Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

26-02-2021 | Año 3 | N°86

Boletín de Seguridad Cibernética

Semana del 19 al 26 de Febrero de 2021

Resumen de la semana en cifras

Hash

5

Sha

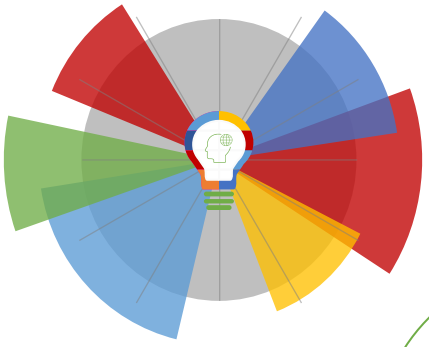
Asociadas a campañas de phishing con archivos que contienen malware

Se advirtieron

13

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

14

para vulnerabilidades

Las mitigaciones son útiles para productos de Mozilla y VMware.

IPs

22

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

Sitios fraudulentos

Imagen del sitio

CSIRT advierte página de programas informáticos falsa	
Alerta de seguridad cibernética	8FFR21-00900-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Febrero de 2021
Última revisión	19 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http://utiltil[.]cl/Sun/office/	
IP	
[131.72.237.67]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00900-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00900-01.pdf	

Imagen del sitio

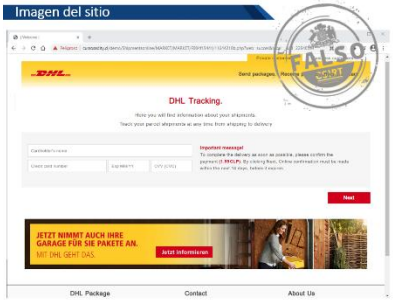
CSIRT advierte suplantación de sitio de alojamiento de archivos	
Alerta de seguridad cibernética	8FFR21-00901-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Febrero de 2021
Última revisión	19 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.nbpropiedades[.]cl/document73839827722/proposal73682732	
IP	
[66.232.107.218]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00901-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00901-01.pdf	

Imagen del sitio

CSIRT informa página fraudulenta que suplanta a banco	
Alerta de seguridad cibernética	8FFR21-00902-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Febrero de 2021
Última revisión	23 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://santan-nder[.]xyz/1614092974/personas/index.asp	
IP	
[198.54.115.194]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00902-01-csirt-informa-de-pagina-fraudulenta-que-busca-suplantar-al-banco-santander/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00902-01.pdf	

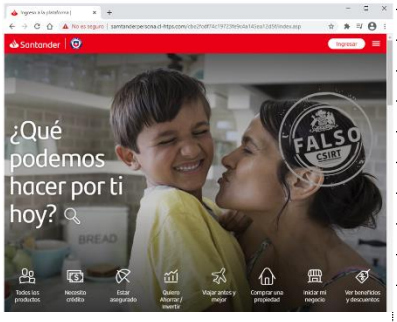
CSIRT advierte página fraudulenta de suplantación bancaria	
Alerta de seguridad cibernética	8FFR21-00903-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Febrero de 2021
Última revisión	24 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://sant-ander-banco[.]ltd/1614093770/personas/index.asp	
IP	
[198.54.114.179]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00903-01-csirt-advierte-de-pagina-fraudulenta-de-suplantacion-bancaria/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00903-01.pdf	

Imagen del sitio



CSIRT advierte de página que suplanta a DHL	
Alerta de seguridad cibernética	8FFR21-00904-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.cursosadity[.]cl/demo/Shipmentsonline/MARKET/MARKET/	
IP	
[209.124.90.240]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00904-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00904-01.pdf	

Imagen del sitio



CSIRT advierte de suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR21-00905-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://samtanderpersona.cl-htps.com/0245b7eeb055160a689aea3d3e2cc31a/index.asp	
IP	
[162.0.215.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00905-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00905-01.pdf	

Imagen del sitio

CSIRT advierte de falso sitio bancario	
Alerta de seguridad cibernética	8FFR21-00906-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.portalsantandercl.es-pehome[.]com/1614260728/personas/index.asp	
IP	
[209.159.156.253]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00906-01-csirt-advierte-de-falso-sitio-bancario/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00906-01-1.pdf	

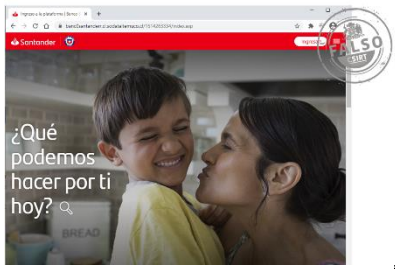
Imagen del sitio

CSIRT advierte por página fraudulenta bancaria	
Alerta de seguridad cibernética	8FFR21-00907-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http://atulitinternational[.]com/1614259242/index.asp	
IP	
[81.19.211.34]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00906-01-csirt-advierte-de-falso-sitio-bancario/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00907-01.pdf	

