Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

24-09-2021 | Año 3 | N°116

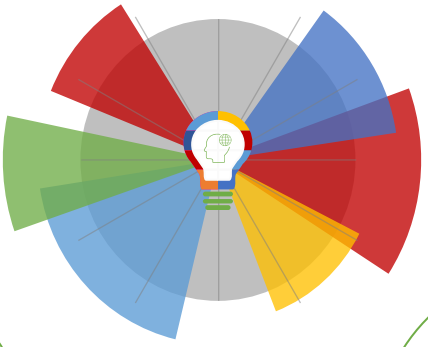
Boletín de Seguridad Cibernética

Semana del 16 al 23 de septiembre de 2021

La semana en cifras

Hash
13
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

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



Parches
33
para vulnerabilidades
Las mitigaciones son útiles en productos de VMware y Apple.

IP
15
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

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 de archivos maliciosos	Tipo de malware	Documento web
df0c6f655c170f3b33acfe6dd51c3492fae142c7e7d314f522062da54ace7eb0	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
4060abf7b75e024090fbd2cb937a60f50698334db53a04f3d82a96bbdd823719	MSIL/Kryptik.ACMW!tr	2CMV21-00222-01
9ebfbd3beb4239fd17b0fc24b9f1ea8d5b56f172e43044d9d4ddba8a4d360dfd	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
2c21dda7bfd0ec4aca1a77ecc65ac7e87996fd72e2f05ed2161b2ee26461008f	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
7da588f04fa53101d5383de2ddb7cf503c59adb6598e10be0d91ece4fdf6dd6d	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00222-01
3eb7d51b8bc7bca27400be167b265335d205e8936312d1b33c2c3dab04385d15	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
c3c71e328575ee408f70f8c88f00df195e7f7e40839b2736ee6baf1858eb9262	MSIL/Kryptik.ACMW!tr	2CMV21-00222-01
90a7307e6814ddd45dee083d9bb39ff07eb9caf9a7cbd2b9f82e34879d9cdb93	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
f71f3c99d8d1673f71b619e402e6c3c511d03b6d2d8aa64bc65015677d09458b	MSIL/Kryptik.ACMJ!tr	2CMV21-00222-01
860d9421928312c17111d020aaa3193597d1f557adda489cd67899a8274f799c	MSIL/Kryptik.ACMW!tr	2CMV21-00222-01
747d33cf088dc73aeb077ce2b91f161bcef7b0471a5f89aad364091893929f65	HTML/Phishing.AWP!tr	2CMV21-00222-01
acc8b2859dbd2adcab62bdc752c358d1ff4464b773ba6dd52ff26aa146eb527e	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01
2cd33b67cedb84528ce335e93eb78187cf37e0d69c66cb55f7ab3deda7050828	MSIL/Kryptik.ACNW!tr	2CMV21-00222-01

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.

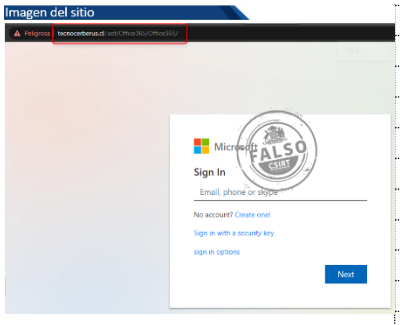
IP	Etiqueta de sistema autónomo	Documento web
157.245.103.184	DIGITALOCEAN-ASN	2CMV21-00222-01
103.153.77.192	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00222-01
103.89.88.75	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00222-01
137.184.134.82	DIGITALOCEAN-ASN	2CMV21-00222-01
138.68.30.3	DIGITALOCEAN-ASN	2CMV21-00222-01
178.128.31.232	DIGITALOCEAN-ASN	2CMV21-00222-01
185.222.57.134	RootLayer Web Services Ltd.	2CMV21-00222-01
185.222.57.150	RootLayer Web Services Ltd.	2CMV21-00222-01
185.222.57.153	RootLayer Web Services Ltd.	2CMV21-00222-01
185.222.58.140	RootLayer Web Services Ltd.	2CMV21-00222-01
45.137.22.115	RootLayer Web Services Ltd.	2CMV21-00222-01
46.231.127.25	RootLayer Web Services Ltd.	2CMV21-00222-01

Nombres de archivos con malware:

N°	Archivo Malware	
1	Payment Advice Copy.zip	2CMV21-00222-01
2	ORDER-20212209-02938273.doc	2CMV21-00222-01
3	New purchase order____pdf.html	2CMV21-00222-01
4	SHIPPING DOC (CI,COO,PL,BL).rar	2CMV21-00222-01
5	PO CB-15GL.docx	2CMV21-00222-01
6	New Order Specifications pdf.iso	2CMV21-00222-01
7	ATG order #55.doc	2CMV21-00222-01
8	message29803.pif	2CMV21-00222-01
9	AWB_1153703596.zip	2CMV21-00222-01
10	pqf0009876545678.zip	2CMV21-00222-01
11	Image001.img	2CMV21-00222-01
12	ginzunza@mbienes.cl/Purchase Order	2CMV21-00222-01
13	fondobecaslab Delivery_FORM 9/22/2021 5:06:15 a.m..htm	2CMV21-00222-01
14	p.muck Delivery_FORM 9/22/2021 4:47:29 a.m..htm	2CMV21-00222-01

