



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 253

semana del 3 al 9 de mayo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

2

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

3

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

25

Las mitigaciones son útiles en productos de F5 y Android.



HASH REPORTADOS

3

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



CONTENIDO

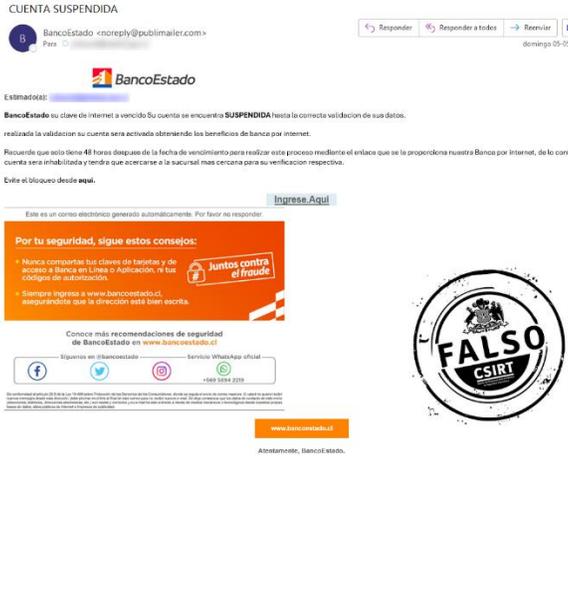
1. Malware.....	3
2. Phishing	4
3. Vulnerabilidades.....	5
4. Noticias y concientización.....	7
5. Recomendaciones y buenas prácticas	9
6. Muro de la Fama	10

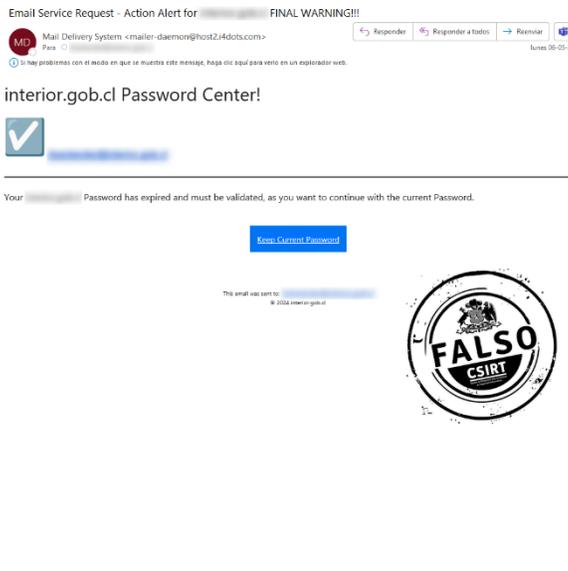
1. Malware

<p>Entrega urgente por DHL</p> <p>Mensaje <mensaje@lovablehn.com> Para DHL_734825514200.rar 624 KB</p>  <p>Atención al cliente.</p> <p>Se adjuntan los documentos de envío especificados para la entrega, confirme que la dirección sea correcta.</p> <p>Copia original del conocimiento de embarque y demás documentos relacionados con el despacho del envío a su puerto.</p> <p>Notificación de evento de autorización de grupo de evento de envío el 2 de mayo de 2024.</p> <p>Número AWB: 4677348255142 Fecha de recepción: 2/05/2024 Fecha prevista de entrega: 05/02/2024 Servicio Platas: 1 REF cliente: 7348255142 Descripción: xxxxxxxxxxxx Envío por: DHL Express</p> <p>Por favor no responda a este correo electrónico. Esta es una aplicación automatizada. Sólo se utiliza para enviar notificaciones proactivas.</p> <p>Departamento de Cuentas por Cobrar</p>	<p>DHL - Suplantación con malware</p> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00461</td></tr><tr><td>Clase de alerta</td><td>Fraude</td></tr><tr><td>Tipo de incidente</td><td>Malware</td></tr><tr><td>Nivel de riesgo</td><td>Alto</td></tr><tr><td>TLP</td><td>Blanco</td></tr><tr><td>Fecha de lanzamiento original</td><td>3 de mayo de 2024</td></tr><tr><td>Última revisión</td><td>3 de mayo de 2024</td></tr></table> <p>Indicadores de compromiso</p> <p>Asunto Entrega urgente por DHL</p> <p>Correo de salida mensaje@lovablehn.com</p> <p>SHA256 37ac69abe12f3ec977df53efd9e10a1c2f40eba5fab217cbce4e0fb5452c669f96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7d9b1d72dec9430f7bddc386ee8a621a9138f59cb921ee725fc592725d29785ac</p> <p>Enlace para revisar loC: https://csirt.gob.cl/alertas/cmV24-00461/</p>	Código de alerta	CMV24-00461	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	3 de mayo de 2024	Última revisión	3 de mayo de 2024
Código de alerta	CMV24-00461														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	3 de mayo de 2024														
Última revisión	3 de mayo de 2024														