Imagen del sitio

CSIRT advierte por página fraudulenta bancaria	
Alerta de seguridad cibernética	8FFR21-00908-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://banc0santanderr.cl.bikemonkey[.]cl/1614262752/index.asp	
IP	
[190.4.193.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00908-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00908-01.pdf	

Imagen del sitio



CSIRT alerta por página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR21-00909-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://banc0santanderr.cl.sodataltemuco[.]cl/1614263334/index.asp	
IP	
[201.148.104.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00909-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00909-01.pdf	

Phishing

Imagen del mensaje

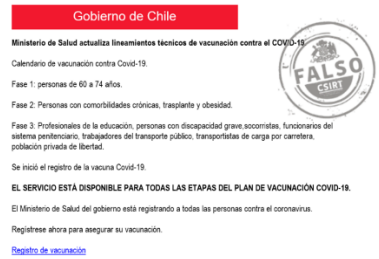
CSIRT advierte phishing de SúperClave bloqueada	
Alerta de seguridad cibernética	8FPH21-00376-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Febrero de 2021
Última revisión	19 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://samtanderpersona-cl.beingbamboo[.]com/b04cb2898fcbb657c1c3c2b6af207eeb/index.asp	
IP	
[68.65.123.231]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00376-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00376-01.pdf	

Imagen del mensaje

CSIRT advierte de campaña de phishing hacia clientes bancarios	
Alerta de seguridad cibernética	8FPH21-00377-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Febrero de 2021
Última revisión	23 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/37AZcva?l=www.santander.cl http://wordpress.roma[.]it/favicon/enviar02.php?l=2010228726 http://www.lacreatura.esivalladolid[.]com/activacion/cuenta-eaqr/	
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/8fph21-00377-1/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00377-01.pdf	

Malware

IMAGEN DEL MENSAJE



CSIRT advierte malware con supuesto registro para vacuna Covid-19	
Alerta de seguridad cibernética	2CMV21-00149-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Febrero de 2021
Última revisión	26 de Febrero de 2021
Indicadores de compromiso	
SHA256	
2B8D65058F4CB144A42AE154AEB3EFF44B11DD3F641B58BBDB09DC61D91FBAC	
D69A4DA64A61E8B7B135F70652CCC210218E7D32BF29D705B1D15A4820921F8E	
6E9A920C888AB3491E36139D0D9FBACF2B615716FADB3650023A65D4E33583D7	
2FCBD6861D299B61A4231DC34BC750907F1C7D2EE9B026C9FC223AE5A6182F03	
3CF21F31C5281600CA70D4C87F4F829F0011C6740084D26C3665D2729B092DA2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00149-01-csirt-advierte-malware-con-falso-registro-de-vacuna-covid-19/	
https://www.csirt.gob.cl/media/2021/02/2CMV21-00149-01.pdf	

Vulnerabilidades

CSIRT informa de vulnerabilidades en productos de Mozilla	
Alerta de seguridad cibernética	9VSA21-00394-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Febrero de 2021
Última revisión	24 de Febrero de 2021
CVE	
CVE-2021-23968 CVE-2021-23969 CVE-2021-23970 CVE-2021-23971 CVE-2021-23972 CVE-2021-23973 CVE-2021-23974 CVE-2021-23975 CVE-2021-23976 CVE-2021-23977 CVE-2021-23978 CVE-2021-23979	
Fabricante	
Mozilla	
Productos afectados	
Mozilla Firefox, versiones de la 60.0 a la 85.0.2. Mozilla Firefox ESR, versiones de la 60.0 a la 78.7.1. Mozilla Thunderbird, versiones de la 60.0 a la 78.7.1. Firefox para Android: versiones 80.1.2. a la 85.1.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00394-01-csirt-informa-de-vulnerabilidades-en-productos-de-mozilla/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00394-01.pdf	

CSIRT alerta vulnerabilidades en VMware	
Alerta de seguridad cibernética	9VSA21-00395-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
CVE	
CVE-2021-21972 CVE-2021-21973	
Fabricante	
VMware	
Productos afectados	
vCenter Server, versiones 6.5 a 7.0 Cloud Foundation, versiones anteriores a la 3.10.1.2, 4.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00395-01-csirt-alerta-vulnerabilidades-en-vmware/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00395-01.pdf	

