CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 248

semana del 28 de marzo al 4 de abril de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

8

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

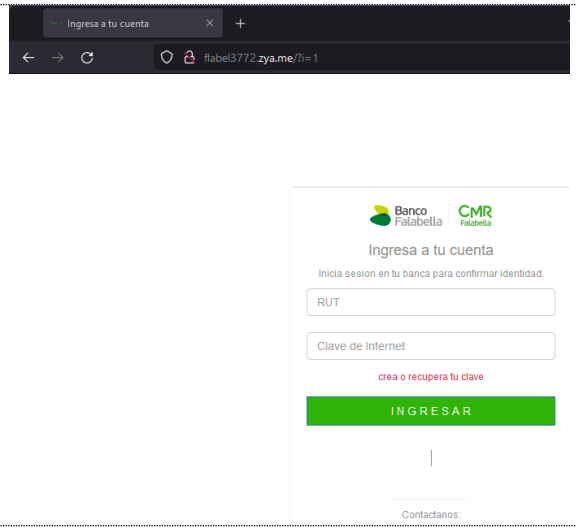
13

Las mitigaciones son útiles en productos de BIND, XZ, HTTP/2 y LayerSlider.

CONTENIDO

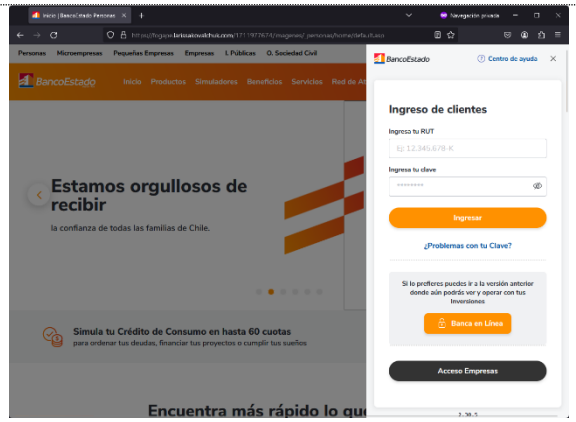
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

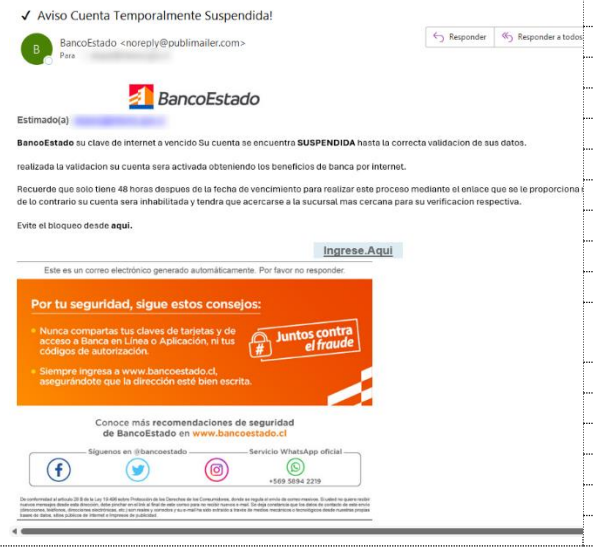


CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Falabella	
Código de alerta	8FFR24-01675
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 abril, 2024
Última revisión	1 abril, 2024
Indicadores de compromiso	
URL del sitio falso	
http://flabel3772[.z}ya.me/?i=1	
URL de redirección	
https://cancelar-compra-4falabella[.]weebly.com/	
Dirección IP sitio falso	
[185.27.134.144]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01675/	

2. Phishing

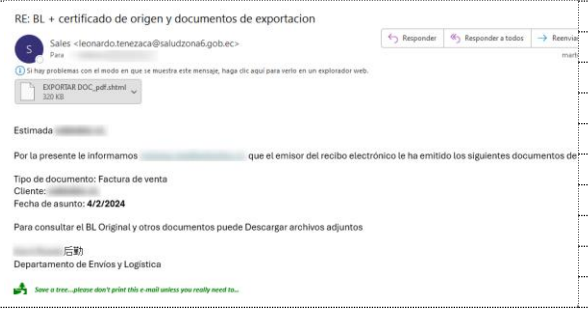


CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00942
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2024
Última revisión	1 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://fogape.larissakovalchuk.com/1711977674/imagenes/_personas/home/default.asp	
URL de redirección	
https://maximocontaval.com/activacion/cuenta-kaoi/	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00942/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00943
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2024
Última revisión	1 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://registrosmshomestado.com/1711982045/imagenes/_personas/home/default.asp	
URL de redirección	
https://comnicenterhomestado.com/activacion/cuenta-jeql/	
Dirección IP sitio falso	
[54.39.196.148]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00943/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	FPH24-00944
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de abril de 2024
Última revisión	2 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://public-b0nstado.com/1712064459/imagenes/_personas/home/default.asp	
URL de redirección	
https://uncerhomestados.club/activacion/cuenta-ldlb/	
Dirección IP sitio falso	
[54.39.196.148]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00944/	



