Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

19-02-2021 | Año 3 | N°85

Boletín de Seguridad Cibernética

Semana del 12 al 18 de Febrero de 2021

Resumen de la semana en cifras

Hash

8

Sha

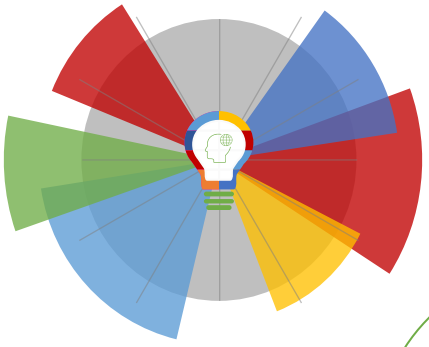
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

11

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

6

para vulnerabilidades

Las mitigaciones son útiles para productos Red Hat y Laravel.

IPs

7

Informadas

Listado de IPs 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

Sitios fraudulentos

Imagen del sitio

CSIRT informa suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR21-00896-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//www.sant-ander-movil[.]xyz/1613657710/personas/index.asp	
IP	
[68.65.120.230]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00896-01-2/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00896-01.pdf	

Imagen del sitio

CSIRT informa página bancaria falsa	
Alerta de seguridad cibernética	8FFR21-00897-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://sant-ander-actualizacion-de-datos[.]app/1613073959/personas/index.asp	
IP	
[198.54.121.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00897-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00897-01.pdf	

Imagen del sitio

CSIRT advierte portal de banco fraudulento	
Alerta de seguridad cibernética	8FFR21-00898-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://santand-er-personas[.]live/1613073431/personas/index.asp	
IP	
[198.54.121.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00898-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00898-01.pdf	

Imagen del sitio

CSIRT advierte suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR21-00899-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//banca-santa-der[.]live/16136611153/personas/index.asp	
IP	
[162.0.235.23]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00899-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00899-01.pdf	

Phishing

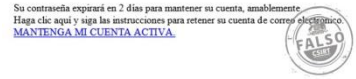
Imagen del mensaje

CSIRT advierte phishing de supuesta cuenta bloqueada	
Alerta de seguridad cibernética	8FPH21-00372-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Febrero de 2021
Última revisión	16 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3jQqqmv?l=www.santander.cl	
URL sitio falso	
https://lolivette[.]com/wp-content/www.santander.cl/pagina/login[.]asp	
IP	
[193.225.199.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00372-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00372-01.pdf	

Imagen del mensaje

CSIRT informa phishing de cuenta bloqueada	
Alerta de seguridad cibernética	8FPH21-00373-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Febrero de 2021
Última revisión	17 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3jQqqmv?l=www.santander.cl	
URL sitio falso	
http://gaborestarsa2005[.]hu/wp-includes/www.santander.cl/pagina/login.asp	
IP	
[185.6.139.216]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00373-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00373-01.pdf	

Imagen del mensaje



CSIRT advierte phishing de caducidad de contraseña	
Alerta de seguridad cibernética	8FPH21-00374-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://zm300.onrender.com/zim[.]html	
IP	
[181.196.107.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00374-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00374-01.pdf	

Imagen del mensaje

CSIRT advierte smishing de tarjeta de crédito bloqueada	
Alerta de seguridad cibernética	8FPH21-00375-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
Indicadores de compromiso	
Urls Redirección	
https[:]//app-validarsms[.]website/?sms=santander	
URL sitio falso	
https[:]//banca-santa-der[.]live/1613656969/personas/index[.]asp	
IP	
[162.0.235.23]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00375-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00375-01.pdf	

Malware

CSIRT advierte malware con supuesto registro para vacuna Covid-19	
Alerta de seguridad cibernética	2CMV21-00147-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2021
Última revisión	12 de Febrero de 2021
Indicadores de compromiso	
SHA256	
675C846849A0A3B373A3C98FF5C2143F6AB87CEF1A0008C5D30383C5CDC3107E	
C9598E8F45BBD36F6CD8B24499BD96DF599BF499A77F4195C1FF3D7D3EAE8212	
0020DB7D3AC1F10CEAC645C12557F0A78472A7DCEE2D7980E911A4AE3350E1C4	
F695B8B7B0AB2FA84DF2903F70F7EFB397F1A03ED09DAF634521A8D5D9D52CE4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00147-01/	
https://www.csirt.gob.cl/media/2021/02/2CMV21-00147-01.pdf	