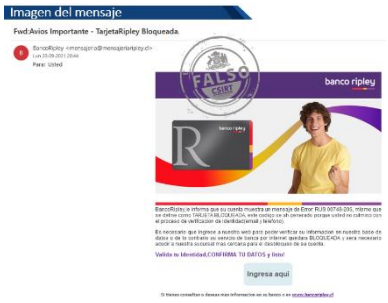
15	shipping documents.rar	2CMV21-00222-01
16	Quotation - Urgent.zip	2CMV21-00222-01
17	Company-catalog.zip	2CMV21-00222-01
18	Company-Profile.zip	2CMV21-00222-01
19	Quotation.jar	2CMV21-00222-01

Sitios fraudulentos



CSIRT alerta de sitio falso que suplanta al correo de Microsoft	
Alerta de seguridad cibernética	8FFR21-01012-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://tecnocerberus[.]cl/.xof/Office365/Office365/	
IP	
[200.73.113.171]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01012-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01012-01.pdf	

Phishing



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00435-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/39zIwF7?l=www.bancoripley.cl	
URL sitio falso	
http://www-bancoripleycl.eait.co[.]za/login	
IP	
[81.169.236.156]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00435-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00435-01.pdf	

CSIRT alerta de campaña de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00436-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/BChile-DigiPass https://lodicomputer.com/news/wp_logs[.]php	
URL sitio falso	
https://bchile-persona-cl.virtualwebmm[.]com/1632358198/persona/login	
IP	
[104.218.54.211]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00436-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00436-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades críticas en productos de VMware	
Alerta de seguridad cibernética	9VSA21-00495-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre de 2021

CVE

CVE-2021-21991	CVE-2021-22007	CVE-2021-22012	CVE-2021-22017
CVE-2021-21992	CVE-2021-22008	CVE-2021-22013	CVE-2021-22018
CVE-2021-21993	CVE-2021-22009	CVE-2021-22014	CVE-2021-22019
CVE-2021-22005	CVE-2021-22010	CVE-2021-22015	CVE-2021-22020
CVE-2021-22006	CVE-2021-22011	CVE-2021-22016	

Fabricante

VMware

Productos afectados

VMware vCenter Server
VMware Cloud Foundation

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00495-01
https://www.csirt.gob.cl/media/2021/09/9VSA21-00495-01.pdf

CSIRT alerta por vulnerabilidades en productos de Apple	
Alerta de seguridad cibernética	9VSA21-00496-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2021
Última revisión	23 de septiembre de 2021

CVE

N/A (Vuln. CWE-939)	CVE-2021-30835	CVE-2021-30846
CVE-2021-30837	CVE-2021-30847	CVE-2021-30849
CVE-2021-30841	CVE-2021-30857	CVE-2021-30851
CVE-2021-30842	CVE-2013-0340	CVE-2021-30810
CVE-2021-30843	CVE-2021-30854	

Fabricante

Apple

Productos afectados

Apple macOS 14.0 a 14.7
Apple tvOS 14.0 a 14.7
Apple iOS 14.0 a 14.8
Apple iPadOS 14.0 a 14.8

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00496-01
https://www.csirt.gob.cl/media/2021/09/9VSA21-00496-01.pdf

Actualidad

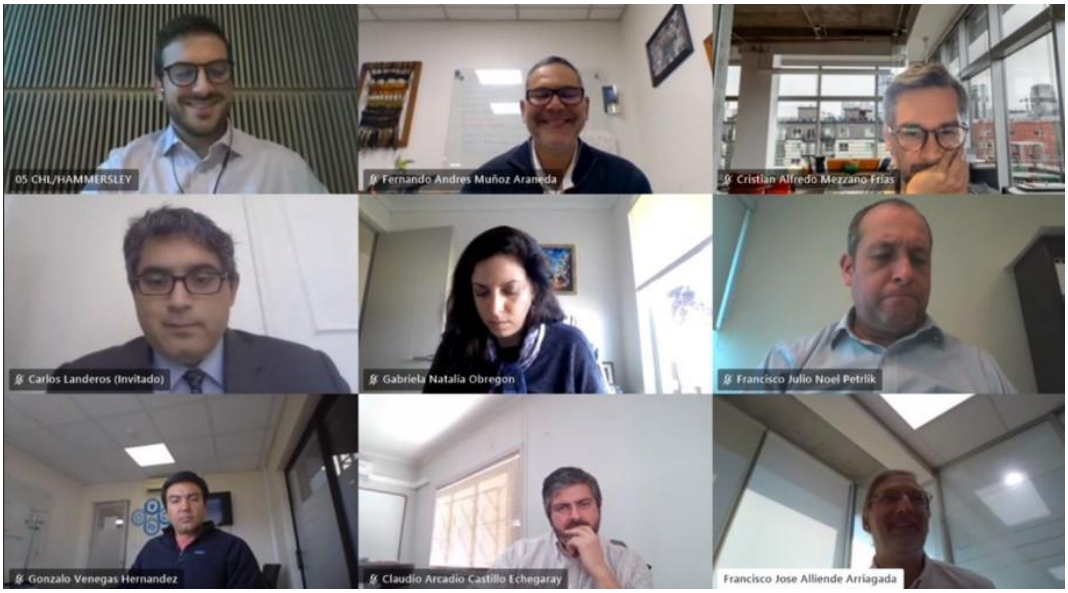
Última oportunidad para inscribirse en el Segundo Simposio de Ciberseguridad para Funcionarios Públicos, realizado por el CSIRT de Gobierno

