CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 179

SEMANA DEL 2 AL 8 DE DICIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

2

Las mitigaciones son útiles en productos de Google y Cacti.

IP INFORMADAS

6

Listado de IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

16

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

6

Asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

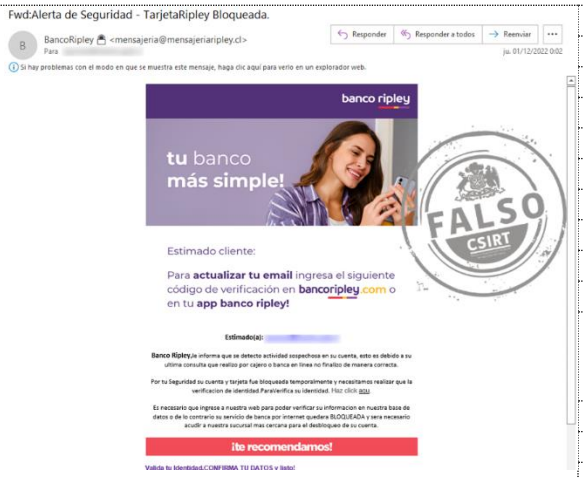
1. Malware

CSIRT alerta de phishing con malware, que suplanta al Portal de Trámites del MTT	
Alerta de seguridad cibernética	2CMV22-00391-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2022
Última revisión	7 de diciembre de 2022
Indicadores de compromiso	
Asunto	
✓ Registro de multas de transito no pagadas	
Correo de salida	
contactorutempresa3.chilesenderinfinformativo[.]online	
SHA256	
9b208a0753be00035aa2ef526a9dbfb031e421ea0f9892b7421ab9d155e713eb 120a57fa1b8c78683d3e04f309a8dd2f84c9f44c66dcb6d6496b30246db22bfb c63063b68362b78469fdf7111af89b74ec541462cd6982aa3342717600ff02ed de87c8713fac002b0b0a0f9b02c4e3ebcccf65282a22f5ab5912a9da00f35c2a 1185c5fc183e63594181f5d7b5f85e793f25b3035531d8cde1fd6bee54ba3564 c09d0790e550694350b94ca6b077c54f983c135fab8990df5a75462804150912	
URL	
http://junho2022.serveftp[.]org/mail/wp/configuracao/config.txt	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00391-01/	
https://www.csirt.gob.cl/media/2022/12/2CMV22-00391-01.pdf	

2. Sitios fraudulentos

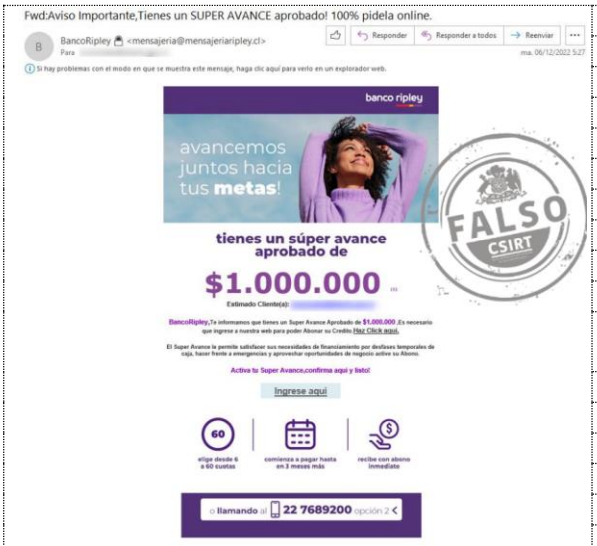
CSIRT alerta de página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01152-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2022
Última revisión	7 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://www.santanderchile-personas.pundirfarms[.]com/1670444369/portada/personas/home.asp	
Dirección IP	
[43.225.55.146]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01152-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01152-01.pdf	

