CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 187

Semana del 27 de enero al 2 de febrero

PARCHES COMPARTIDOS

3

Las mitigaciones son útiles en productos de OpenEMR, QNAP y Lexmark.

IP INFORMADAS

8

URL ADVERTIDAS

13

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

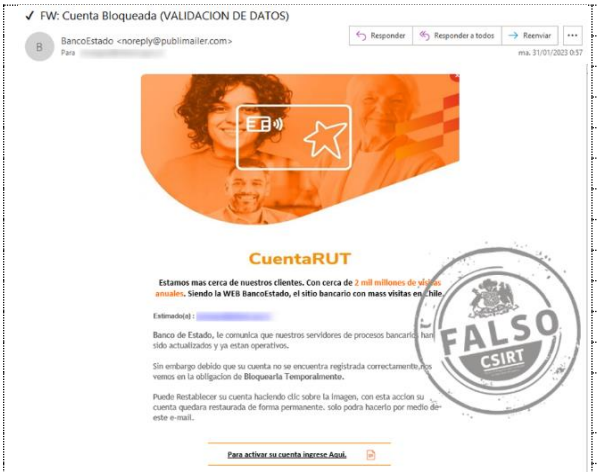
CSIRT alerta de nueva campaña de phishing que suplanta al SII	
Alerta de seguridad cibernética	8FPH23-00731-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//ppcproyectos[.]com/incoming.php?id=TYDWITCABYEVVZMTFEWZXDURJWGKMDLNAJCWVWEKJJKAESKALSVXDZSBHXRESJWLREDOOFWCWUYHPKWGBM	
Dirección IP	
[198.59.144.138]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00731-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00731-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a Impuestos Internos	
Alerta de seguridad cibernética	8FPH23-00732-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023
Indicadores de compromiso	
Dirección IP	
[198.59.144.138]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00732-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00732-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00733-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//cartoonpuzzl3s[.]com/activacion/cuenta-bpwz/	
URL sitio falso	
https[:]//xtraillconver[.]com/1674842723/imagenes/_personas/home/default.asp	
Dirección IP	
[138.128.189.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00733-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00733-01.pdf	

CSIRT alerta de campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00734-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2023
Última revisión	30 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//smartgift[.]live/ips_cl/?cep=ADpcvY4BIMnvUrAW9fx58sqTbjRe25a7RiuOiwXC_-2Y2fTYOJmDp42E-8Htv8msrXSiDuN0bmLZZ5ZWDcUpZCeDOka_1cVJ7OpbjLvjP0UtEFc7bd71_Dhsbw-xY61uHCyLqTHq-zeqR6mUD0VfgX4b38enLC1YHiwW008epixUtQfSnEx6FvbYOTVC_miypOqhiaCoUbhLDqVUUsEQIao8IK_cS3Qy98gWLwtgINzFs2irz1qHz-oXXeTHfgSxhosxbT37OxtT-ViuXGUoYRIQe_6B2UbGjYCCsXni3mijBdhc2NdzNyt8qok7Isfw670FxHsfBDa-9i9XG4uDofRPVP_v-MuXCpEoEraN9SLZ1_eQJs6u5hQZfcehSKHb&lptoken=165974c584b3519f647c	
Dirección IP	
[84.32.190.20]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00734-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00734-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al SII	
Alerta de seguridad cibernética	8FPH23-00735-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2023
Última revisión	30 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//tequilamisorpresa[.]com/ytweshdg.php?id=wkwxfybauwrkeqzgapwyjkugypdfwqupdiuqkfmkewdounxwysesjljrxcbgledjfbctzpjhekj	
Dirección IP	
[65.99.252.243]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00735-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00735-01.pdf	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00736-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-aotq/	
URL sitio falso	
https://prestamoonlineibk[.]net/1675171907/imagenes/_personas/home/default.asp	
Dirección IP	
[186.64.119.85]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00736-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00736-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00737-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//cartoonpuzzl3s[.]com/activacion/cuenta-htna/	
URL sitio falso	
https[:]//xtraillconver[.]com/1675189288/imagenes/_personas/home/default.asp	
Dirección IP	
[138.128.189.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00737-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00737-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00738-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//nwmmayorsa[.]com/activacion/cuenta-igzs/	
URL sitio falso	
https[:]//nmhportal[.]click/1675190214/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.21.215]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00738-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00738-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00739-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de febrero de 2023
Última revisión	1 de febrero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-vbvq/	
URL sitio falso	
https[:]//prestamoonlineibk[.]net/1675256303/imagenes/_personas/home/default.asp	
Dirección IP	
[186.64.119.85]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00739-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00739-01.pdf	

2. Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica que afecta a productos Lexmark	
Alerta de seguridad cibernética	9VSA23-00778-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023
CVE	
CVE-2023-23560	
Fabricantes	
Lexmark	
Productos afectados	
Múltiples aparatos Lexmark, los que aparecen listados en su comunicado oficial (https://publications.lexmark.com/publications/security-alerts/CVE-2023-23560.pdf).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00778-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA22-00778-01.pdf	

CSIRT comparte información de vulnerabilidad crítica en QNAP NAS	
Alerta de seguridad cibernética	9VSA23-00779-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023
CVE	
CVE-2022-27596	
Fabricantes	
QNAP	
Productos afectados	
QTS 5.0.1 y QuTS hero h5.0.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00779-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00779-01.pdf	

CSIRT alerta de vulnerabilidades críticas en OpenEMR	
Alerta de seguridad cibernética	9VSA23-00780-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	2 de febrero de 2023
Última revisión	2 de febrero de 2023
CVE	
CVE-2022-27596	
Fabricantes	
OpenEMR	
Productos afectados	
CVE no disponible CVE no disponible CVE no disponible	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00780-01/	
https://www.csirt.gob.cl/media/2023/02/9VSA23-00780-01.pdf	

3. Concientización

Ciberconsejos | Cómo crear una clave segura

Esta semana queremos recordarles la importancia de contar con contraseñas únicas y difíciles de adivinar para los ciberdelincuentes, con los siguientes ciberconsejos. Y es que definir contraseñas que sean fáciles de recordar, pero difíciles de adivinar, es el desafío que tienen los usuarios de internet.

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-clave-segura_2023/.

Ciberdiccionario Volumen 28

Los conceptos definidos en el ciberdiccionario del CSIRT de Gobierno esta semana: TIC, actores estatales, sistemas heredados o legacy y OSINT. Pueden encontrar todos los números del ciberdiccionario, junto a nuestros ciberconsejos y otras guías de concientización siempre en https://www.csirt.gob.cl/recomendaciones/.

Enlace: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-28/

4. 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.

- Didye Paolo Orellana Ponce
- Julian Leou
- Javier Ignacio Candia Tapia
- Miguel Morales Saravia

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.03 16:55:19 -03'00'