CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 250

semana del 12 al 18 de abril de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

7

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

2

Las mitigaciones son útiles en productos de Palo Alto y PuTTY.

HASH REPORTADOS

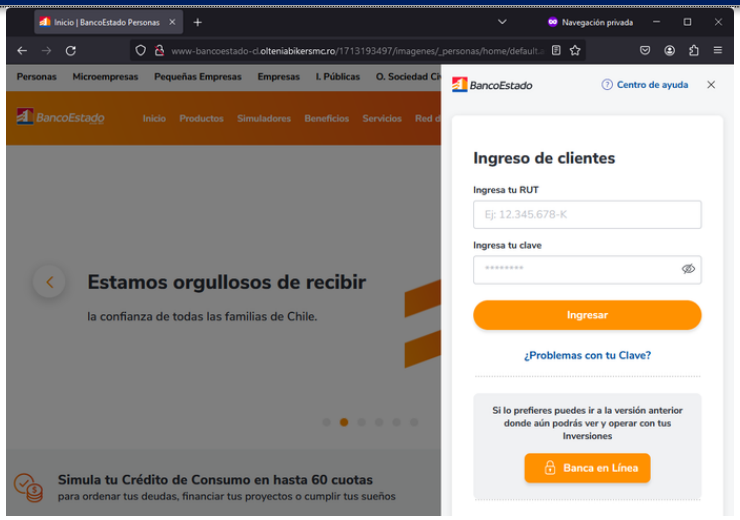
4

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

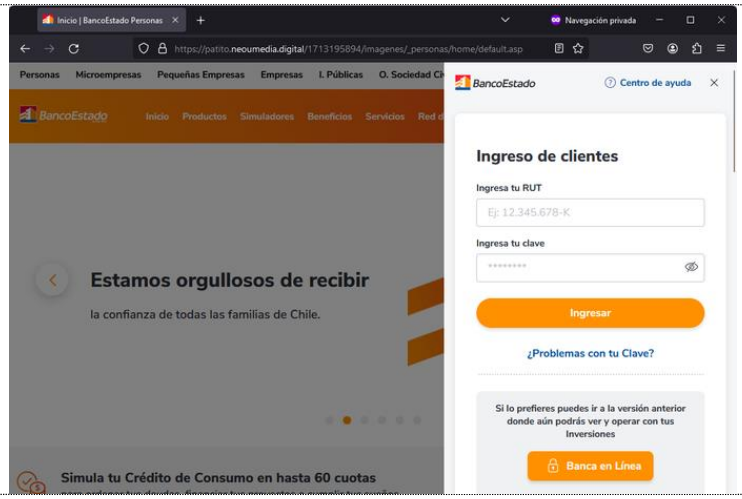
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

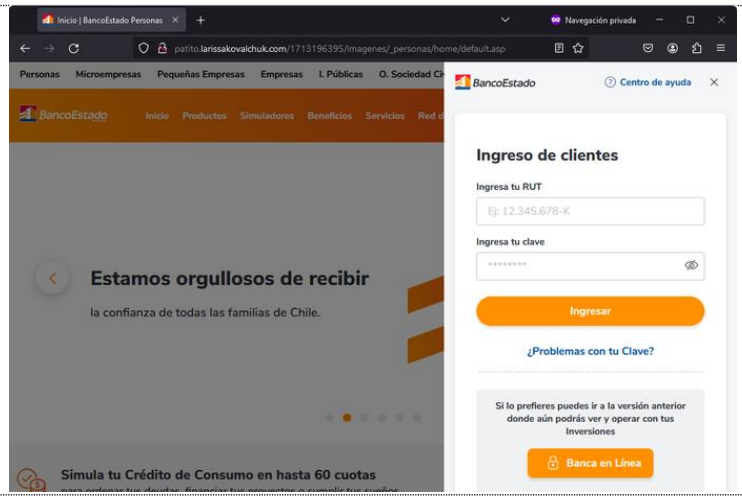
1. Sitios fraudulentos



BancoEstado - Falsificación	
Código de alerta	FFR24-01677
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
http://www-bancoestado-cl.olteniabikersmc.ro/1713193497/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[37.156.180.190]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01677/	