2. Phishing

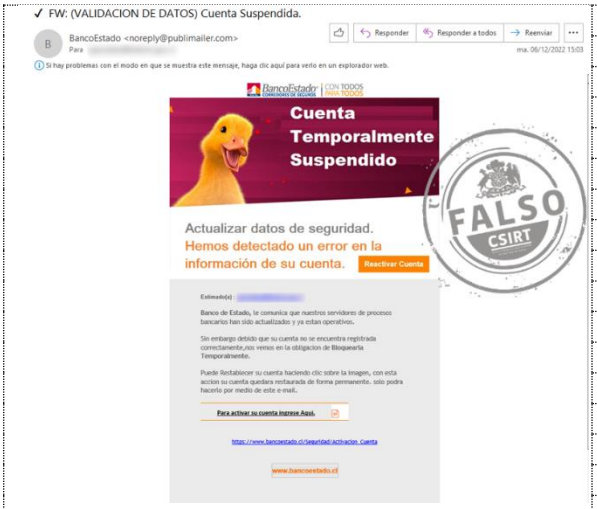


CSIRT alerta de campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00669-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de diciembre de 2022
Última revisión	2 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3VFe425?l=www.bancoripley.cl https://wordpress-413449-1536776.cloudwaysapps[.]com/bancoripley/cuenta-zsif/	
URL sitio falso	
https://web.bancoripley.cl.buckrealty[.]net/1669899391/login	
Dirección IP	
[64.91.247.208]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00669-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00669-01.pdf	

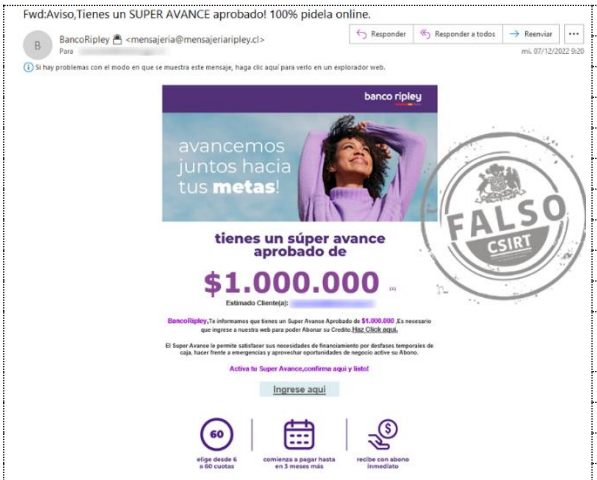
CSIRT alerta ante campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00670-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de diciembre de 2022
Última revisión	2 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
http://cnct.us/5bNKJ2 https://portal-bancochile.cl.townrealstate[.]com/	
URL sitio falso	
https://portal-bancochile.cl.townrealstate[.]com/1669917041/bchile-web/persona/login/index.html/login	
Dirección IP	
[185.146.22.242]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00670-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00670-01.pdf	



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00671-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2022
Última revisión	6 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3UPthNv?l=www.bancoripley.cl http://swiatjezyka[.]pl/bancoripley/cuenta-agss/	
URL sitio falso	
https://web.bancoripley-cl.bigfishservices.com[.]au/1670330557/login	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00671-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00671-01.pdf	



CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00672-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2022
Última revisión	6 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://nhmwcotitostado[.]info/activacion/cuenta-zlsn/	
URL sitio falso	
https://smscotito[.]info/1670350927/imagenes/_personas/home/default.asp	
Dirección IP	
[213.136.93.164]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00672-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00672-01.pdf	



CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00673-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2022
Última revisión	7 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3BaZlEr?l=www.bancoripley.cl https://ethosmoveisplanejados.com[.]br/bancoripley/cuenta-frwc/	
URL sitio falso	
https://web-bancoripley.cl.bigfishservices.com[.]au/1670418013/login	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00673-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00673-01.pdf	

3. Vulnerabilidades

CSIRT comparte información de parche para nueva vulnerabilidad en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00750-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2022
Última revisión	6 de diciembre de 2022
CVE	
CVE-2022-4262	
Fabricantes	
Google	
Productos afectados	
Chrome anteriores a 108.0.5359.94.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00750-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00750-01.pdf	

CSIRT comparte nueva vulnerabilidad en Cacti	
Alerta de seguridad cibernética	9VSA22-00751-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2022
Última revisión	6 de diciembre de 2022
CVE	
CVE-2022-46169	
Fabricantes	
Cacti	
Productos afectados	
Cacti versión 1.2.22.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00751-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00751-01.pdf	