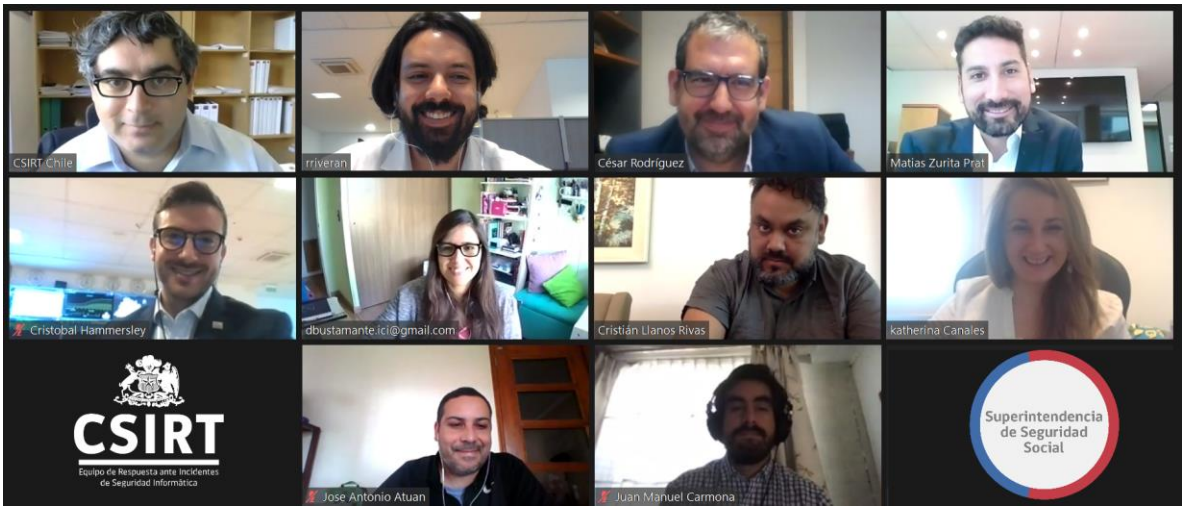
IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
5,188,206,234	Krez 999 Eood	4IIA21-00030-01
45,142,120,180	Uninet S.A. de C.V.	4IIA21-00030-01
87.246.7.243	Internet Hosting LTD	4IIA21-00030-01
78,128,113,130	Miti 2000 EOOD	4IIA21-00030-01
141.98.80.133	NForce Entertainment BV	4IIA21-00030-01
185.24.233.33	Sternforth Ltd.	4IIA21-00030-01
45,142,120,147	Uab host baltic, lt	4IIA21-00031-01
2.57.122.16	Pptechnology limited	4IIA21-00031-01
103,133,111,129	Vietnam posts and telecommunications group	4IIA21-00031-01
210.92.18.169	Ehostict	4IIA21-00031-01

Actualidad

CSIRT presenta a la Suseso resultados de Evaluación de Madurez en Ciberseguridad de las Cajas de Compensación



El CSIRT de Gobierno, dependiente de la Subsecretaría del Interior, presentó a la Superintendencia de Seguridad Social (Suseso) los resultados de la Evaluación de la Madurez en Ciberseguridad de las Cajas de Compensación, entidades que son fiscalizadas por la Suseso.

La correspondiente reunión, hecha de forma virtual, fue dirigida por los dos más altos cargos de las respectivas instituciones, César Rodríguez, superintendente (s) de la Suseso e intendente de Beneficios Sociales, y Carlos Landeros, director nacional del CSIRT de Gobierno.

Esta evaluación tiene como objetivo principal conocer las oportunidades de mejora, en términos de ciberseguridad, dentro de las distintas cajas de compensación. Es además la primera vez que el CSIRT evalúa la madurez de la ciberseguridad en este tipo de instituciones.

La iniciativa permite asimismo a la Suseso y el CSIRT avanzar hacia el desarrollo de una circular que fije normativas y estándares comunes entre todas las cajas de compensación, proceso que ya se encuentra en su recta final en lo relativo a las mutuales, entidades igualmente fiscalizadas por la Suseso.

Ciberconsejos para evitar ser víctimas del spoofing

Los ataques a las conexiones inalámbricas son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas para saltarse las medidas de seguridad, infectar o tomar control de nuestros dispositivos.

Un ataque de spoofing ocurre cuando una persona pretende ser otra con el fin de inducir a su víctima a que comparta sus datos personales o para que haga alguna acción en nombre del falsificador. Normalmente, el timador se esforzará en establecer una relación de confianza con su objetivo, para asegurarse de que comparta sus datos sensibles con más facilidad.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-ser-victimas-del-spoofing/

Ciberconsejos para una conexión a redes Wifi públicas más segura

En vacaciones, solemos estar menos tiempo en nuestra casa y al usar internet, en ocasiones, conectamos nuestros dispositivos a redes wifi abiertas, las que están disponibles en distintos lugares como restaurante, supermercado, hoteles, estaciones de metro, etc., para tener mejor conexión o ahorrar en consumo de datos. Sin embargo, debemos tener cuidado, ya que detrás de esta alternativa hay delincuentes que se aprovechan para cometer algunos delitos.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-conexion-a-redes-wifi-publicas-mas-segura/

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.

- Roberto Sapiain

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.26 15:32:52 -03'00'