Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

07-01-2022 | Año 4 | N°131

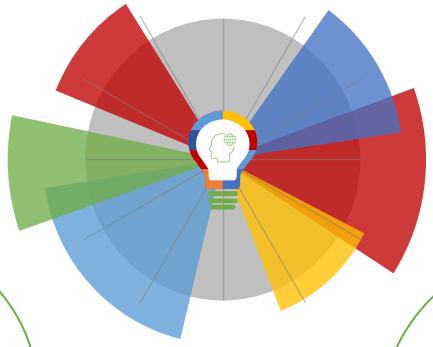
Boletín de Seguridad Cibernética

Semana del 31 de diciembre de 2021 al 06 de enero de 2022

La semana en cifras

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

Se advirtieron
7
URL
Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches
29
para vulnerabilidades
Las mitigaciones son útiles en productos Google, Nessus, Apache y VMware

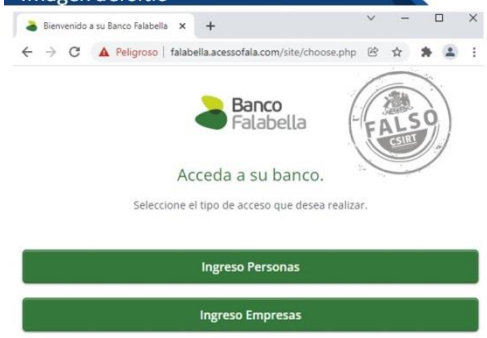
IP
5
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

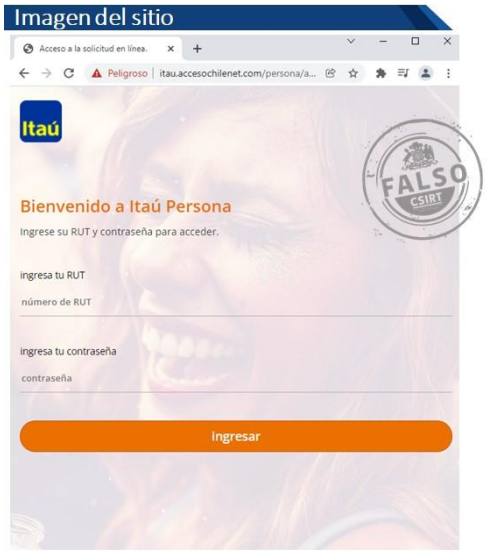
Imagen del sitio



CSIRT advierte sitio web falso del Banco Falabella	
Alerta de seguridad cibernética	8FFR21-01044-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de enero de 2022
Última revisión	6 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://falabella.acessofala[.]com/site/choose.php	
IP	
[52.188.63.37]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01044-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01044-01.pdf	

Imagen del sitio

CSIRT informa se suplantación de sitio web del Banco de Chile	
Alerta de seguridad cibernética	8FFR21-01045-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de enero de 2022
Última revisión	6 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
http://165.232.187[.]8/1641480100/bcochile-web/persona/login/index.html/login	
IP	
[165.232.187.8]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01045-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01045-01.pdf	



CSIRT advierte sitio web falso del Banco Itaú	
Alerta de seguridad cibernética	8FFR21-01046-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de enero de 2022
Última revisión	6 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://itau.accesochilenet[.]com/choose.php	
IP	
[52.188.63.37]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01046-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01046-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00458-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2021
Última revisión	31 de diciembre de 2021
Indicadores de compromiso	
URL redirección	
http://stz-fmba.ru/wp-includes/certificates/enviar[.]php?l=761930910	
https://sspmprimaryschool[.]com/activacion/cuenta-rpec/	
URL sitio falso	
https://www-bancoripley-cl.refinance-homeloan[.]com/1640956417/login	
IP	
[170.239.84.62]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00458-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH21-00458-01.pdf	

Imagen del mensaje


CSIRT advierte phishing con supuesto paquete que proviene de Correos de Chile	
Alerta de seguridad cibernética	8FPH21-00459-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://restaurant-newport[.]jp/wp-includes/ID4/ID3/	
IP	
[170.239.84.62]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00459-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00459-01.pdf	