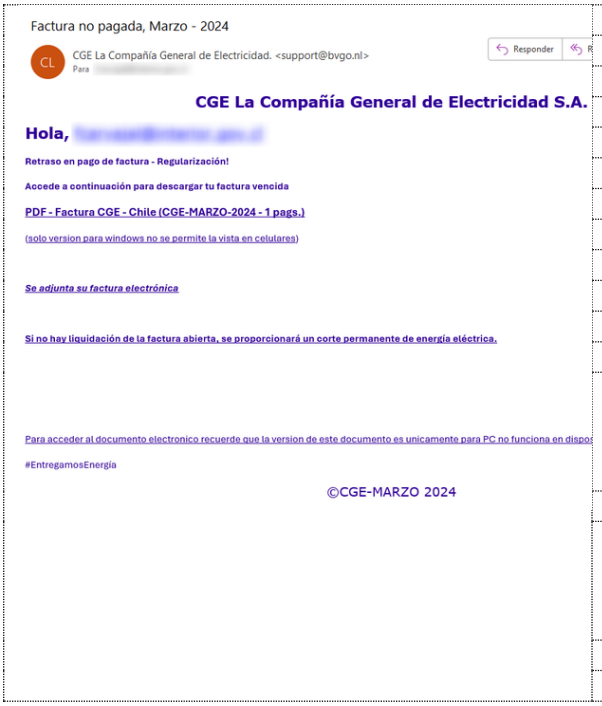


BancoEstado - Falsificación	
Código de alerta	FFR24-01678
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.neoumedia.digital/1713195894/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[203.161.53.92]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01678/	



BancoEstado - Falsificación	
Código de alerta	FFR24-01679
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
http://patito.larissakovalchuk.com/1713196395/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01679/	

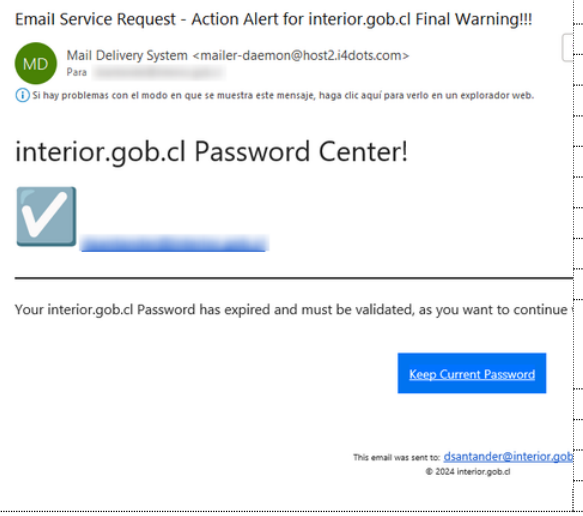
2. Malware



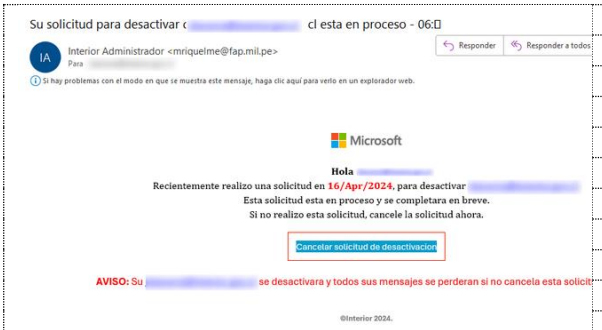
Compañía General de Electricidad (CGE) - Suplantación con malware	
Código de alerta	CMV24-00458
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2024
Última revisión	5 de abril de 2024
Indicadores de compromiso	
Asunto	
REQUERIMIENTO PARA RESOLVER EL TRÁMITE- Últimos dias. - (7322458)	
Correo de salida	
support@bvgo.nl support@the-californian.digipreprod.fr support@cynthiashomesonline.com support@thenonprofittimes.com	
SHA256	
0b54964ac1a1b50ba932561aee89eb9e21c388a2f1ce8034399b79dc078cf289 71e76703ed27e2360577c159daf60e2b26d470090f80dce9fa0ecaf07139075e 7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00458/	