CONTACTO Y REDES SOCIALES CSIRT

2. Phishing

 <p>CUENTA SUSPENDIDA</p> <p>BancoEstado <noreply@publimailer.com> Para: [Redacted] domingo 05:00</p> <p>BancoEstado</p> <p>Estimado(a): [Redacted]</p> <p>BancoEstado su clave de internet a vencido. Su cuenta se encuentra SUSPENDIDA hasta la correcta validación de sus datos. realice la validación su cuenta sera activada obteniendo los beneficios de banca por internet.</p> <p>Recuerde que solo tiene 48 horas después de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona nuestra Banca por internet, de lo contrario su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificación respectiva.</p> <p>Evite el bloqueo desde aquí.</p> <p>Ingrese Aquí</p> <p>Por tu seguridad, sigue estos consejos:</p> <ul style="list-style-type: none"> Nunca compartas tus claves de tarjetas y de acceso a Banca en Línea o Aplicación, ni tus códigos de autorización. Siempre ingresa a www.bancoestado.cl, asegurándote que la dirección está bien escrita. <p>Conoce más recomendaciones de seguridad de BancoEstado en www.bancoestado.cl</p> <p>Síguenos en Facebook, Twitter, Instagram, Servicio WhatsApp oficial +569 3054 2219</p> <p>www.bancoestado.cl</p> <p>Atentamente, BancoEstado.</p>	<p>BancoEstado - Phishing</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>FPH24-00957</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>6 de mayo de 2024</td> </tr> <tr> <td>Última revisión</td> <td>6 de mayo de 2024</td> </tr> </table> <p>Indicadores de compromiso</p> <p>Asunto email CUENTA SUSPENDIDA</p> <p>URL del sitio falso https://patito.larissakovalchuk.com/1715002357/imagenes/_personas/home/default.asp</p> <p>URL sitio redirección https://temucoproduce.com/activacion/cuenta-nldo/</p> <p>Dirección IP sitio falso [122.201.66.57]</p> <p>Enlace para revisar loC: https://csirt.gob.cl/alertas/fph24-00957/</p>	Alerta de seguridad cibernética	FPH24-00957	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	6 de mayo de 2024	Última revisión	6 de mayo de 2024
Alerta de seguridad cibernética	FPH24-00957														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	6 de mayo de 2024														
Última revisión	6 de mayo de 2024														

 <p>Email Service Request - Action Alert for interior.gob.cl FINAL WARNING!!!</p> <p>Mail Delivery System <mailer-daemon@host24dots.com> Para: [Redacted] lunes 06:00</p> <p>interior.gob.cl Password Center!</p> <p>Your Password has expired and must be validated, as you want to continue with the current Password.</p> <p>Reset Current Password!</p> <p>This email was sent to [Redacted] @ 2024 interior.gob.cl</p>	<p>BancoEstado - Phishing</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>FPH24-00958</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>6 de mayo de 2024</td> </tr> <tr> <td>Última revisión</td> <td>6 de mayo de 2024</td> </tr> </table> <p>Indicadores de compromiso</p> <p>Asunto email Email Service Request - Action Alert for interior.gob.cl FINALWARNING!!!</p> <p>URL del sitio falso https://cloudflare-ipfs.com/ipfs/bafybeidihzirgflcmm3hlceu4wshnbxk5m7cjrraps73rzwwam2rtphom/login-update%20%281%29.html#{Correoelectronico}</p> <p>Dirección IP sitio falso [104.17.96.13]</p> <p>Enlace para revisar loC: https://csirt.gob.cl/alertas/fph24-00958/</p>	Alerta de seguridad cibernética	FPH24-00958	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	6 de mayo de 2024	Última revisión	6 de mayo de 2024
Alerta de seguridad cibernética	FPH24-00958														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	6 de mayo de 2024														
Última revisión	6 de mayo de 2024														

