Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

20-08-2021 | Año 3 | N°111

Boletín de Seguridad Cibernética

Semana del 13 al 19 de agosto 2021

La semana en cifras

Hash

4

SHA

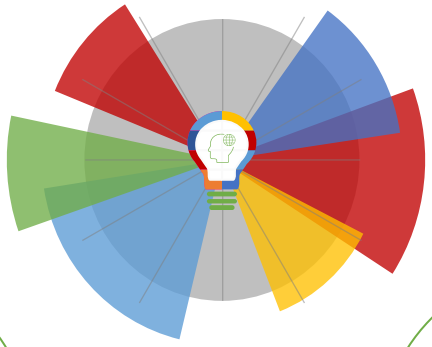
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

11

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

31

para vulnerabilidades

Las mitigaciones son útiles en productos de Adobe.

IP

7

Informadas

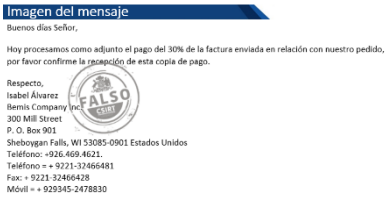
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Malware

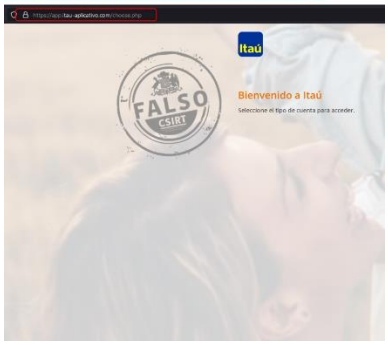
CSIRT alerta por campaña de phishing que suplanta a la Universidad de Chile	
Alerta de seguridad cibernética	2CMV21-00213-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
SHA256	
CF319EF6390C70A7EA468A4FB14F6AEEC8CB708C8621E9CCACF482E564C24715 00BD94F5DC7EB6E30CFE1DB9E7E7E6538C34768A6364D5B5D0F07209FB94F650	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00213-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00213-01.pdf	



CSIRT alerta de campaña de phishing que difunde malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00214-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
SHA256	
5D3245861842E4B8DE436C0423072FB3CEA02F991F611B52637E7634B2CF8F66 BE63B5F1E9EEB9CB151ECEB866B338626026F606A2656F3545651C94078821CC	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00214-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00214-01.pdf	

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de una página fraudulenta que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR21-01003-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://app.itau-aplicativo[.]com/choose.php	
IP	
[80.78.23.157]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01003-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01003-01.pdf	

Imagen del sitio

CSIRT alerta ante un sitio fraudulento que suplanta al BCI	
Alerta de seguridad cibernética	8FFR21-01004-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
http://139.99.233[.]26/1629464710/personas	
IP	
[139.99.233.26]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01004-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01004-01.pdf	

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01005-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://bacosantandle0r[.]xyz/1629465515/personas/index.asp	
IP	
[66.29.141.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01005-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01005-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante campaña de smishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH21-00425-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2021
Última revisión	12 de agosto de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/2VJHum3	
URL sitio falso	
https://chileatiende-sms[.]xyz/?sms=Santander https://suertedeldia[.]store/1628785543/personas/index.asp	
IP	
[68.65.123.97]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00425-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00425-01.pdf	

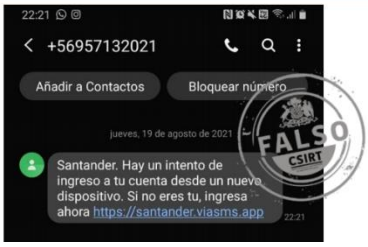
Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta a DHL	
Alerta de seguridad cibernética	8FPH21-00426-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://0ddbdb7c8f4432481.temporary[.]link//AE6ZEFZ4C6X615D5RDX58EFG8/VC5F6GF26SQ5F6DG65H65FH/cl-es/BOBMSX02X1/	
IP	
[199.250.216.7]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00426-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00426-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH21-00427-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://app.itau-cl.com/choose[.]php	
URL redirección	
https://www.atrilcom.com/wp-admin/js/	
IP	
[50.31.134.90]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00427-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00427-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de smishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH21-00428-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://app.itau-cl.com/choose[.]php	
URL redirección	
https://www.atrilcom.com/wp-admin/js/	
IP	
[50.31.134.90]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00428-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00428-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades graves en productos Adobe	
Alerta de seguridad cibernética	9VSA21-00482-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto de 2021

CVE

CVE-2021-36072	CVE-2021-36067	CVE-2021-36046	CVE-2021-36055
CVE-2021-36078	CVE-2021-36068	CVE-2021-36047	CVE-2021-36056
CVE-2021-36073	CVE-2021-36069	CVE-2021-36048	CVE-2021-36057
CVE-2021-36079	CVE-2021-36049	CVE-2021-36050	CVE-2021-36064
CVE-2021-36074	CVE-2021-36076	CVE-2021-36051	CVE-2021-36058
CVE-2021-36075	CVE-2021-36059	CVE-2021-36052	CVE-2021-36065
CVE-2021-36077	CVE-2021-36070	CVE-2021-36053	CVE-2021-36066
CVE-2021-36071	CVE-2021-36045	CVE-2021-36054	

