Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

31-12-2021 | Año 3 | N°130

Boletín de Seguridad Cibernética

Semana del 24 al 31 de diciembre de 2021

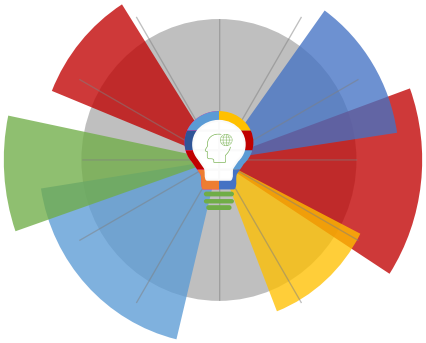
La semana en cifras

Hash

4

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

1

para vulnerabilidades

Las mitigaciones son útiles en Apache Logj4.

IP

9

Informadas

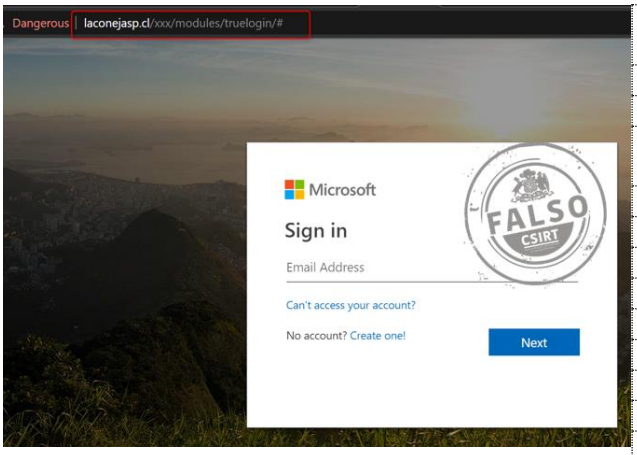
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

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

Sitios fraudulentos



CSIRT alerta ante sitio fraudulento que suplanta la plataforma de correos de Microsoft	
Alerta de seguridad cibernética	8FFR21-01040-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2021
Última revisión	28 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
hXXp://laconejasp[.]cl/xxx/modules/truelogin/	
IP	
[50.87.148.157]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01040-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01040-01.pdf	

CSIRT alerta de página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01041-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2021
Última revisión	30 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://bancosantander.cl.addzone[.]lk/1640779649/index.asp	
IP	
[85.187.128.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01041-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01041-01.pdf	

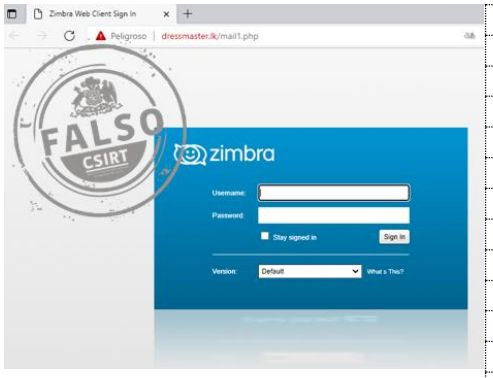
https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

CSIRT alerta de página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01042-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2021
Última revisión	30 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://soportecliente.cl.monzoon[.]lk/1640779655/index.asp	
IP	
[85.187.128.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01042-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01042-01.pdf	

CSIRT alerta de página falsa que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR21-01042-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2021
Última revisión	30 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://juandfar.github.io/Detflix/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01042-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01042-01.pdf	

Phishing

CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00456-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2021
Última revisión	28 de Diciembre de 2021
Indicadores de compromiso	
URL redirección	
hXXps://bit[.]ly/3yQftc9?l=www.bancoripley.cl	
URL sitio falso	
hXXps://www-bancoripley-cl.tractari-bistrita[.]ro/1640722093/login	
IP	
[185.181.101.3]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00456/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00456-01-1.pdf	



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00457-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2021
Última revisión	30 de Diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
www.dressmaster[.]lk	
IP	
[203.143.21.140]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00457-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00457-01.pdf	

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

Vulnerabilidades

CSIRT alerta de nueva vulnerabilidad en Apache Log4j2	
Alerta de seguridad cibernética	9VSA21-00539-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2021
Última revisión	29 de diciembre de 2021
CVE	
CVE-2021-44832	
Fabricante	
Apache	
Productos afectados	
Apache Log4j2 2.0-beta7 a 2.17.0, exceptuando 2.3.2 y 2.12.4.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00539-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00539-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno.

