CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 230

semana del 24 al 30 de noviembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

9

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

15

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

9

Las mitigaciones son útiles en productos de Google y ownCloud.

HASHES COMPARTIDOS

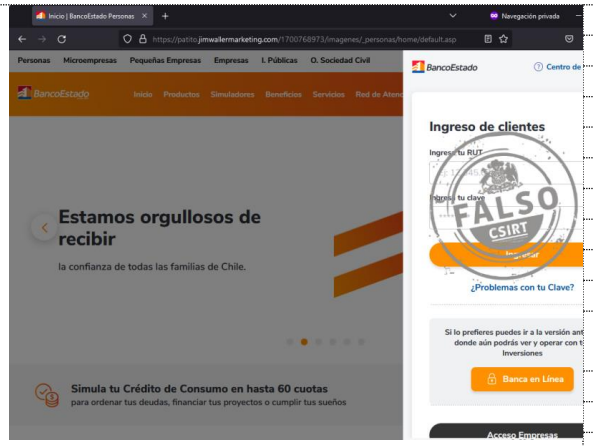
4

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

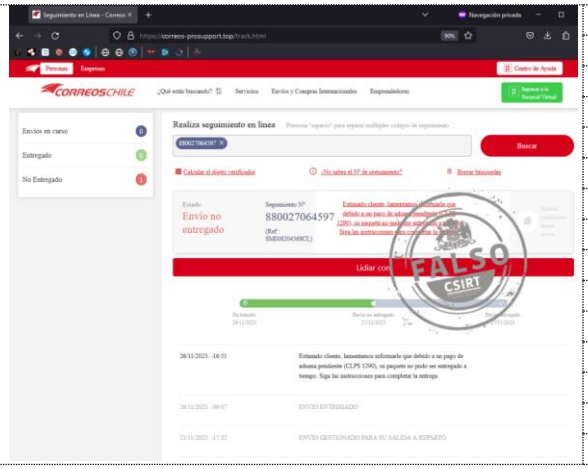
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

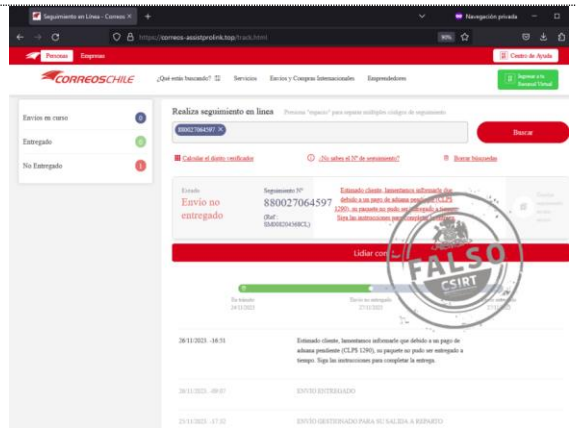


CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00911-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 noviembre, 2023
Última revisión	24 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.jimwallermarketing[.]com/1700768973/imagenes/_personas/home/default.asp	
URL redirección	
https://patitojouxstore[.]com/activacion/cuenta-hhcu/	
Dirección IP sitio falso	
[65.181.111.11]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00911-01/	

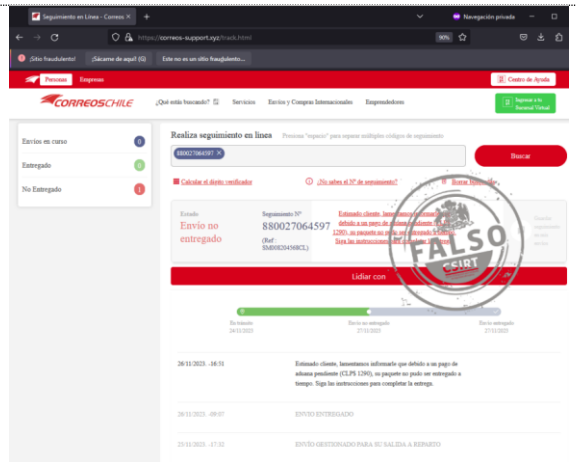
2. Sitios fraudulentos



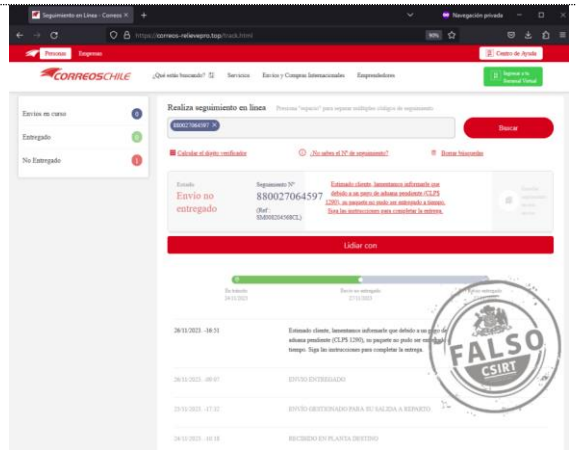
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01582-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-prosupport[.]top/track.html	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01582-01/	