Alerta General - Phishing	
Alerta de seguridad cibernética	FPH24-00944
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de abril de 2024
Última revisión	2 de abril de 2024
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00945/	

3. Vulnerabilidades

BIND - Vulnerabilidad	
Código de alerta	9VSA24-00992-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 marzo, 2024
Última revisión	28 marzo, 2024
CVE	
CVE-2023-4408	
Fabricante	
BIND	
Productos afectados	
9.0.0 a 9.16.45	
9.18.0 a 9.18.21	
9.19.0 a 9.19.19	
9.9.3-S1 a 9.11.37-S1	
9.16.8-S1 a 9.11.37-S1	
9.16.8-S1 a 9.16.45-S1	
9.18.11-S1 a 9.18.21-S1	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/9vsa24-00992/	

ZX Utils - Vulnerabilidad	
Código de alerta	VSA24-00993
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2024
Última revisión	1 de abril de 2024
CVE	
CVE-2024-3094	
Fabricante	
XZ	
Productos afectados	
XZ Utils 5.6.0	
XZ Utils 5.6.1	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-00993/	

LayerSlider, plugin de WordPress - Vulnerabilidad	
Código de alerta	VSA24-00994
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de abril de 2024
Última revisión	3 de abril de 2024
CVE	
CVE-2024-2879	
Fabricante	
Layerslider	
Productos afectados	
LayerSlider 7.9.11 a 7.10.0	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-00994/	

HTTP/2 y otros - Vulnerabilidades	
Código de alerta	VSA24-00994
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2024
Última revisión	4 de abril de 2024
CVE	
CVE-2024-27983	CVE-2024-28182
CVE-2024-27919	CVE-2024-27316
CVE-2024-2758	CVE-2024-31309
CVE-2024-2653	CVE-2024-30255
CVE-2023-45288	CVE-2024-24549
Fabricante	
Múltiples proveedores, entre ellos: HTTP/2 Apache Tomcat Apache Traffic Server Envoy proxy Golang h2 Rust crate nghttp2 Node.js Tempesta FW	
Productos afectados	
Apache Tomcat 11.0.0-M1 a 11.0.0-M16 10.1.0-M1 a 10.1.18, 9.0.0-M1 a 9.0.85 8.5.0 a 8.5.98	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-00994/	

4. Noticias y concientización

Coordinador Nacional de Ciberseguridad en CNN por la ley de ciberseguridad

El Coordinador Nacional de Ciberseguridad, Daniel Álvarez Valenzuela, explica a Futuro 360 de CNN el avance que representa para Chile la promulgación (con apoyo transversal) de la Ley Marco de Ciberseguridad, junto con la creación de la nueva Agencia Nacional de Ciberseguridad.

La nota completa aquí: https://ciberseguridad.gob.cl/noticias/coordinador-nacional-cnn-ley-marco/

Radio Futuro | ""Falta respaldo de información": coordinador de Ciberseguridad advierte sobre deficiencias en gestión ante ataques cibernéticos"

El coordinador nacional de Ciberseguridad, Daniel Álvarez, conversó con Andrea Moletto de #FuturoPQN, de la Radio Futuro, sobre la situación de la ciberseguridad en Chile y las implicancias de la promulgación de la nueva Ley Marco de Ciberseguridad.

La nota completa: https://www.futuro.cl/2024/04/falta-respaldo-de-informacion-coordinador-de-ciberseguridad-advierte-sobre-deficiencias-en-gestion-ante-ataques-ciberneticos/

El Tiempo (Colombia) | Chile se suma a Colombia y otros países de la región con nueva ley de ciberseguridad

Daniel Álvarez, coordinador nacional de ciberseguridad de Chile, habló con El Tiempo de Colombia sobre las claves de la Ley Marco de Ciberseguridad con la que le significan ser el primer país de América Latina y el Caribe en tener una agencia de este tipo y un marco regulatorio de vanguardia en este campo.

En video: https://www.youtube.com/watch?v=MU2I5zaH0GE

Ciberconsejos Operación Renta 2024

Ante el tradicional aumento de las campañas de phishing que buscan aprovecharse de la Operación Renta suplantando al Servicio de Impuestos Internos y la Tesorería General de la República, compartimos recomendaciones para que los ciudadanos sepan evitar caer en este tipo de engaños.

La guía completa: https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-operacion-renta-2024/

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.

- Pablo Cornejo Pérez
- Antonio Ricardo Osses Izquierdo
- Pablo Viveros
- César Labbé
- Eduardo Araya

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.04.05 18:33:48 -03'00'