Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

02-12-2021 | Año 3 | N°126

Boletín de Seguridad Cibernética

Semana del 26 de noviembre
al 02 de diciembre de 2021

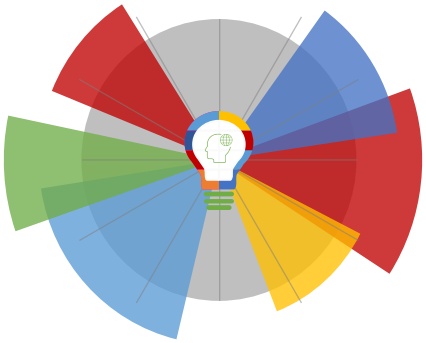
La semana en cifras

Hash

8

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

60

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

4

para vulnerabilidades

Las mitigaciones son útiles en productos Trend Micro, HP y Wordpress.

IP

9

Informadas

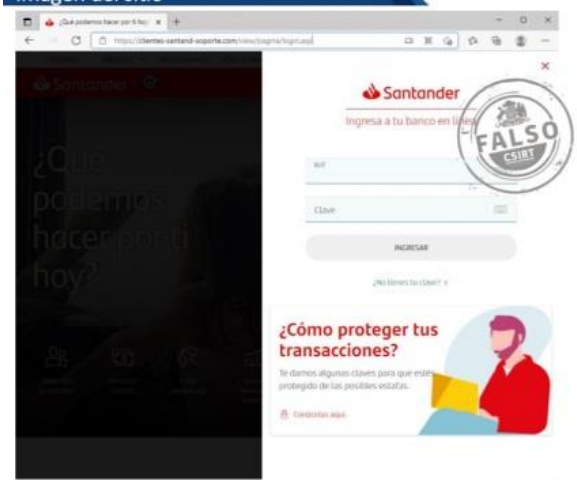
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

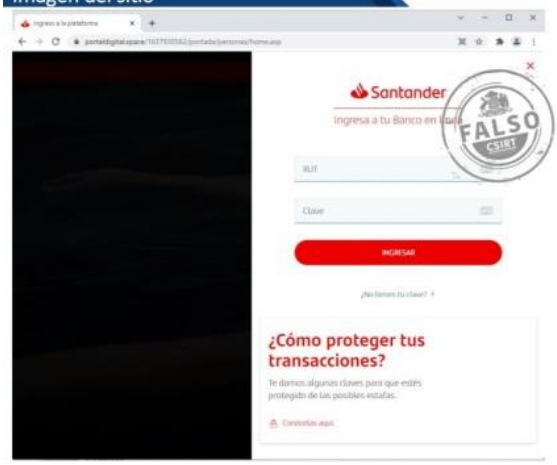
Sitios fraudulentos

Imagen del sitio



CSIRT informa suplantación de sitio web del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01023-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Noviembre de 2021
Última revisión	26 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://clientes-santand-soporte[.]com/view/pagina/login.asp	
IP	
[144.217.215.210]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01024-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01023-01.pdf	

Imagen del sitio



CSIRT advierte página fraudulenta del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01024-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Noviembre de 2021
Última revisión	26 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://portaldigital[.]space/1637930562/portada/personas/home.asp	
IP	
[51.255.26.63]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01024-01-2/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01024-01.pdf	

Imagen del sitio

CSIRT advierte sitio web que suplanta la tienda Casaldeas	
Alerta de seguridad cibernética	8FFR21-01025-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2021
Última revisión	30 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.cliosale[.]online/	
IP	
[167.160.17.166]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01025-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01025-01.pdf	

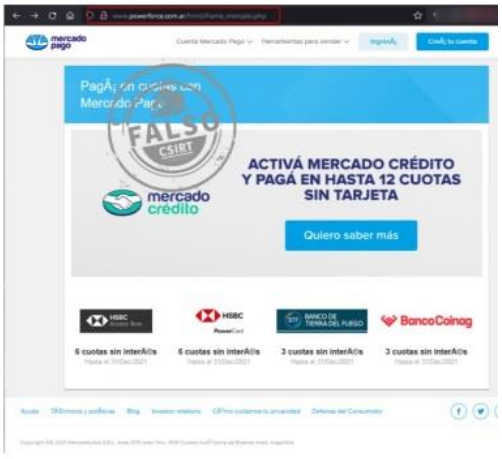
Imagen del sitio

CSIRT informa página falsa de la tienda Rosen	
Alerta de seguridad cibernética	8FFR21-01026-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2021
Última revisión	30 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.camasshopcl[.]shop/	
IP	
[5.255.62.142]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01026-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01026-01.pdf	

Imagen del sitio

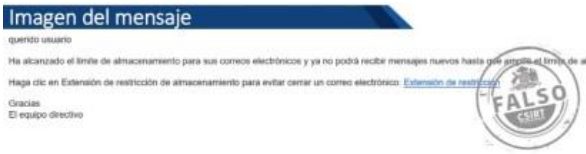
CSIRT advierte suplantación del sitio web del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01027-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de diciembre de 2021
Última revisión	01 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
http://santanderfuc[.]com/	
IP	
[162.241.216.188]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01027-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01027-01.pdf	

