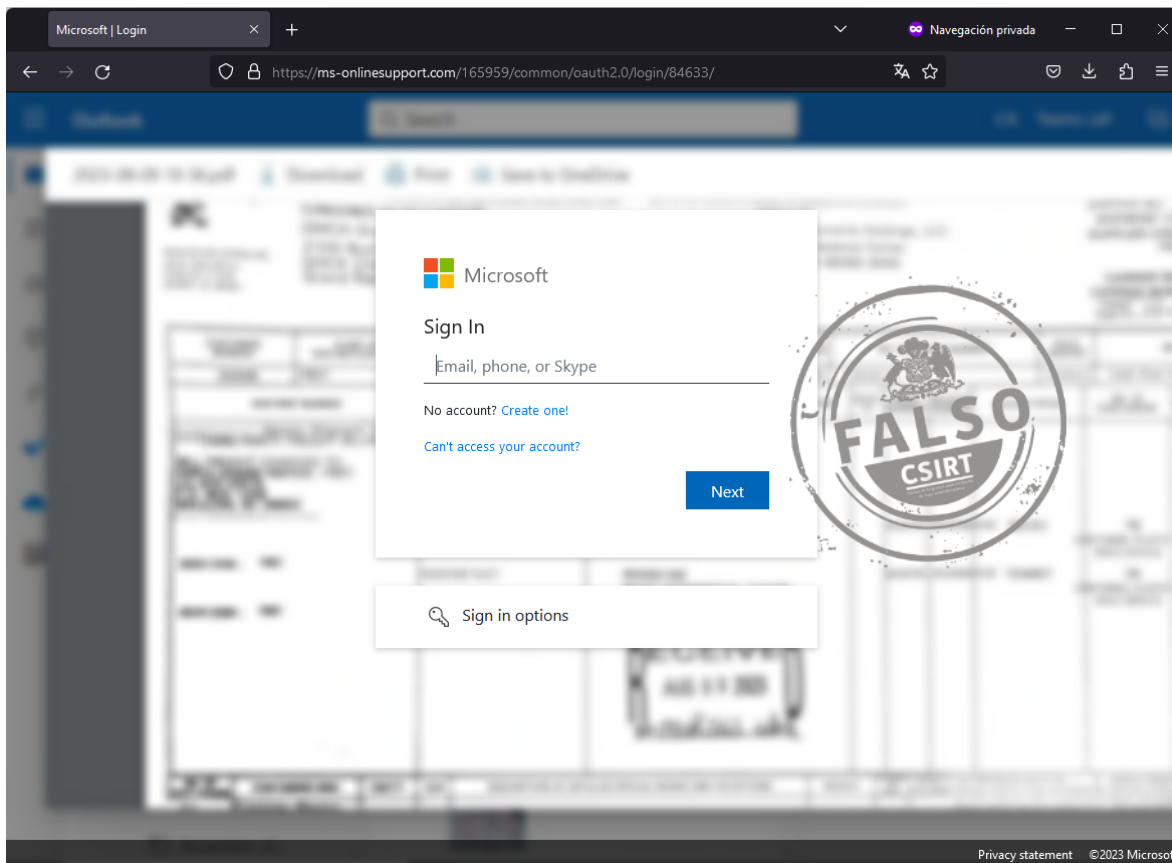


Imagen 2: Sitio fraudulento

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

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