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

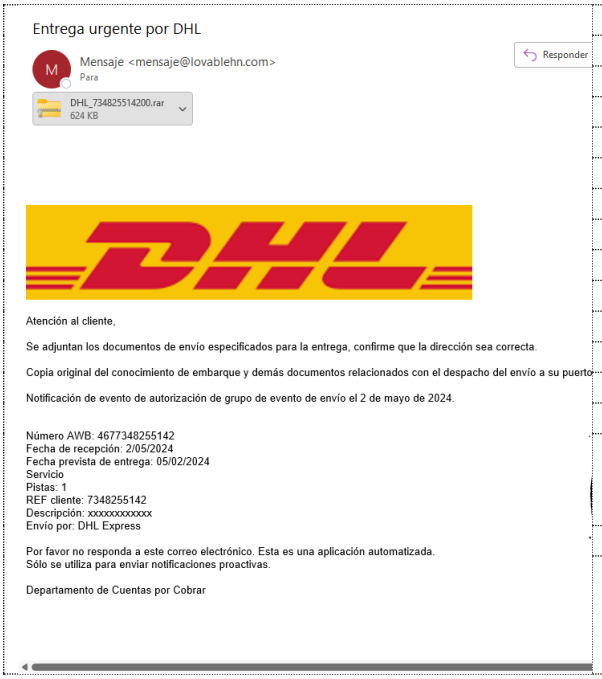
3

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

CONTENIDO

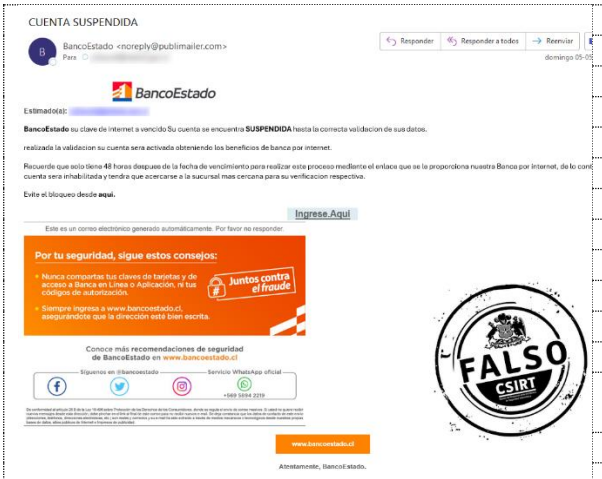
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Malware

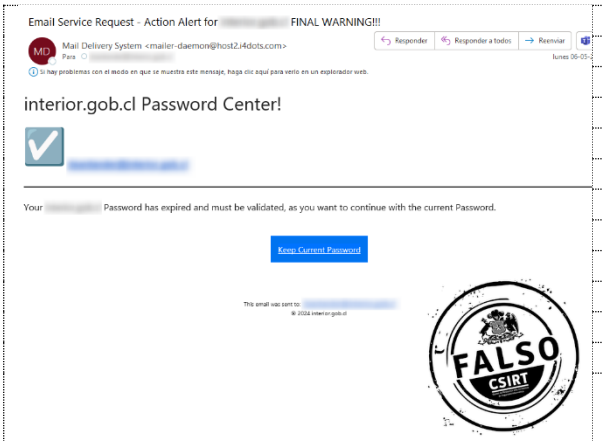


DHL - Suplantación con malware	
Código de alerta	CMV24-00461
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de mayo de 2024
Última revisión	3 de mayo de 2024
Indicadores de compromiso	
Asunto	
Entrega urgente por DHL	
Correo de salida	
mensaje@lovablehn.com	
SHA256	
37ac69abe12f3ec977df53efd9e10a1c2f40eba5fab217cbce4e0fb5452c669f 96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7 d9b1d72dec9430f7bddc386ee8a621a9138f59cb921ee725fc592725d29785ac	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00461/	

2. Phishing



BancoEstado - Phishing	
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
Indicadores de compromiso	
Asunto email	
CUENTA SUSPENDIDA	
URL del sitio falso	
https://patito.larissakovalchuk.com/1715002357/imagenes/_personas/home/default.asp	
URL sitio redirección	
https://temucoproduce.com/activacion/cuenta-nldo/	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00957/	



BancoEstado - Phishing	
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
Indicadores de compromiso	
Asunto email	
Email Service Request - Action Alert for interior.gob.cl FINALWARNING!!!	
URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/bafybeidihzirgfqlcmm3hlceu4wshnbxk5m7cjrraps73rzwwam2rtphom/login-update%20%281%29.html#{Correoelectronico}	
Dirección IP sitio falso	
[104.17.96.13]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00958/	