Imagen del sitio



CSIRT informa suplantación de sitio web de Mercado Pago	
Alerta de seguridad cibernética	8FFR21-01028-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
hXXp://www.powerforce.com[.]ar/html/iframe_mercado.php	
IP	
[190.210.9.23]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01028-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01028-01.pdf	

Phishing



CSIRT advierte phishing con supuesto límite de almacenamiento de correo electrónico	
Alerta de seguridad cibernética	8FPH21-00447-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://webclient.moreapp[.]com/#/form/61a8db13a81fa95369a1b08c	
IP	
[151.101.65.195]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00447-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00447-01.pdf	

CSIRT advierte phishing con supuesta actividad sospechosa del Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00448-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 de diciembre de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3EcCWWz?l=www.bancoripley.cl	
https://infektionsschutz7r[.]de/wp-includes/Requests/enviar.php?l=469125219	
URL sitio falso	
http://www-bancoripleycl[.]karav.org/	
IP	
[185.179.24.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00448-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00448-01.pdf	

Imagen del mensaje

CSIRT informa phishing vía WhatsApp con falsa promoción del supermercado Jumbo	
Alerta de seguridad cibernética	8FPH21-00449-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 de diciembre de 2021
Indicadores de compromiso	
URL redirección	
http://crowdeddiminish[.]website/jumbo/tb.php?_t=16384573351638457519215	
URL sitio falso	
https://ekpved[.]tw/nsM1Dvla/jumbo/?_t=1638474116820#1638474123738	
URL sitio propaganda	
https://s1.l-o-a-d-i-n-g[.]biz/?p3=70371961580782882 47#	
https://s.prizeoffer[.]net/win?round=1&tid=5t31p2hzr5qjbfkh8ca8sgwgo,15426683	
https://download-step1[.]com/download.html?an=vi&cid=c63b0qde8uobgwj64	
IP	
[104.21.79.85]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00449-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00449-01.pdf	

Malware

CSIRT comparte IoC de campaña de phishing con malware descubierta por la PDI, para su bloqueo	
Alerta de seguridad cibernética	2CMV21-00252-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2021
Última revisión	29 de Noviembre de 2021

Indicadores de compromiso

SHA256

5afda8caa4b0965e6e98b66b677f0d31f0b6e863da591a98fc3991b62a26d9fb
b0562deb87049cf41c53484bc5705cffb6e5798d29c804fc25ef1fc79dccb680
37ec1209daa15ba2bb2a9d9c372960703125e0b0acfa0736cb2ae10edfad7d62
59d14a53849a19d0dd5ccaf63a85955adbd313c9ec7d92422c0fcdda357b8ce0
1acebc9946af2303aae313154909c31ce6b01c7d9e78392f414e0088cbae4ac9

IoC URL incluidos los archivos

https://klevvrtech[.]com/zxywJAC24KJ/ji.html
https://srkcampus[.]org/OYcMRJbL/ji.html
https://stebet[.]co.id/fbmKk6n48G/ji.htm
https://headlineproductions[.]ro/rOJX6ai7AkZE/op.html
https://jrcapital[.]uk/eft8gfFqw/op.html
https://lc-bilingua[.]com/8wp9k9RPDzn/op.html

IoC URL similitud

acelle.rey[.]agency/corruptiaperiam/explicaboaut-5364880
acelle.rey[.]agency/corruptiaperiam/magnamsint-5523695
acelle.rey[.]agency/corruptiaperiam/minusqui-5521155
acelle.rey[.]agency/corruptiaperiam/namiure-5429433
acelle.rey[.]agency/corruptiaperiam/quidemea-5422513
acelle.rey[.]agency/corruptiaperiam/quiin-5442646
andyhermawan[.]net/doloresearum/eaqueaut-6475420
dev.plussizenation[.]com/eumin/etquia-5364880
dev.plussizenation[.]com/eumin/insed-5422513
dev.plussizenation[.]com/eumin/maioresaperiam-5508573
dev.plussizenation[.]com/eumin/natussapiente-5365031
dev.plussizenation[.]com/eumin/quiadeserunt-6461399
dev.plussizenation[.]com/eumin/repellatperspiciatis-6486302
dev.plussizenation[.]com/eumin/uthic-5523695
emailverify.rey[.]agency/exercitationemaccusantium/corporisquo-5442646
emailverify.rey[.]agency/exercitationemaccusantium/quinecessitatibus-5521155
erp.rey[.]agency/repellatreprehenderit/aliasaut-6473321
erp.rey[.]agency/repellatreprehenderit/delenitiatque-6493436
erp.rey[.]agency/repellatreprehenderit/iureducimus-6470868
heat.rey[.]agency/temporeconsequuntur/iureid-5516255
monsolde[.]ch/modiquae/debitismolestias-5508573
monsolde[.]ch/modiquae/debitisvoluptatem-5365031