Vulnerabilidades

CSIRT alerta de nuevas vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00540-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2022
Última revisión	5 de enero de 2022
CVE	
CVE-2022-0109 - CVE-2022-0120 - CVE-2022-0118 CVE-2022-0116 - CVE-2022-0115 - CVE-2022-0114 CVE-2022-0113 - CVE-2022-0112 - CVE-2022-0111 CVE-2022-0110 - CVE-2022-0108 - CVE-2022-0096 CVE-2022-0107 - CVE-2022-0106 - CVE-2022-0105 CVE-2022-0104 - CVE-2022-0103 - CVE-2022-0102 CVE-2022-0101 - CVE-2022-0100 - CVE-2022-0099 CVE-2022-0098 - CVE-2022-0097 - CVE-2022-0117	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones 70.0.3538.67 a 96.0.4664.110	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00540-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00540-01.pdf	

CSIRT comparte vulnerabilidades del servidor Apache HTTP Server	
Alerta de seguridad cibernética	9VSA22-00541-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
CVE	
CVE-2021-44224 CVE-2021-44790	
Fabricante	
Apache	
Productos afectados	
Tenable.sc: 5.14.0, 5.14.1, 5.15.0, 5.16.0, 5.17.0, 5.18.0, 5.19.0, 5.19.1, Parche 202001.2, Parche 202110.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00541-01/	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00541-01/	

CSIRT advierte vulnerabilidad en la herramienta Nessus	
Alerta de seguridad cibernética	9VSA22-00542-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
CVE	
CVE-2021-3711 CVE-2021-3712	
Fabricante	
Nessus	
Productos afectados	
Monitor de red Nessus: 5.0, 5.1, 5.2, 5.3, 5.4, 5.4.1, 5.5.0, 5.5.1, 5.6.0, 5.6.1, 5.7.0, 5.7.1, 5.8.0, 5.8.1, 5.9.0, 5.9.1, 5.10.0, 5.10.1, 5.11.0, 5.11.1, 5.12.0, 5.12.1, 5.13.0, 5.13.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00542-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA21-00542-01.pdf	

CSIRT informa vulnerabilidades de VMware	
Alerta de seguridad cibernética	9VSA21-00543-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
CVE	
CVE-2021-22045	
Fabricante	
VMware	
Productos afectados	
VMware ESXi VMware Estación de trabajo VMware Fusion Fundación VMware Cloud	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00534-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00534-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
CSIRT recomienda 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	N° Documento
281f2b06c0f48ac5f8efdc88616c2c35a4a52e17393374912aefc116e67c409e	W32/Injector	2CMV21-00266-01
d3bd6b3af36d9a5f4c3203b90c08be8163c94aa95ded25ba1e41a82af39ecdfa	MSIL/GenKryptik	2CMV21-00266-01
d512daa0ae47e6e6dc5c3521d7797f61eac5c9fc202868f04fc078c06c912828	MSIL/GenKryptik	2CMV21-00266-01

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
Quotation.lzh	2CMV21-00266-01
D00501 DIB Bur Dubai New Branch.uue	2CMV21-00266-01
SHIPPING ADVICE 4084301002.zip	2CMV21-00266-01

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

Actualidad

Ciberconsejos conexiones a VPN

Una VPN es una red privada virtual (Virtual Private Network por sus siglas en inglés) que permite conectar de forma segura uno o más dispositivos a internet. Puede ser utilizada tanto por una persona natural como una organización y tiene múltiples beneficios, como por ejemplo, proteger el tráfico de internet de la vista o interferencia de terceros, mantener la privacidad de las actividades en línea, entre otros.

El CSIRT de Gobierno explica con mayor detalle qué es una VPN, para qué se utiliza, cómo funciona y qué precauciones tener:

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.

- Patricio Godoy
- Camila Contreras
- Mariangel Fernández
- Víctor Cofré
- Cristián Acuña
- Rodrigo Hess
- Diego Neira
- Andrés Barrientos
- Felipe Pizarro
- Francisco Fernández