Fabricante

Adobe

Productos afectados

Adobe Photoshop 2020 versión 21.2.10 y anteriores.
Adobe Photoshop 2021 versión 22.4.3 y anteriores.
Adobe Bridge CC versión 11.1 y anteriores.
Adobe Media Encoder: 15.0, 15.1, 15.2, 15.3, 15.4
Adobe XMP-Toolkit-SDK 2020.1

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00482-01
https://www.csirt.gob.cl/media/2021/08/9VSA21-00482-01.pdf

Actualidad

Este Mes del Niño, el CSIRT de Gobierno lanza cuentos para aprender a estar seguros en línea

En agosto, la revista CiberSucesos, que cada mes publica en su sitio web el CSIRT de Gobierno), presenta un especial con 9 cuentos sobre ciberseguridad para niños, ordenados por edad. Léala aquí: https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-cuentos-mes-del-nino/.

"Parte de nuestro rol como CSIRT de Gobierno es concientizar a la población sobre las formas seguras de interactuar con internet, incluyendo los juegos en línea y las redes sociales. Y eso debe incluir, lógicamente, a los chilenos más jóvenes. Por eso decidimos dedicar nuestra revista mensual a crear cuentos que entreguen conceptos de ciberseguridad de forma fácil y entretenida a niñas, niños y adolescentes", explica el Subsecretario del Interior, Juan Francisco Galli.

"Para escribir estos cuentos pedimos ayuda a nuestros propios funcionarios, quienes hicieron un espacio entre sus numerosas tareas protegiendo la ciberseguridad de nuestro país para idear pequeñas historias que hablan de temas que nuestros niños deben saber", explica Carlos Landeros, Director Nacional del CSIRT de Gobierno. "Les agradezco enormemente su compromiso, ya que además de sus labores de todos los días, en este servicio 24/7, asumieron la responsabilidad de salir de lo común y liberar sus lados creativos para hacer posible este proyecto. Fue un desafío para muchos de ellos, acostumbrados a sus labores como especialistas en ciberseguridad, periodistas y abogados", agrega.

Director del CSIRT de Gobierno realiza presentación sobre Ataques a la Cadena de Suministro en conferencia de Novared

Este jueves tuvo lugar la segunda jornada del Novared Security Workshop 2021, que contó con la presencia de autoridades y expertos en ciberseguridad, incluyendo al Director Nacional del CSIRT de Gobierno, Carlos Landeros, quien realizó la presentación «Riesgos contemporáneos a la cadena de suministros».

Este tipo de ataques afectan a un proveedor, de manera de infectar a varios de sus clientes, y así multiplicar su efectividad. Más aún, con esta técnica, los cibercriminales pueden burlar las defensas de las empresas clientes, que tienen a tener menos defensas en las conexiones provenientes de proveedores conocidos.

La noticia también la pueden leer en el siguiente enlace: https://www.csirt.gob.cl/noticias/director-del-csirt-de-gobierno-novared/.

Ciberguías | Cómo Protegernos Contra el Fraude a los Emails Corporativos (BEC)

Una de las formas de estafa digital más peligrosas para las empresas e instituciones son los que atacan directamente los emails corporativos (BEC, por «business email compromise»), especialmente el denominado Fraude del CEO.

Para saber cómo funcionan estas estafas, y cómo estar más seguros ante ellas, el CSIRT de Gobierno elaboró una completa ciberguía, que pueden encontrar aquí: https://www.csirt.gob.cl/recomendaciones/ciberguias-como-protegernos-contra-el-fraude-a-los-emails-corporativos-bec/.

El Comando de la Semana | No. 13 WPSCAN

En la sección El Comando de la Semana esta vez les traemos a WPSCAN, un escáner de vulnerabilidades de WordPress de caja negra que se puede usar para encontrar problemas de seguridad. La herramienta utiliza para ello una base de datos de 23,107 vulnerabilidades de WordPress.

El objetivo de estos comandos que compartimos semanalmente no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-13/.

El Control de la Semana | No. 7 Sistema de Gestión de Contraseñas

La Ficha de Control Normativo que compartimos en esta ocasión versa sobre los elementos principales a tener en consideración al momento de definir un Sistema de Gestión de Contraseñas. En el documento descargable a continuación, encontrarán restos consejos y otras consideraciones, parte de nuestra serie de fichas de control normativo.

Pueden descargar esta quinta ficha semanal, aquí: https://www.csirt.gob.cl/media/2021/08/El-Control-de-la-semana-N%C2%B06-A.9.1.2_v1.pdf.

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 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.

- María José Briceño Nikulin
- Andrés Peñailillo
- Jair Palma
- Álvaro Villalón
- Rodrigo Mundaca Villalobos
- Andrés Aldana F.
- Daniel Manosalvas
- Camilo Andrés Bastías Valenzuela
- Romel Rivas
- Eduardo Andrés Riveros Roca
- Alan Cisterna

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.08.20 13:18:41 -04'00'