3. Vulnerabilidades

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/	

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	

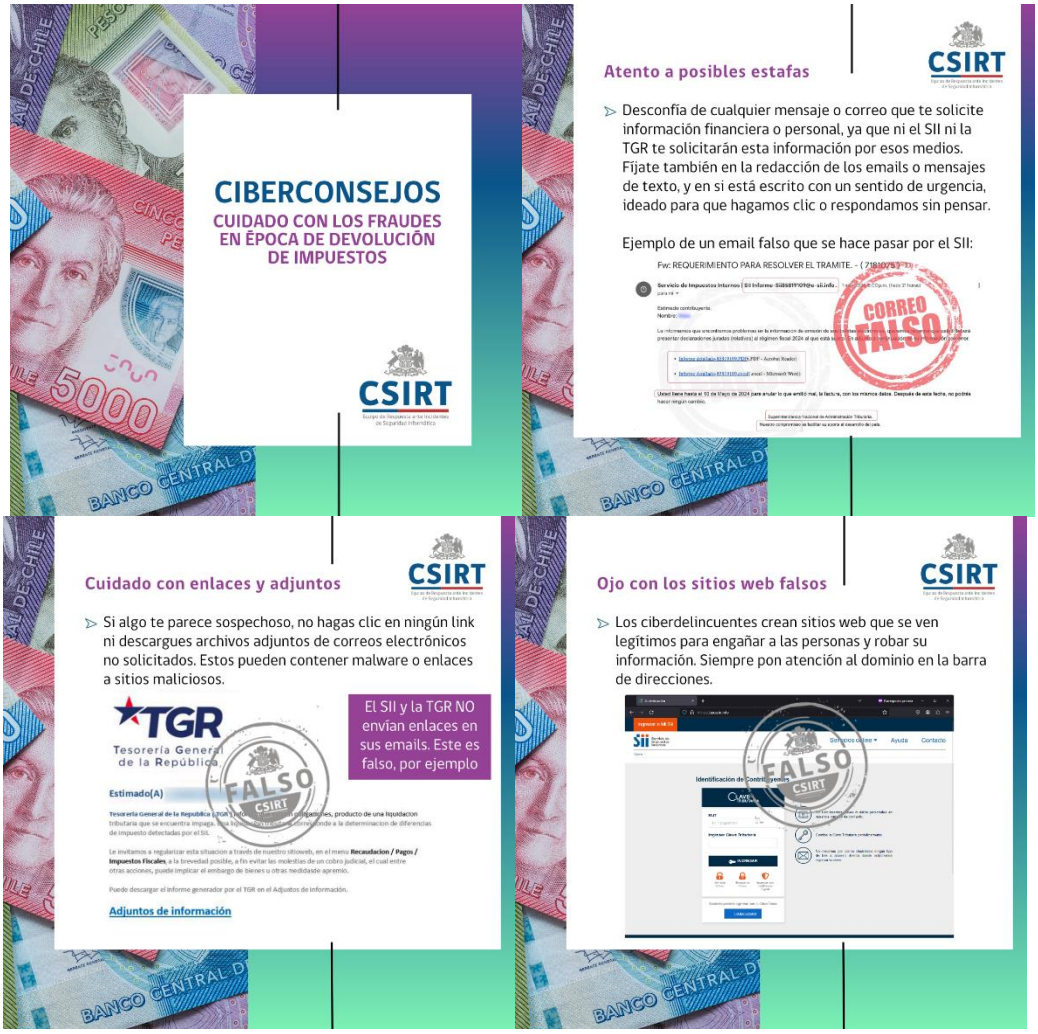
	CVE-2023-43530 CVE-2023-43531 CVE-2024-21477
	Fabricante
	Android
	Productos afectados
	Android 14
	Enlaces para revisar el informe:
	https://csirt.gob.cl/alertas/vsa24-01013

4. Noticias y concientización

Ciberconsejos | Devolución de impuestos

Siempre debemos estar atentos a posibles estafas en internet, y los momentos de alto nivel de transacciones, como es la Operación Renta y su devolución de impuestos, son períodos del año en que debemos extremar la cautela. Por eso elaboramos las siguientes recomendaciones para que estemos todos al tanto de algunas formas en que pueden tratar de robarnos nuestro dinero y datos personales. ¡Revísalos y compártelos!

La campaña completa, para descargar y compartir con sus trabajadores, amigos y familiares, aquí: https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-devolucion-de-impuestos2024/.



"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/

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.

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.05.10 16:01:44 -04'00'