Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

04-03-2022 | Año 4 | N°139

Boletín de Seguridad Cibernética

Semana del 25 de febrero al 03 de marzo de 2022

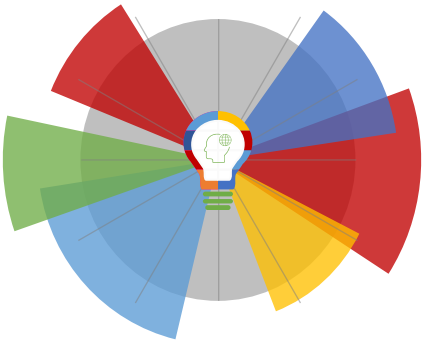
La semana en cifras

Se advirtieron

3

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches

11

para vulnerabilidades

Las mitigaciones son útiles en productos SolarWinds, Cisco y PJSIP

IP

2

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

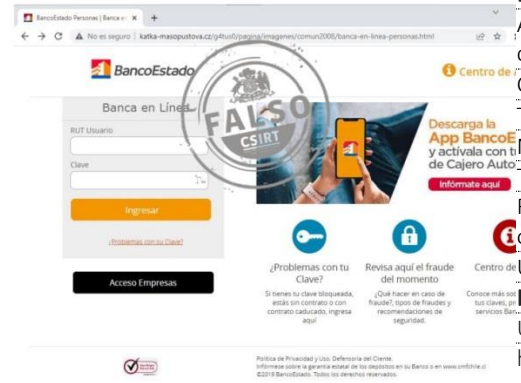
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob https://www.linkedin.com/company/csirt-gob

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de nueva página fraudulenta que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FFR22-01058-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2022
Última revisión	28 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
http://www.katka-masopustova[.]cz/g4tus0/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[46.101.52.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01058-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01058-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante campaña de smishing que suplanta a Copec	
Alerta de seguridad cibernética	8FPH22-00477-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
URL SMS	
http://mailpersuade[.]top/copec/tb.php?khflmume16461726956 07	
URL sitio falso	
https://cxjyuet[.]cn/mqQtEYMb/copec/?_t=1646222910875#164 6222911898	
IP	
[104.21.47.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00477-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00477-01.pdf	

Vulnerabilidades

CSIRT alerta ante nueva vulnerabilidad en SolarWinds Serv-U	
Alerta de seguridad cibernética	9VSA22-00581-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2022
Última revisión	3 de marzo de 2022
CVE	
CVE-2021-35250	
Fabricante	
SolarWinds	
Productos afectados	
Servidor FTP Serv-U: 15.3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00581-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00581-01.pdf	

CSIRT alerta ante vulnerabilidades críticas en productos de Cisco	
Alerta de seguridad cibernética	9VSA22-00582-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Bajo
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2022
Última revisión	3 de marzo de 2022
CVE	
CVE-2022-20754 CVE-2022-20755 CVE-2022-20756 CVE-2022-20762 CVE-2022-20765	
Fabricante	
Cisco	
Productos afectados	
CVE-2022-20754 y CVE-2022-20755: Cisco Expressway Series y Cisco TelePresence VCS 14.0 y anteriores. CVE-2022-20762: Cisco Ultra Cloud Core – Subscriber Microservices Infrastructure 2020.02.2, 2020.02.6, 2020.02.7. CVE-2022-20756: Cisco Identity Services Engine RADIUS Service 2.4 a 3.1. CVE-2022-20665: Cisco StarOS 21.24 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00582-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00582-01-1.pdf	

CSIRT alerta de vulnerabilidades en PJSIP	
Alerta de seguridad cibernética	9VSA22-00583-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2022
Última revisión	3 de marzo de 2022
CVE	
CVE-2021-43299 CVE-2021-43300 CVE-2021-43301 CVE-2021-43302 CVE-2021-43303	
Fabricante	
PJSIP	
Productos afectados	
Versión 2.11.1 o inferior	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00583-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00583-01.pdf	

Actualidad

CSIRT de Gobierno y Cuna Cultural reúnen actores del ciberespacio nacional en contra del acoso digital

El reciente y devastador caso de Drayke Hardman, niño estadounidense de 12 años que se quitó la vida siendo víctima de bullying, nos recuerda la importancia de reforzar la educación en materias del uso de la tecnología desde la infancia, incluyendo la entrega de las herramientas adecuadas para una mejor convivencia digital.