CSIRT advierte malware con supuesto registro de vacuna Covid-19	
Alerta de seguridad cibernética	2CMV21-00148-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Febrero de 2021
Última revisión	17 de Febrero de 2021
Indicadores de compromiso	
SHA256	
675c846849a0a3b373a3c98ff5c2143f6ab87cef1a0008c5d30383c5cdc3107e	
c4b4e70e79e75c71cc78f2668b09e461ac428c1fb700248c9e514ea5c6ede9b1	
00517fb74362600edc6a19aed8f05600edb754cfbbcd2a9f5e20100aed41bf72	
3cf21f31c5281600ca70d4c87f4f829f0011c6740084d26c3665d2729b092da2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00148-01/	
https://www.csirt.gob.cl/media/2021/02/2CMV21-00148-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades que afectan a productos Red Hat	
Alerta de seguridad cibernética	9VSA21-00391-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Febrero de 2021
Última revisión	16 de Febrero de 2021
CVE	
CVE-2020-27827 - CVE-2020-35498 - CVE-2020-17525 CVE-2021-1721	
Fabricante	
Red Hat	
Productos afectados	
openvswitch2.13 (Red Hat package): 2.13.0-71.el8fdp, 2.13.0-72.el8fdp dotnet5.0 (Red Hat package): 5.0.102-2.el8_3 Red Hat Enterprise Linux Fast Datapath: 8. Red Hat Enterprise Linux for ARM 64 – Extended Update Support: 8.1 Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.1 Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.1 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux for x86_64: 8.0 Red Hat Enterprise Linux Server – TUS: 8.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00391-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00391-01.pdf	

CSIRT comparte mitigaciones obtenidas de Laravel	
Alerta de seguridad cibernética	9VSA21-00392-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Febrero de 2021
Última revisión	17 de Febrero de 2021
CVE	
CVE-2021-3129	
Fabricante	
Laravel	
Productos afectados	
Ignition, versiones 1.16.0 a 1.16.4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00392-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00392-01.pdf	

CSIRT advierte de una vulnerabilidad que afecta a Agora Video SDK	
Alerta de seguridad cibernética	9VSA21-00393-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2021
Última revisión	18 de Febrero de 2021
CVE	
CVE-2020-25605	
Fabricante	
Agora Video SDK	
Productos afectados	
Agora SDK, versions anteriores a la 3.2.1. Aplicaciones como eHarmony, MeetMe, Skout, Plenty of Fish, Talkspace, Practo, Dr. First's Backline y el robot personal temi	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00393-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00393-01.pdf	

Actualidad

Cibersucesos no. 7

Promover una vuelta a clases virtual segura es el eje de esta séptima edición de Cibersucesos, que lanzamos hoy como CSIRT de Gobierno. Así, como tema principal ofrecemos un decálogo de convivencia en las redes sociales, dirigido a los jóvenes, para que sepan qué hacer al enfrentarse al lado oscuro de la interacción digital, como el ciberbullying, la exposición a contenido violento y perturbador, la sextorsión y la violación de su privacidad.

En la misma línea, compartimos los pasos a seguir para que los niños tengan la mayor seguridad al conectarse para recibir sus clases de forma virtual, tendencia que continúa desde el año pasado a causa de la pandemia, y que se ha visto posibilitada en muchos casos gracias a los esfuerzos del Gobierno para proveer de computadores y conexión de internet a estudiantes vulnerables a lo largo del país. Colombia es la nación que comparte su ejemplo en la sección Cooperación Internacional, a través de la experiencia de "En TIC confío", iniciativa destinada a concientizar a los jóvenes para adquirir hábitos saludables en internet.

En Comunidad Hacker, los creadores de la Fundación Katy Summer comparten los proyectos e iniciativas que han desarrollado para combatir el ciberacoso a los menores, en honor a su hija, Katy Winter, que murió a causa de este flagelo de la vida online que afecta a niños y adolescentes. Asimismo, nuestros expertos de la sección Legal analizan, en esta ocasión, las implicancias judiciales del ciberacoso o ciberbullying, cómo se define y su regulación (o más bien, falta de) en nuestro país.

Ver más: https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-7/

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- 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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Cristóbal Herrera
- Armando Valenzuela
- Romel Rivas
- Edith Ramos
- Jacob Salazar

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.19 12:10:16 -03'00'