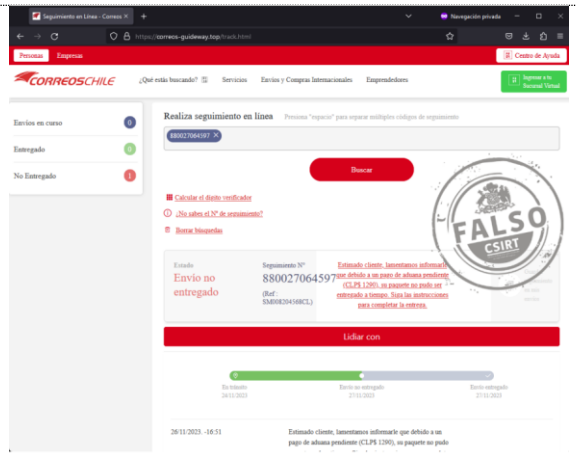
CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01583-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-assistprolink[.]top/track.html	
Dirección IP sitio falso	
[170.106.98.119]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01583-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01584-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-support[.]xyz/track.html	
Dirección IP sitio falso	
[43.130.0.162]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01584-01/	

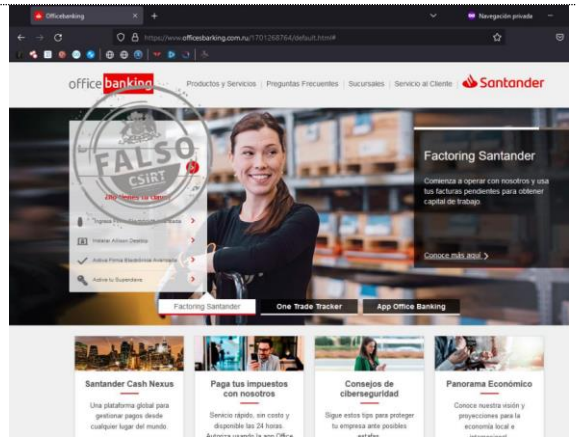


CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01585-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-relievepro[.]top/track.html	
Dirección IP sitio falso	
[43.159.141.163]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01585-01/	

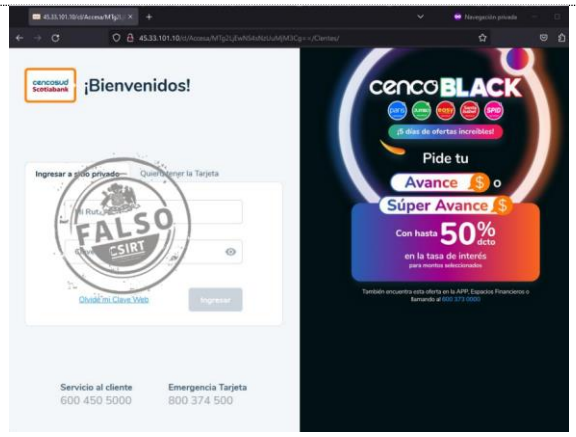


CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01586-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-guideway[.]top/track.html	
Dirección IP sitio falso	
[43.153.56.208]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01586-01/	

CSIRT alerta de un nuevo sitio fraudulento que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01587-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 noviembre, 2023
Última revisión	29 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www-bancofalabella-cl.jenniferkries[.]com/1701268066/home	
Dirección IP sitio falso	
[192.185.198.239]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01587-01/	



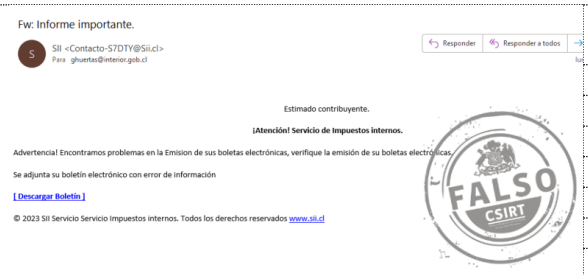
CSIRT alerta de una nueva página fraudulenta que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01588-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 noviembre, 2023
Última revisión	29 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.officesbarking[.]com.ru/1701268764/default.html	
Dirección IP sitio falso	
[104.21.81.98]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01588-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FFR23-01589-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 noviembre, 2023
Última revisión	29 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
http://45.33.101[.]10/cl/Accesa/MTg2LjEwNS4xNzUuMjM3Cg==/Clentes/	
Dirección IP sitio falso	
[45.33.101.10]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01589-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing con malware Mekotio, que suplanta al SII	
Alerta de seguridad cibernética	2CMV23-00436-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 noviembre, 2023
Última revisión	27 noviembre, 2023
Indicadores de compromiso	
URL-Dominio	
https://burgerbarsaintlouis[.]com/octubreSiifactura/?hash={mail} https://nobreakdesign[.]com.br/exenovo/facturaSiinopagada.zip?210217484 support@orientbethlehem[.]net	
SHA256	
87122c413761c8055b76eb3c8e2b1fca3bf64e6b668006705931251d935e0053 c819d4be69eb4f4de0e31cce25bb9c8235b9a700ccaeba554c44ed144959e036	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00436-01/	