4. Actualidad

CSIRT de Gobierno y 8.8 realizaron segunda versión de 8.8 Gobierno, evento de ciberseguridad para funcionarios del Estado

Ingrid Inda, Directora del CSIRT de Gobierno, Red de Conectividad del Estado (RCE) y Jefa de la División de Redes y Seguridad Informática de la Subsecretaría del Interior

Con una importante asistencia, este 5 de diciembre se realizó la segunda versión de la conferencia 8.8 Gobierno, donde se expusieron los avances, las recomendaciones y los próximos desafíos en materia de ciberseguridad y ciberinteligencia, desde el punto de vista de los organismos públicos.

La actividad se efectuó en la antigua sede del Congreso Nacional y estuvo organizada por el CSIRT de Gobierno del Ministerio del Interior y la 8.8 Computer Security Conference. Lea la nota completa aquí: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-y-8-8-realizaron-segunda-version-de-8-8-gobierno-evento-de-ciberseguridad-para-funcionarios-del-estado/.

La apertura estuvo a cargo del **Coordinador Nacional de Ciberseguridad, Daniel Álvarez**, quien catalogó la ciberseguridad como un tema prioritario para el Gobierno actual, ya que, como destacó "cuando hablamos de ciberseguridad no estamos protegiendo computadores, sino que personas". Asimismo, recaló la importancia de este tipo de encuentros: "creo que unir en un mismo espacio a la comunidad técnica encargada de la ciberseguridad de las organizaciones públicas, con la comunidad que hace investigación teórica y práctica, es esencial".

Posteriormente, **Gabriel Bergel, famoso hacker white hat, cofundador y CEO de 8.8, así como partner asociado de Seguridad y Resiliencia en Kyndryl**, hizo un recorrido por todas las conferencias 8.8 que desde 2011 viene realizando. "Esta conferencia nació con el único objetivo de compartir información, democratizar el conocimiento y crear comunidad en torno a la ciberseguridad", afirmó.

Por su parte, **Ingrid Inda, Directora del CSIRT de Gobierno, Red de Conectividad del Estado (RCE) y Jefa de la División de Redes y Seguridad Informática de la Subsecretaría del Interior**, realizó la exposición "Radiografía Nacional: Realidad de la Ciberseguridad en el Estado: Avances y Desafíos", mostrando la situación actual de la seguridad cibernética del Estado.

Carlos Silva, encargado del CSIRT de Gobierno.

En este contexto, Inda puntualizó: "Cada 4 años, la OEA levanta un informe de madurez de sus 32 países; tenemos el de 2016 y el de 2020, por lo que ahora hay que trabajar para el de 2024. El Estado hizo un levantamiento con la subsecretaría en relación a nuestro nivel de madurez, por lo que hay ciertas recomendaciones respecto de los aspectos más débiles en los sistemas de gestión de seguridad de la información, y no todos lo han tomado con seriedad".

La presentación continuó con **Carlos Silva, encargado del CSIRT de Gobierno**, quien mostró estadísticas del tráfico de la RCE, destacando que se bloquearon 178.998 correos maliciosos dirigidos a los funcionarios del estado, de enero a noviembre, período en que hubo más de 8 millones de intentos de explotar alguna vulnerabilidad en los activos de la RCE. "Para enfrentar la gran cantidad de amenazas que vemos a diario se requiere del trabajo en equipo, contar con grupos cohesionados y afiatados, para así lograr el éxito de la protección de los sistemas y de las personas".

5. Concientización

Ciberdiccionario Volumen 24

Volvemos con un nuevo número de nuestro Ciberdiccionario para comenzar diciembre de 2022 con cuatro nuevos conceptos: password spray, hacktivismo, patrimonio digital y superficie de ataque.

Pueden encontrar la campaña completa también en nuestro sitio web oficial, siempre con nuevos consejos: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-24/.

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.

- Christian Abarca
- Claudio Toledo Contreras
- Roberto Zúñiga
- Bernardita Mujica Dittborn
- Elisa Helena Vargas Mejías
- Alejandro Ignacio Carreño Baeza
- José Mauricio Rojas Palma