3. Phishing

BancoEstado - Phishing	
Alerta de seguridad cibernética	FPH24-00950
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://fogape.larissakovalchuk.com/1713187838/imagenes/_personas/home/default.asp	
URL de redirección	
https://panavalpaiso.com/activacion/cuenta-raij/	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00950/	



Ministerio del Interior y Seguridad Pública - Phishing	
Alerta de seguridad cibernética	FPH24-00951
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/bafybeidihzirgfqlcmm3hlceu4wshnbxk5m7cjrraps73rzwwam2rtphom/login-update%281%29.html#{Correoelectronico}	
Dirección IP sitio falso	
[104.17.96.13]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00951/	



Microsoft - Phishing	
Alerta de seguridad cibernética	FPH24-00952
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de abril de 2024
Última revisión	16 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/QmfCzd6H3fmoowa2wiURc3W2nttyE6A4pzKDLL1kFfnyqL/#{Correo electronico}	
Dirección IP sitio falso	
[104.17.96.13]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00952/	

4. Vulnerabilidades

paloalto NETWORKS

Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: **csirt.gob.cl/vulnerabilidades**

Palo Alto Networks PAN-OS – Vulnerabilidades	
Código de alerta	VSA24-01002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2024
Última revisión	12 de abril de 2024
CVE	
CVE-2024-3400	
Fabricante	
Palo Alto	
Productos afectados	
Palo Alto Networks PAN-OS • Anteriores a 11.1.2-h3 • Anteriores a 11.0.4-h1 • Anteriores a 10.2.9-h1	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01002/	

Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: **csirt.gob.cl/vulnerabilidades**

PuTTY y otros - Vulnerabilidades	
Código de alerta	VSA24-01003
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2024
Última revisión	17 de abril de 2024
CVE	
CVE-2024-31497	
Fabricante	
Varios	
Productos afectados	
PuTTY 0.68 a 0.80 FileZilla 3.24.1 a 3.66.5 WinSCP 5.9.5 a 6.3.2 TortoiseGit 2.4.0.2 a 2.15.0 TortoiseSVN 1.10.0 a 1.14.6	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01003/	

4. Noticias y concientización

Coordinador Nacional presentó en Panamá los avances legislativos de ciberseguridad

"Hoy, Chile está a la vanguardia en Latinoamérica en seguridad digital. La reciente publicación en el Diario Oficial de la Ley Marco de Ciberseguridad instaura un modelo de gobernanza que no existe en América Latina, que representa un orgullo y un desafío. Esto, ya que la implementación de la ley traerá importantes beneficios a nuestro país en materia de regulación, coordinación, prevención y contención de incidentes", aseguró Daniel Álvarez, Coordinador Nacional de Ciberseguridad de Chile.

Álvarez fue uno de los expositores del nuevo capítulo de las IV Jornadas STIC, actividad que organiza el Centro Criptológico Nacional (CCN-CNI), el Instituto Nacional de Ciberseguridad (INCIBE), el Mando Conjunto del Ciberespacio (MCCE) y RootedCON, todas de España, en conjunto con el Gobierno de Panamá, el Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

En la instancia, el Coordinador Nacional indicó que "considerando el actual escenario, es necesario fomentar y fortalecer la colaboración entre los países en temas de ciberseguridad, y este tipo de actividades nos permite generar esos lazos y alianzas para que juntos trabajemos en soluciones que nos ayuden a incrementar el nivel de seguridad en el ciberespacio".

Adicionalmente, el Coordinador Nacional de Ciberseguridad participó en el panel sobre "El rol del CSIRT en las Estrategias Nacionales de Ciberseguridad" en conjunto al responsable del CSIRT de República Dominicana y en el panel titulado "Marcos institucionales - Colaboración intersectorial" junto a los responsables de los gobiernos de Brasil, Uruguay y un representante del BID.

Ciberconsejos | Cinco consejos básicos de ciberseguridad

Recomendaciones que todos debemos conocer para navegar de manera más cibersegura. ¡Compártelo con tus amigos y familiares! Pueden encontrar la campaña completa aquí, para descargar en formato PDF: https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-cinco-consejos-basicos-de-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.

5. 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.

- Mauricio Andrés Alarcón Jara
- Jaime Rodrigo Pérez Lahaye
- Alejandra Rubilar Peña
- Nelson Salas
- Alexis Daneri

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.04.19 16:00:26 -04'00'