Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

23-09-2022 | Año 4 | N°168

Boletín de Seguridad Cibernética

Semana del 15 al 22 de septiembre de 2022

La semana en cifras

Parches

1

para vulnerabilidades

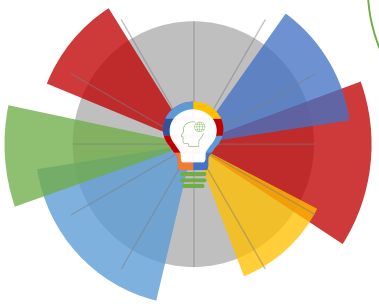
Las mitigaciones son útiles en productos de VMware.

IP

11

Informadas

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



Se advirtieron

20

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

9

Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

Contenido

Malware

CSIRT alerta de nueva campaña de phishing con malware que suplanta a entidad municipal	
Alerta de seguridad cibernética	2CMV22-00346-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de septiembre de 2022
Última revisión	21 de septiembre de 2022
Indicadores de compromiso	
Asunto	
(sin asunto)	
Correo de salida	
egis.lolol@gmail.com	
SHA256	
Doc 02321- Aviso de pago.xlsx SHA256: 187f085ad4f062f5ca8faf70d7b096fd7f274e5aef00808a56d0f557aaf90ee2 Document_iXRMjTBCuC_2.zip SHA256: 8d02bd62d1e1f6c1e71ab8c5133933ce58b908a6bf01130877320c2c2f9a7ac1 Document_iXRMjTBCuC.zip SHA256: 11c48b78a99bace6753b56701d4f17a39c300ad1fd3b511679907b290614a263 Document.pdf.rar SHA256: 2315c1385b4bedcc4f7fe0b08a383450c873ba81033e7ef347697c4032cd78a8 Document.pdf.scr SHA256: dc7ef7b92c427b3e04afe4cb73ce3b766c1e53b24d1cf68e96a3785840cfe0fb annotation.UnsupportedAppUsage.module10.exe SHA256: 140813a0a56d26c95c94addd1d44462cd93d51d5f66b9bd2ea00b94f9b8d8d52	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00346-01/	
https://www.csirt.gob.cl/edia/2022/09/2CMV22-00346-PH-01.pdf	

Imagen del mensaje

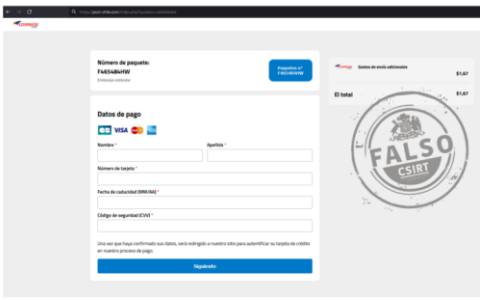
CSIRT alerta de nuevo phishing que suplanta a compañía mexicana	
Alerta de seguridad cibernética	2CMV22-00347-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2022
Última revisión	22 de septiembre de 2022
Indicadores de compromiso	
Asunto	
RE: ORDEN DE COMPRA 045190	
Correo de Salida	
facturas@lusen.com.mx	
SHA256	
Nombre: ORDEN DE COMPRA 045190.xlsx SHA256: f83628e8db4f7c65ed636e17a1ab69a2b0f14a7e1cf9afca77b682b6d51f8677	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00347-01/	
https://www.csirt.gob.cl/media/2022/09/2CMV22-00347-PH-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing en falsa repuesta a puesto laboral	
Alerta de seguridad cibernética	2CMV22-00348-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2022
Última revisión	14 de septiembre de 2022
Indicadores de compromiso	
Asunto	
Curriculum Vitae Rita	
Correo de Salida	
vipechi@gmail.com	
SHA256	
Nombre: Curr&#65533;culum Vitae Rita.zip SHA256: 95cec8fc25e5a9779e991f002c78a786c3dd9354acbb0820f90528e9ac39f043 Nombre: Currículum Vitae Rita.ex SHA256: 64cc998a2f7e9e180ef01e860eaf4fa6ec9cd397cf10a2798540f84b9af48095	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00348-01/	
https://www.csirt.gob.cl/media/2022/09/2CMV22-00348-PH-01.pdf	

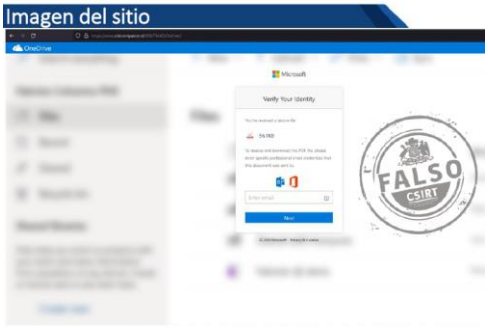
Sitios fraudulentos

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR22-01095-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://post-chile[.]com/index.php?success=validatedok	
IP	
[5.42.199.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01095-01/	
https://www.csirt.gob.cl/media/2022/08/8FFR22-01095-01.pdf	