Esta es uno de las motivaciones detrás de la iniciativa Cuna Cultural, la primera campaña de ciberhigiene para niños y jóvenes en edad escolar, que busca incentivar el uso responsable de internet en niños, niñas y adolescentes del país, a través de comunidades educativas y centros de familia e infancia. Para ello, contempla un programa educativo de formación ciudadana dedicado a prevenir situaciones de acoso y vulnerabilidad que dañen o afecten la condición física y emocional de los menores de edad durante su etapa de desarrollo y escolar.

Ayer, Cuna Cultural reunió en la sede del CSIRT de Gobierno a importantes actores del mundo de la ciberseguridad y la protección de nuestros menores en internet, para reforzar su compromiso con su concientización en formas seguras de relacionarse en línea, y en la eliminación de riesgos digitales que buscan dañar a niños, niñas y adolescentes.

Sobre la labor de Cuna Cultural, el Subsecretario del Interior, Juan Francisco Galli destacó que “iniciativas como las de Cuna Cultural son cada día más importantes, en la medida en que una mayor parte de nuestras vidas transcurre en línea, lo que lógicamente también incluye a niños, niñas y adolescentes. Se vuelve clave enseñarle a los NNA sobre conductas seguras en internet, para que sepan cómo protegerse ante flagelos como el grooming y el cyberbullying, que tengan claro, por ejemplo, que no deben cometer acoso en línea y que si lo sufren, deben denunciarlo. Y para lograr ello se debe construir previamente un ambiente de confianza con padres y profesores, como los que busca generar Cuna Cultural”.

En la misma línea, el CSIRT de Gobierno, dependiente de la Subsecretaría del Interior, continúa su combate al cyberbulling a través de la concientización, con la publicación periódica de consejos para mejorar la convivencia digital, especialmente de los niños y adolescentes, y de guías que entregan los pasos para realizar la denuncia en los casos de ciberacoso. “Resulta muy importante que acompañemos a niños, niñas y adolescentes en su interacción con Internet, que mantengamos confianza con ellos y estar atentos ante cualquier señal de que puedan estar siendo víctimas de acoso, y denunciar estos actos inmediatamente ante las plataformas respectivas y, de poner en

riesgo a NNA, a la PDI y el Ministerio Público", indica el Director del CSIRT de Gobierno, Vartan Ishanoglu.

"Los hijos e hijas son reflejo de sus padres y madres. El rol de las comunidades escolares es amplio, ya que para lograr el objetivo de un clima escolar positivo deben mediar entre distintos modelos de parentalidad, trabajando proactivamente para lograr una buena convivencia en su comunidad", explican Evangely Zamorano y Emanuel Pacheco desde la Fundación Katy Summer, cuya finalidad es terminar con el acoso escolar.La fundación añade que "el dolor que generan las agresiones en el bullying se sienten muy intensamente y puede conducir a situaciones irreversibles", complementando con el dato de que el 55% de los jóvenes entre 15 y 19 años declaró haber sido ciberacosado al menos una vez en los últimos tres meses del 2021, y el 44% de estos mostraron sintomatología depresiva severa. Esto, según un estudio de la Fundación Katy Summer para la Secretaría General de Gobierno (Segegob).