Recomendamos a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash	Tipo Malware	Documento web
883d702af603ae021218da994040382660c48ecd76bac4be1a8e670881b17082	MSIL/Kryptik	2CMV21-0265-01
71a0e72a83e3a8df998aedc83fbbbcdf261000b34f37cf10fa9f432a7cc4b70f	W32/Generic	2CMV21-0265-01
a02968737104558993a408e3629fa7d7907065998d2c9749c9ce829e549a0670	MSIL/Zilla	2CMV21-0265-01
1f15e558398fde6bac4830d5c4558ceecfc16a93702d30ce99e2ec9f6441c90d	FSA/RISK_HIGH	2CMV21-0265-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso. Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	ASN	Documento web
2.56.59.69	AS-SERVERION	AS 399471	2CMV21-00265-01
2.58.149.105	AS-SERVERION	AS 399471	2CMV21-00265-01
2.56.56.64	AS-SERVERION	AS 399471	2CMV21-00265-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

Nombres de archivos con malware	Documento web
SHIPPING ADVICE 4081791001.zip	2CMV21-00265-01
NEW ORDER CF211-24400.r00	2CMV21-00265-01
Product Inquiry Catalogue.gz	2CMV21-00265-01

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

Actualidad

¿De qué se tratan las vulnerabilidades en Apache Log4j 2 y qué debemos hacer al respecto?

El presente texto también se encuentra disponible en: https://www.csirt.gob.cl/noticias/resumen-apache-log4j-2/.

¿Qué es Log4j 2?

Log4j 2 es una biblioteca de elementos usada por los desarrolladores de software para mantener un registro de actividades o logging en diversas aplicaciones. Es muy popular, por lo que se le puede encontrar en todo tipo de software de un gran número de proveedores.

Algunos ejemplos de programas que usan Log4j2 son algunos tan populares como iCloud, Minecraft y la plataforma de juegos online Steam, e incluso cosas en las que probablemente no pensaríamos, como cargadores de autos eléctricos.

¿Por qué está en las noticias?

El 10 de diciembre el CSIRT de Gobierno compartió con la comunidad la existencia de una vulnerabilidad grave en Log4j 2, apodada Log4Shell[1].

Para esta vulnerabilidad grave ya existen hoy parches (actualizaciones que corrigen las vulnerabilidades), siendo el más reciente la versión 17.1[2] de Log4j, que además resuelve otras vulnerabilidades menos importantes descubiertas en los últimos días.

¿Qué debemos hacer?

Los responsables de ciberseguridad de toda organización deben identificar los programas que usan Log4j y actualizarlos cuanto antes, según las instrucciones del proveedor que corresponda. Por eso, el CSIRT también publicó una lista de enlaces a los sitios donde los principales proveedores de software informan de cuáles de sus productos usan Log4j[3].

