Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

24-12-2021 | Año 3 | N°129

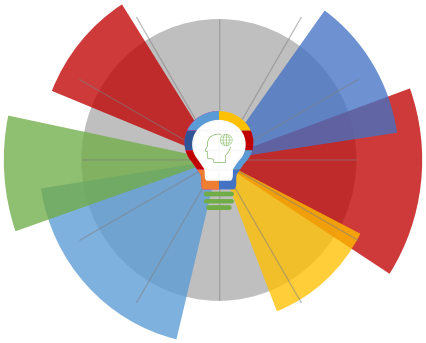
Boletín de Seguridad Cibernética

Semana del 17 al 23 de diciembre de 2021

La semana en cifras

Hash
3
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
6
URL
Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches
8
para vulnerabilidades
Las mitigaciones son útiles en productos de Apache, VMware, SolarWinds y SonicWall.

IP
4
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

Malware

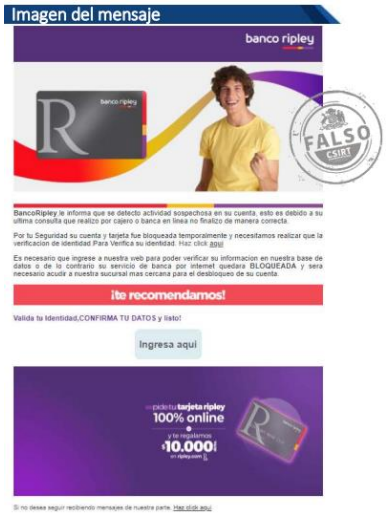
CSIRT advierte phishing con malware que proviene supuestamente de la TGR	
Alerta de seguridad cibernética	2CMV21-00264-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2021
Última revisión	23 de diciembre de 2021
Indicadores de compromiso	
SHA256	
8A4EED8C0743024BD75892723167CB79C709EBA11398725ED80FCE4004D240628A17EF86BB6E20E5F814402EC29418A9CA40D02529C5099663206DFE2795B9889a22ea7afb147c33a49ad8b521d1ee847db3710afc3ffe929a01db98026381d3	
IoC URL	
http://viv[.]az/chat/domino/stone/mail/?cid//id/AQQkADAwATYwMAItZjIyAGUtZGU5My0wMAItMDAKABAAoMPyI% [54.193.3.31]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00264-01/	
https://www.csirt.gob.cl/media/2021/12/2CMV21-00264-01.pdf	

Sitios fraudulentos

CSIRT advierte sitio web falso de Correos Chile	
Alerta de seguridad cibernética	8FFR20-01039-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2021
Última revisión	23 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
hXXps://futureexpertsgeophysics[.]com/.well-known/cl/9d543b71be613c9694eb3f6d3779b12a/	
IP	
[104.21.68.160]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-01039-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR20-01039-01.pdf	

Phishing

CSIRT alerta phishing para activar supuestamente el bono IFE Universal	
Alerta de seguridad cibernética	8FPH20-00454-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2021
Última revisión	22 de Diciembre de 2021
Indicadores de compromiso	
URL redirección	
hxxps://jeandescardtshtpmmh[.]com/LIFELIFEISGOODOOO	
hxxps://jeandescardtshtpmmh[.]com/LIFELIFEISGOODOOO/1ae67da1107e057f084290ebc9b5c726/	
URL sitio falso	
hXXps://bancoestado-personas[.]gq/run?&rpsnv=edc10c00d8e6e26af72eb3d0aa3f86c48d54cdc1	
IP	
[204.12.234.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00454-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH20-00454-01.pdf	



CSIRT alerta de phishing de supuesta cuenta bloqueada	
Alerta de seguridad cibernética	8FPH20-00455-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2021
Última revisión	23 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
http://web-bancoripley-cl.karav[.]org/1640267115/login	
IP	
[204.12.234.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00455-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH20-00455-01.pdf	

Vulnerabilidades

CSIRT comparte nueva vulnerabilidad y mitigaciones para Apache Log4j 2	
Alerta de seguridad cibernética	9VSA21-00535-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de diciembre de 2021
Última revisión	18 de diciembre de 2021
CVE	
CVE-2021-45105	
Fabricante	
Apache	
Productos afectados	
Apache Log4j 2.0-beta9 a 2.16.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00535-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00535-01.pdf	

CSIRT advierte vulnerabilidades en VMware One Access	
Alerta de seguridad cibernética	9VSA21-00536-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2021
Última revisión	20 de diciembre de 2021
CVE	
CVE-2021-22056 CVE-2021-22057	
Fabricante	
VMware	
Productos afectados	
VMware Workspace One: 20.10.0.0, 20.10.0.1, 21.08.0.0, 21.08.0.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00536-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00536-01.pdf	

CSIRT advierte vulnerabilidades de SolarWinds Orion	
Alerta de seguridad cibernética	9VSA21-00537-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2021
Última revisión	21 de diciembre de 2021
CVE	
CVE-2021-35248 CVE-2021-35244 CVE-2021-35234	
Fabricante	
SolarWinds	
Productos afectados	
Plataforma Orion: 2020.2.6, 2020.2.6 HF1, 2020.2.6 HF2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00537-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00537-01.pdf	

CSIRT comparte vulnerabilidades entregadas para SonicWall SMA 100	
Alerta de seguridad cibernética	9VSA21-00538-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2021
Última revisión	21 de diciembre de 2021
CVE	
CVE-2021-20049 CVE-2021-20050	
Fabricante	
SolarWinds	
Productos afectados	
SMA 100: 10.2.0.2-20sv, 10.2.0.3-24sv, 10.2.0.5-d-29sv, 10.2.0.6-31sv, 10.2.0.7-34sv, 10.2.0.8-37sv, 10.2.1.0-17sv, 10.2.1.1 -19sv, 10.2.1.2-24sv	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00538-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00538-01.pdf	

Actualidad

CSIRT de Gobierno lanza 1510, nuestro nuevo número para emergencias cibernéticas

Un número de teléfono corto y recordable, fácil de usar, gratuito y confidencial, para que cualquier persona pueda rápidamente alertar al CSIRT de Gobierno de emergencias e incidentes de ciberseguridad. Eso buscamos conseguir con el lanzamiento del 1510, número de discado rápido más recordable y fácil de dar a conocer que el único número de contacto antes disponible, +(562) 2486 3850, que de todas formas seguirá vigente. Estas imágenes también se encuentran disponibles en: https://www.csirt.gob.cl/recomendaciones/nuevo-numero-1510/.

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.24 17:03:50 -03'00'