3. Vulnerabilidades



VSA24-01012
Alerta de Vulnerabilidades
F5 BIG-IP Next Central Manager

CSIRT



Detalles e informe en <https://csirt.gob.cl/alertas>

F5 BIG-IP Next Central Manager - Vulnerabilidades		
Código de alerta	VSA24-01012	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	9 de mayo de 2024	
Última revisión	9 de mayo de 2024	
CVE, puntaje CVSS y EPSS al momento de la publicación		
CVE-2024-21793	7.5	0.04%
CVE-2024-26026	7.5	0.04%
Fabricante		
F5		
Productos afectados		
F5 BIG-IP Next Central Manager		
Desde 20.0.1 y anteriores a 20.2.0		
Enlaces para revisar el informe:		
https://csirt.gob.cl/alertas/vsa24-01012/		



VSA24-01013
Alerta de Vulnerabilidades
Android

CSIRT



android

Detalles e informe en <https://csirt.gob.cl/alertas>

ArubaOS - Vulnerabilidades		
Código de alerta	VSA24-01013	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	9 de mayo de 2024	
Última revisión	9 de mayo de 2024	
CVE y EPSS al momento de la publicación		
CVE-2024-23706	0.04%	
CVE-2024-0024		
CVE-2024-0025		
CVE-2024-23705		
CVE-2024-23708		
CVE-2024-0043		
CVE-2024-23707		
CVE-2024-23709		
CVE-2023-4622		
CVE-2023-6363		
CVE-2024-1067		
CVE-2024-1395		
CVE-2023-32871		
CVE-2023-32873		
CVE-2024-20056		
CVE-2024-20057		
CVE-2024-21471		
CVE-2024-21475		
CVE-2024-23351		
CVE-2024-23354		
CVE-2023-33119		
CVE-2023-43529		

CONTACTO Y REDES SOCIALES CSIRT

Boletín de Ciberseguridad N° 253

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



BOLETÍN 13BCS24-00262-01 | Semana del 3 al 9 de mayo de 2024

CVE-2023-43530

CVE-2023-43531

CVE-2024-21477

Fabricante

Android

Productos afectados

Android 14

Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/vsa24-01013>

CONTACTO Y REDES SOCIALES CSIRT

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

“Comienza un nuevo ciclo, que estará marcado por el desafío de desarrollar las capacidades nacionales para incrementar el nivel de madurez en ciberseguridad”

El martes 24 de abril, la Comisión de Economía y Productividad Digital de la CNC organizó un encuentro para hablar sobre la Ley Marco de Ciberseguridad, actividad que contó con la participación de Daniel Álvarez, Coordinador Nacional de Ciberseguridad.

Álvarez comenzó su presentación destacando que: “El lunes 8 de abril se publicó en el Diario Oficial de Chile, la Ley N°21.663, marco regulatorio de ciberseguridad en el país. Con esto comienza un nuevo ciclo para la ciberseguridad en Chile y, probablemente, para América Latina. Su objetivo es establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos y los particulares. Asimismo, fija los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad, además de establecer las atribuciones y obligaciones de los organismos del Estado y los particulares”.

Además, agregó: “La ley es resultado de la implementación de la planificación primaria desarrollada en la primera Política Nacional de Ciberseguridad 2018-2022, cuya primera medida era la aprobación de una ley general sobre ciberseguridad. Con la publicación de la Ley N°21.663 se cumple esa medida que era parte del objetivo estratégico de contar con una infraestructura resistente. En concreto, la nueva Ley Marco de Ciberseguridad crea la Agencia Nacional de Ciberseguridad (ANCI). Este organismo será el rector de la ciberseguridad, permitirá fijar normativa técnica, dictará protocolos y estándares para prevenir, reportar y resolver incidentes de ciberseguridad o ciberataques”.

La nota completa: <https://ciberseguridad.gob.cl/noticias/comienza-un-nuevo-ciclo-que-estara-marcado-por-el-desafio-de-desarrollar-las-capacidades-nacionales-para-incrementar-el-nivel-de-madurez-en-ciberseguridad/>



CONTACTO Y REDES SOCIALES CSIRT

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

5. 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.

CONTACTO Y REDES SOCIALES CSIRT

6. 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.

- Williams Ignacio Diaz Santander
- Jaime Uribe
- Miguel Becerra
- Ramon Eduardo Moraga Diaz
- Orlando Navarrete
- Víctor Henriquez

CONTACTO Y REDES SOCIALES CSIRT