CSIRT alerta de nueva campaña de phishing que suplanta al SII, difundiendo el malware Mekotio	
Alerta de seguridad cibernética	2CMV23-00437-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 noviembre, 2023
Última revisión	28 noviembre, 2023
Indicadores de compromiso	
URL-Dominio	
http://lucacocinas.com[.]ar/swf/abs/TGR/VF9IU7TS9S8D3_Boleta_Pendiente_3171_4D2F_8B51_9C5E_002839921.php http://medulashvili[.]ge/Data/Boleta/Sii/H6F3VB881I0/home.php?hash=P0s&CAYdj1=sII	
SHA256	
3250311de041c22eab029c97e95b6d2710f5f026ebaf2ea90e85afca6ae14007 ff06652a3243b538a50715d9a8d44c3b8ca34aff98cc8d1cf6b2fd0a0c139982	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00437-01/	

4. Vulnerabilidades

CSIRT comparte información de vulnerabilidades que afectan a Google Chrome, una de ellas de día cero	
Alerta de seguridad cibernética	9VSA23-00937-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 noviembre, 2023
Última revisión	29 noviembre, 2023
CVE	
CVE-2023-6345 CVE-2023-6351 CVE-2023-6350 CVE-2023-6346 CVE-2023-6347 CVE-2023-6348	
Fabricante	
Google	
Productos afectados	
Chrome, todas sus versiones	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00937-01/	

CSIRT comparte información sobre tres nuevas vulnerabilidades críticas en ownCloud	
Alerta de seguridad cibernética	9VSA23-00938-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 noviembre, 2023
Última revisión	30 noviembre, 2023
CVE	
CVE-2023-49103 CVE-2023-49104 CVE-2023-49105	
Fabricante	
ownCloud	
Productos afectados	
CVE-2023-49104: graphapi, versiones de la 0.2.0 a la 0.3.0. CVE-2023-49104: Core de 10.6.0 a 10.13.0. CVE-2023-49105: Oauth2 anteriores a la versión 0.6.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00938-01/	

5. Noticias y concientización

Ciberconsejos para una navegación segura

Más consejos siempre disponibles en https://csirt.gob.cl/recomendaciones/.

Exitosa convocatoria a conversatorio del CSIRT de Gobierno y encargados de ciberseguridad de organismos públicos

Con más de 80 asistentes, todos ellos encargados de ciberseguridad de organismos del Estado y de empresas públicas, tuvo lugar este lunes el primer conversatorio organizado por el CSIRT de Gobierno para, principalmente, dar a conocer mejor sus funciones y los servicios que ofrecemos a los organismos públicos de todo el país. Junto con ello, el jefe del CSIRT, Cristian Bravo, presentó la visión de este organismo del estado actual de la seguridad digital en Chile y su futuro próximo, especialmente en lo relativo al proyecto de Ley Marco de Ciberseguridad y a la futura creación de la Agencia Nacional de Ciberseguridad.

Además de exponer la visión del CSIRT, un gran objetivo de este encuentro fue conocer las necesidades y responder las preguntas de los encargados de ciberseguridad de los organismos del Estado presentes en la sesión, que tuvo lugar en el Auditorio del Edificio Moneda Bicentenario, sede del CSIRT de Gobierno.

Los datos de la jornada y la presentación de Cristian Bravo en formato PDF:
https://www.csirt.gob.cl/noticias/conversatorio-csirt-encargados-estado-2023/

6. Recomendaciones y buenas prácticas

- 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 que los sitios web a los que se ingrese sean los oficiales.

7. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Gonzalo Andrés Araya Navarrete Phishing
- Francisco Jiménez Alcántara Phishing
- Alan Lagos Phishing
- Fernando Miguel Rojas Duran Directorio Expuesto
- Diego Bardalez Plaza SQL Injection

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.12.01 17:09:55 -03'00'