Además, "de aquellos jóvenes que viven ciberacoso, un 47% se autolesiona pero menos del 5% pide ayuda a su familia o comunidad escolar. Esto demuestra el daño concreto en la salud mental que tiene hoy nuestra juventud", indicaron en Katy Summer. Conversar sobre el acoso escolar con los niños y sus familias es primordial hoy en un contexto de regreso a clase clases presenciales, considerando que se mantendrá la convivencia digital de los jóvenes por internet.

Asimismo, Blanquita Honorato, Subsecretaria de la Niñez, resalta que desde su cartera, "estamos convencidos de que el bullying es muchas veces consecuencia de ambientes y dinámicas familiares violentas o poco sanas", por lo que "el Estado, en su rol de garante de los derechos de los niños, y para abordar las temáticas que afectan a NNA, debe también trabajar con las familias para promover y fortalecer su rol protector primordial". En este sentido, la secretaria de Estado resalta que la próxima a ser promulgada Ley de Garantías de los Derechos de la Niñez y Adolescencia, la que "establece mayores responsabilidades y facultades para el Estado en torno a asumir este rol de garante, no solo para actuar en casos de bullying sino también para prevenirlo y promover entornos saludables para el desarrollo óptimo de NNA".

El Senador Kenneth Pugh, quien lidera la Mesa de Trabajo de Ciberseguridad de la Cámara Alta, señala por su parte que "la violencia en la redes sociales está llegando a niveles alarmantes, con discursos de odio y desinformación", por lo que "debemos, como país, hacer esfuerzos muy importantes desde la temprana edad para inculcar un uso responsable de la internet y todos los medios que ella nos brinda, como por ejemplo las redes sociales". Así, señala el Senador, es fundamental guiar a los niños y niñas en su exposición a internet, supervisando que vaya siendo realizada de acuerdo a su edad, hasta que tengan la madurez necesaria para navegar solos.

Esto es clave porque para el Senador Pugh, "no podemos permitir que los más violentos se apropien del ciberespacio, y que por esas acciones condenables otros tengan que sufrir los efectos

de la ciberviolencia, llevando incluso en extremos a algunos a quitarse la vida por ello". El parlamentario termina haciendo un llamado a denunciar los casos de ciberacoso, porque hacerlo podría salvar una vida.

El Subsecretario de Telecomunicaciones, Francisco Moreno, complementa recordando que "de acuerdo a datos de una radiografía digital que conocimos hace algunas semanas, el 30% de los niños entre 8 y 12 años y el 50% de los niños entre 13 y 17 años se conectan a internet más de 4 horas al día. Además, el 55% de los consultados señaló haber sido contactado por personas que no conocen, el 55% dijo haber jugado en línea con personas que no conocen, el 38% señaló haber sido víctima de burlas, el 37% señaló que vio o recibió fotos o videos violentos y el 21% reconoció haberse burlado de otras personas". En vista de esta realidad, agrega, "es fundamental que generemos un ambiente seguro y libre de bullying, tanto en la vida real como en la vida digital y que además generemos las condiciones para que nuestros niños puedan adquirir habilidades cognitivas que permitan a los usuarios relacionarse sanamente entre sí a través de la pantalla, haciendo uso responsable de la tecnología".

La hiperconexión de los NNA, "trae consigo responsabilidades respecto de su seguridad, privacidad y bienestar, existiendo el permanente riesgo de ser expuestos a algún tipo de violencia, abuso o explotación", explica asimismo el Prefecto Inspector Leonel Fuentes, Jefe Nacional de Delitos Económicos y Medio Ambiente de la Policía de Investigaciones (PDI).

Ciberconsejos para proteger a tus hijos en redes sociales

Ya comenzó el año escolar y muchos padres, emocionados por el primer día de clases, publican fotografías de sus hijos para guardar esos lindos recuerdos. En los ciberconsejos que entrega el CSIRT cada semana, hablamos sobre lo que nunca debes publicar para cuidar y resguardar la seguridad de los niños y niñas.

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 los sitios web que se ingresen sean los oficiales.

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Milton Matamala
- Felipe Pizarro
- Miguel Bretti