Este martes 28 de septiembre comienza nuestro Segundo Simposio de Ciberseguridad para Funcionarios Públicos, por lo que quedan muy pocos días para ser parte y los volvemos a invitar a que se inscriban: https://simposio-ciberseguridad.csirt.gob.cl.

Las clases y talleres del simposio, realizadas todas por funcionarios del CSIRT de Gobierno tocarán una serie de temas, como el uso de herramientas *open source*, los conceptos clave que determinan la seguridad de las páginas web, los controles para mitigar las amenazas de ciberseguridad y los procedimientos necesarios para conseguir la revocación de nombres de dominio.

La inscripción debe verificarse con el correo institucional o corporativo. La agenda detallada y más información aquí:
https://www.csirt.gob.cl/noticias/comienzan-las-inscripciones-para-el-segundo-simposio-de-ciberseguridad-para-funcionarios-publicos-realizado-por-el-csirt-de-gobierno/.

La Ciberseguridad Industrial fue el foco de una productiva presentación realizada por el CSIRT de Gobierno ante gerencia del grupo Saesa



En el marco del trabajo de colaboración público-privada del CSIRT de Gobierno, nuestra institución realizó una presentación a miembros de la alta gerencia del Grupo Saesa, empresa que es parte de la asociación Empresas Eléctricas, la que a su vez mantiene un convenio con el CSIRT.

Comenzó el evento el director nacional del CSIRT de Gobierno, Carlos Landeros, quien realizó su presentación titulada «Ciberseguridad desde la primera línea», que trataba, entre otras cosas, sobre las diferencias de la ciberseguridad cuando se trata de procesos industriales, debido a la convergencia entre las tecnologías de la información (IT) y las tecnologías operacionales (OT).

El director nacional también detalló las implicancias del proyecto de Ley Marco de Ciberseguridad (que también crea la Agencia Nacional de Ciberseguridad). Siguió luego la presentación de Cristóbal Hammersley, asesor jurídico del CSIRT de Gobierno, quien habló del trabajo realizado por la institución para implementar normas sectoriales de ciberseguridad.

.

Más detalles de lo presentado: csirt.gob.cl/noticias/la-ciberseguridad-industrial-fue-el-foco-de-una-productiva-presentacion-realizada-por-el-csirt-de-gobierno-ante-gerencia-del-grupo-saesa/.

El Comando de la Semana | No. 18 DIRB

El protagonista de nuestro Comando de la Semana en esta ocasión a DIRB, escáner de contenido web. Busca objetos web existentes (y/u ocultos). Funciona lanzando un ataque basado en diccionario contra un servidor web y analizando la respuesta.

DIRB viene con un conjunto de listas de palabras de ataque preconfiguradas para un uso fácil, pero también puede usar listas personalizadas. Además, si bien DIRB se puede utilizar como un escáner CGI clásico, debemos recordar que es un escáner de contenido, no un escáner de vulnerabilidades. El objetivo principal de DIRB es ayudar en la auditoría profesional de aplicaciones web.

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-18/.

El Control de la Semana | No. 12 Registro de Eventos

Esta semana, nuestra Ficha de Control Normativo muestra cómo crear instrucciones, medidas y controles para un elemento esencial de la Política General de Seguridad de la Información en una organización: el Registro de Eventos.

Todo equipo y sistema bien diseñado contempla funciones de auditoría, trazas de error y mensajería sobre estatus del procesamiento y funcionamiento. Estos registros hablan de lo que está sucediendo en nuestros sistemas, sus problemas, y recopilan señales que nos pueden ayudar a diagnosticar un problema.

Por eso, en el documento descargable a continuación encontrarán los detalles más importantes a tener en consideración al momento de definir nuestros controles para el Registro de Eventos.
Pueden descargar esta nueva ficha semanal, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-12/.

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.

- Álvaro Ignacio Riquelme Oyarzo
- Fernando Flores Tobar
- Francisco Javier Gutiérrez
- Claudio Urquiza
- Gisselle Valeria Hernández Plaza
- Juan Correa
- César Soto Espinoza
- Daniela González
- Seung Hyun Baek
- Julio Marín Arriagada

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.24 15:51:08 -03'00'