Imagen del sitio



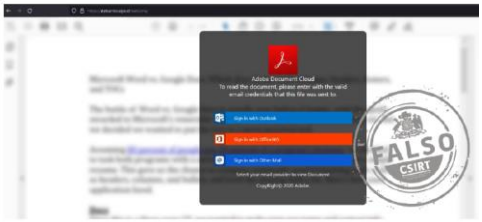
CSIRT alerta de sitio falso que suplanta a Microsoft One Drive	
Alerta de seguridad cibernética	8FFR22-01096-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.cristomipastor[.]cl/85875445/Odrivex/	
IP	
[186.64.119.240]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01096-01/	
https://www.csirt.gob.cl/media/2022/08/8FFR22-01096-01.pdf	

Imagen del sitio

CSIRT advierte de sitio fraudulento que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR22-01097-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022

Indicadores de compromiso
URL sitio falso
https://www.cristomipastor[.]cl/85875445/Odrivex/
IP
[186.64.118.110]
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/8ffr22-01097-01/
https://www.csirt.gob.cl/media/2022/09/8FFR22-01097-01.pdf

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a Adobe Cloud	
Alerta de seguridad cibernética	8FFR22-01098-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://delbarriovalpo[.]cl/welcome/	
IP	
[186.64.116.165]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01098-01/	
https://www.csirt.gob.cl/media/2022/09/8FFR22-01098-01.pdf	

Imagen del sitio

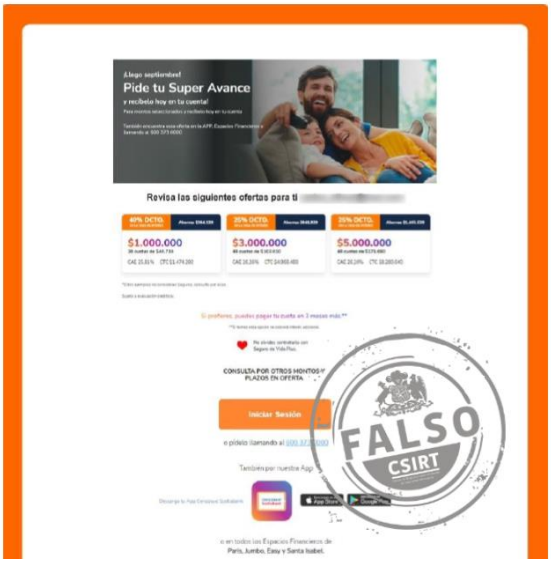
CSIRT alerta de sitio fraudulento que suplanta a Serfonac	
Alerta de seguridad cibernética	8FFR22-01099-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://brigadas.serfonac[.]cl/expressiveness.php	
IP	
[201.148.104.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01099-01/	
https://www.csirt.gob.cl/media/2022/09/8FFR22-01099-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de campaña de phishing con falso bono IFE Laboral pendiente	
Alerta de seguridad cibernética	8FPH22-00591-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de septiembre de 2022
Última revisión	15 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bit[.]ly/3S1YUCf http://165.22.241[.]40/de5a95d9eaae025e357d9b20e176fc55/9c95436bb7fe54aee4dcad2b3e0a5500/0973051cee2c4e1cf5RONS	
URL sitio falso	
https://banestado-en-linea[.]ml/linea?1254789653o36j7q3p6c5	
IP	
[204.11.58.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00591-01/	
https://www.csirt.gob.cl/media/2022/09/8FPH22-00591-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FPH22-00592-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de septiembre de 2022
Última revisión	15 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://cutt[.]ly/PCTSDlh https://cencohelados[.]top/ https://mitarjetacencosud-cl.loginscotiabank-cl[.]gq/	
URL sitio falso	
https://mitarjetacencosud-cl.loginscotiabank-cl[.]gq/1663267837/login/index.html	
IP	
[104.21.87.62]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00592-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00592.01.pdf	

Imagen del mensaje

CSIRT alerta de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00593-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands[.]com.np/Recuperalo_Aqui/cuenta-sqft/	
URL sitio falso	
https://view.premiumjp2020[.]com/1663678353/portada/personas/home[.]asp	
IP	
[186.64.118.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00593-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00593-01.pdf	

Imagen del mensaje

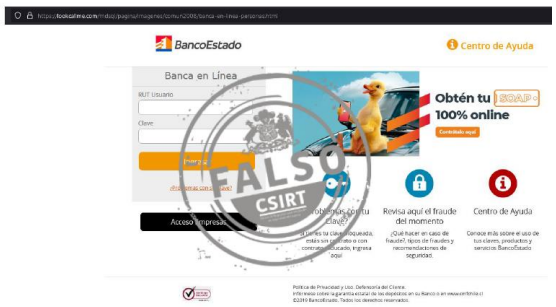
CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00594-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2022
Última revisión	22 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bit.ly/3xFaBqX?l=www.bancoripley.cl https://plrprofitskit.com/activacion/cuenta-ndou/ https://web.bancoripley.cl.avtoplam.ru/	
URL sitio falso	
https://web.bancoripley.cl.avtoplam.ru/1663788283/login	
IP	
[91.219.194.21]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00594-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00594-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco de