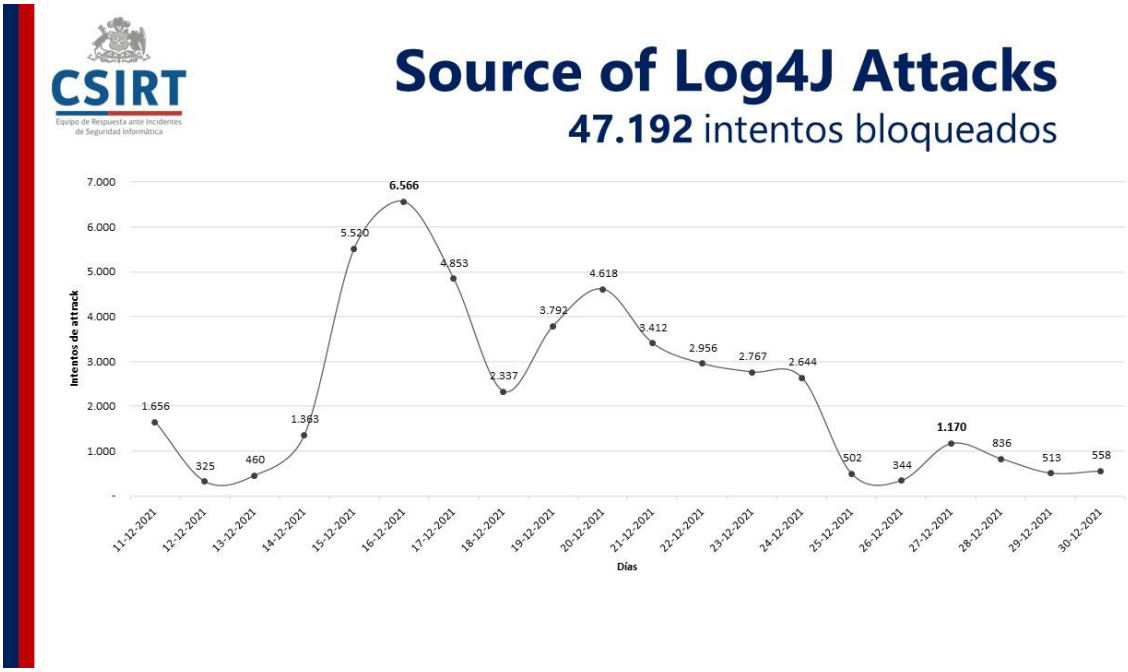
Los usuarios no deben asustarse, no hay nada en particular que deban hacer respecto de Logj4, salvo estar atentos a que los productos afectados sean efectivamente parchados. En este sentido

[1] https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00531-01/
[2] https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00539-01/
[3] https://www.csirt.gob.cl/noticias/alerta-apache-log4j-2/

solo debe seguir las mismas precauciones recomendadas siempre, como mantener sus aparatos y programas actualizados, y hacer estas actualizaciones desde los sitios y tiendas oficiales de sus dispositivos. Asimismo, es un buen momento para recordar que deben tener contraseñas seguras (consejos aquí) y activar el doble factor de autenticación en sus aparatos y cuentas virtuales.

Pese a lo extendido del uso de Apache Log4j 2, y la enorme cantidad de ataques registrados que explotan sus vulnerabilidades, no se ha conocido de víctimas prominentes al día de hoy, siendo probablemente la de mayor notoriedad el Ministerio de Defensa de Bélgica[4], entidad que reconoció haber sufrido un ataque que explota Logj4 pero sin dar más detalles. También se supo de una corredora vietnamita de criptomonedas que sufrió un ransomware (secuestro de archivos digitales) por US$ 5 millones gracias a la explotación de Log4Shell.

Esta es la evolución de los intentos de ataques relacionados con Log4j a la Red de Conectividad del Estado que han sido detectados al día por el CSIRT de Gobierno durante diciembre. Tras un peak de 6.566 a mediados de mes, se aprecia una tendencia a la baja.



[4] https://www.zdnet.com/article/belgian-defense-ministry-confirms-cyberattack-through-log4j-exploitation/

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.

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

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.

- Maldito Informático
- Felipe Pizarro Astudillo
- Vianka Valentina Vivanco Varela
- Hanz Sandoval
- Roberto Andrés Barrueto Guarda
- Víctor Andrés Cartagena Farías
- Víctor Cofré
- Mauricio Guerra
- Luis
- David Jacob Segura Zúñiga
- Adrián Muñoz Montenegro
- Cristóbal Herrera
- Maximiliano Molina