monsolde[.]ch/modiquae/fugaomnis-6486302 monsolde[.]ch/modiquae/veniamsed-5423829 monsolde[.]fr/magninulla/corporiset-5423829 monsolde[.]fr/magninulla/enimut-5429433 monsolde[.]fr/magninulla/quoderror-6461399 nengmita.siganam[.]com/nobisvelit/estut-5516255 radone[.]ma/rerumdolores/dolorvoluptatum-6470868 radone[.]ma/rerumdolores/quasiin-6470690 radone[.]ma/rerumdolores/quieum-6493436 rock-roll.com[.]my/saepedoloribus/atrepudiandae-6475420 rock-roll.com[.]my/saepedoloribus/illoveritatis-6470690 rock-roll.com[.]my/saepedoloribus/magniomnis-6473321
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv21-00253-01/
https://www.csirt.gob.cl/media/2021/11/2CMV21-00253-01.pdf

CSIRT advierte campaña de phishing con malware con falso informe bancario	
Alerta de seguridad cibernética	2CMV21-00253-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2021
Última revisión	29 de Noviembre de 2021
Indicadores de compromiso	
SHA256	
EF15184F2B0E3D3E2D8D193E80EAB99219B1A21D6006EE3FF8EADF0A1BA4CA68 63DEDEE1EDB28A4E584B488066E2C31F1F07EA13BE7B4C5CFE0CAB625F6867D0	
IoC Red	
http://kbfvzoboss.bid/alien/fre.php http://alphastand.trade/alien/fre.php http://alphastand.win/alien/fre.php http://secure01-redirect.net/fx/fre.php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00253-01/	
https://www.csirt.gob.cl/media/2021/11/2CMV21-00253-01.pdf	

CSIRT informa campaña de malware con falsa orden de compra	
Alerta de seguridad cibernética	2CMV21-00254-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2021
Última revisión	29 de Noviembre de 2021
Indicadores de compromiso	
SHA256	
aefbd29fa01b6796341be145648ff5d0c776752cdf526865a88e70e20ae32bc2	
IoC Red	
www.yukotopia[.]com/dy26	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00254-01/	
https://www.csirt.gob.cl/media/2021/11/2CMV21-00254-01.pdf	

Vulnerabilidades

CSIRT advierte vulnerabilidad en Trend Micro Security	
Alerta de seguridad cibernética	9VSA21-00525-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2021
Última revisión	30 de Noviembre de 2021
CVE	
CVE-2021-43772	
Fabricante	
Trend Micro	
Productos afectados	
Trend Micro Security (consumer): 15, 16, 17, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00525-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00525-01.pdf	

CSIRT alerta de vulnerabilidades en varias multifuncionales HP	
Alerta de seguridad cibernética	9VSA21-00526-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2021
Última revisión	30 de Noviembre de 2021
CVE	
CVE-2021-39237 CVE-2021-39238	
Fabricante	
HP	
Productos afectados	
Ciertas multifuncionales HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide y HP PageWide Managed. Lista completa en: https://support.hp.com/us-en/document/ish_5000383-5000409-16.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00526-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00526-01.pdf	

CSIRT alerta de vulnerabilidad en popular plugin de WordPress	
Alerta de seguridad cibernética	9VSA21-00527-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 de diciembre de 2021
CVE	
CVE-2021-42367	
Fabricante	
Wordpress	
Productos afectados	
Variation Swatches for WooCommerce, versiones anteriores a la 2.1.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00527-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00527-01.pdf	

Actualidad

Ciberconsejos para comprar con seguridad este Black Friday

Esta noche comienza un nuevo evento de ofertas del comercio nacional, en el molde de las rebajas posteriores al Día de Acción de Gracias en Estados Unidos. Y por primera vez, es la Cámara de Comercio de Santiago quien organiza su propio Black Friday, con más de 500 tiendas online y 933 locales físicos adheridos.

Puedes ver los ciberconsejos en el siguiente enlace, que incluye también un PDF fácil de descargar, compartir e imprimir: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-black-friday-2021/

Ciberconsejos para evitar caer en estafas esta Navidad

Muchos ya comenzamos a planificar nuestras compras navideñas, ya sea de forma presencial u online. Y si prefieres los canales digitales, debes saber que los ciberdelincuentes utilizan distintas técnicas para robar tus claves o tu dinero.

Por eso, el CSIRT de Gobierno, junto con Entel y la Cámara Nacional de Comercio, preparamos estos ciberconsejos para comprar más seguro en estas fechas. Puedes compartir con tu familia y amigos las imágenes en esta publicación o también el resumen descargable en PDF, disponible aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-navidad-2021/

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.

- Juan Pablo Escobar Carrasco
- Victor Cofré