Chile	
Alerta de seguridad cibernética	8FPH22-00595-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2022
Última revisión	22 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://is.gd/7Y250s	
URL sitio falso	
https://wwvportalpersonas-soportebdchile.cl.scgfounders.com/1663855444/bcochile-web/persona/login/index.html/login	
IP	
[162.241.169.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00595-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00595-01.pdf	

Imagen del sitio



CSIRT alerta de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00596-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2022
Última revisión	22 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://depart.digitalnoticias.com.mx/activacion/cuenta-fizb/ https://lookcallme.com/mdsql/	
URL sitio falso	
https://lookcallme.com/mdsql/pagina/imagenes/comun2008/banca-en-linea-personas.htm	
IP	
[186.64.114.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00596-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00596-01.pdf	

Vulnerabilidades

CSIRT alerta de nueva vulnerabilidad en VMware Tools	
Alerta de seguridad cibernética	9VSA22-00703-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2022
Última revisión	20 de septiembre de 2022
CVE	
CVE-2022-31676	
Fabricantes	
VMware	
Productos afectados	
VMware Tools 2.x.y, 11.x.y y 10.x.y.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00703-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00703-01.pdf	

Actualidad

Exitosa tercera reunión de los Comités de Innovación en Ciberseguridad de la OEA, organizada junto al CSIRT de Gobierno

En la sede de Centro de Estudios de Postgrado y Educación Continua de la Universidad de Santiago (Usach), ubicada en Las Condes, se reunieron este miércoles los más importantes representantes de la ciberseguridad y el desarrollo tecnológico de Chile, convocados por la Organización de los Estados Americanos (OEA) con motivo de su tercera reunión de los Consejos de Innovación en Ciberseguridad (CIC), la primera realizada en persona en lugar de manera telemática.

La instancia contó, como ceremonia de apertura, con mensajes de las más altas autoridades, continuó con presentaciones de expertos en la materia y un panel participativo, y cerró con un taller de pensamiento creativo. Así, abrió la jornada Silvia Díaz, Ministra de Ciencia, Tecnología, Conocimiento e Innovación, seguida del Rector de la Usach, Rodrigo Vidal; Daniel Álvares, Coordinador Nacional de Ciberseguridad (Ministerio del Interior); Alison Treppel, Secretaria del Comité Interamericano contra el Terrorismo (CICTE) de la OEA –conectada telemáticamente desde Washington, D.C.- y Claudio Ortiz, Director Gerente de Cisco en Chile.

Asimismo, al evento asistieron la subsecretaria de Ciencia, Tecnología, Conocimiento e Innovación, Carolina Gainza; la jefa de División de Redes y Seguridad Informática del Ministerio del Interior, Ingrid Inda; el Senador Kenneth Pugh, la Diputada Helia Molina; el Gerente General de Cisco Chile, Claudio Ortiz y representantes de la Subsecretaría de Economía, el Ministerio de Educación, la Universidad de Chile, Inacap y Reuna, entre otras organizaciones.

Alerta de Seguridad Cibernética: Se reitera necesidad de parchar vulnerabilidades críticas en servidores de correo

El CSIRT de Gobierno quiere hacer un llamado a las instituciones públicas del Estado, a las entidades en convenio de colaboración y a los administradores de sistemas y público en general, para que tomen medidas de carácter preventivo para subsanar una vulnerabilidad en el servidor Exchange de Microsoft (CVE-2021-34473), y que revisen el estado de la seguridad en los servidores de correos basados en Zimbra vinculados a la vulnerabilidad CVE-2022-37042.

Detalles: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-actualizar-correo/

Alerta de Seguridad Cibernética: Explotación activa de vulnerabilidad en firewall Sophos

El CSIRT de Gobierno alerta a las instituciones públicas del Estado, a las entidades en convenio de colaboración y a los administradores de sistemas y público en general, ante la explotación activa de una vulnerabilidad (CVE-2022-1040) en el firewall de Sophos.

Detalles: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-sophos

Ciberdiccionario Volumen 17

Esta semana en una nueva edición del ciberdiccionario del CSIRT de Gobierno compartimos la definición de los siguientes términos: ataques de fuerza bruta, baiting, malvertising o adware y suplantación de identidad. Pueden ser descargados como imagen, aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-17

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 campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Antonio Alexis Vincent Cortés
- Roberto Plaza
- Sebastián Guillermo Leiva Valenzuela
- Andrés Jara González
- Gonzalo Iván Rivera Arismendi
- RiskIQ IRT
- Pablo Andrés Fabres Fabres
- María Paulina Matta Vattier
- Claudio González
- Roberto Jara Díaz