CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 204

semana del 26 de mayo al 1 de junio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

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

URL ADVERTIDAS

49 URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

14 Las mitigaciones son útiles en productos de Google (Chrome) y Barracuda.

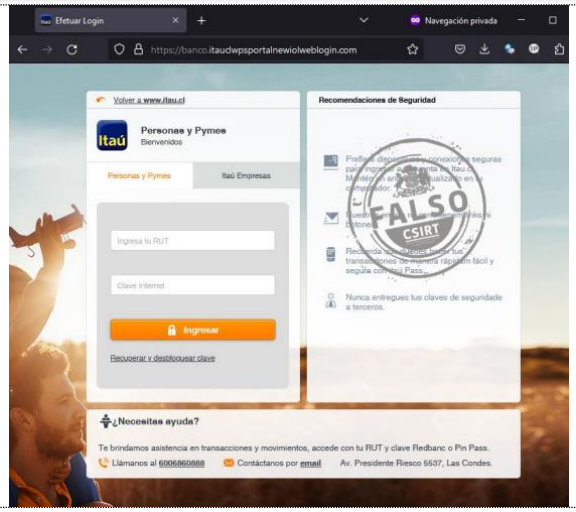
HASH REPORTADOS

14 asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

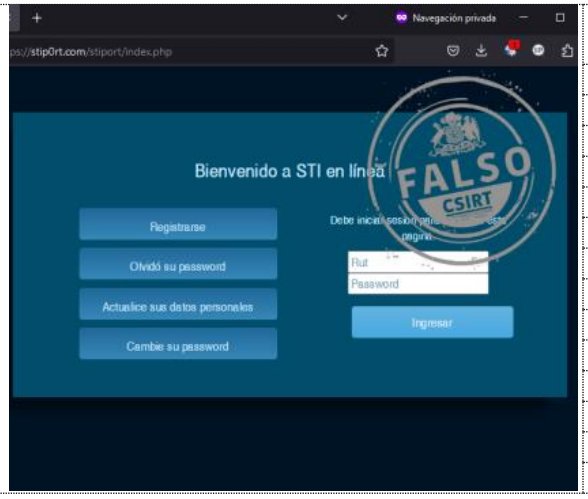
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

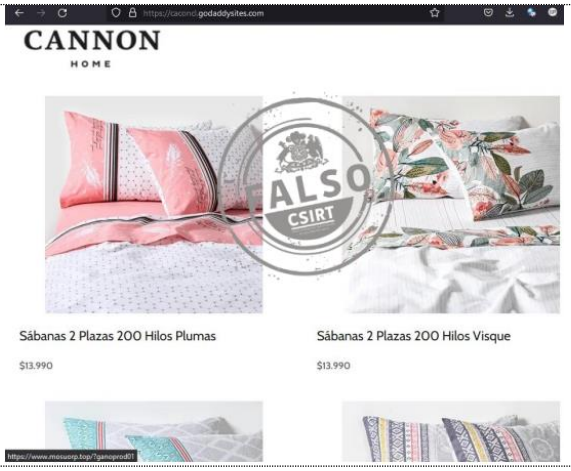


CSIRT alerta ante nuevo sitio fraudulento que suplanta a Banco Itaú	
Alerta de seguridad cibernética	8FFR23-01339-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://banco.itauclwpsportalnewiolweblogin[.]com/	
Dirección IP	
[20.226.87.125]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01339-01	

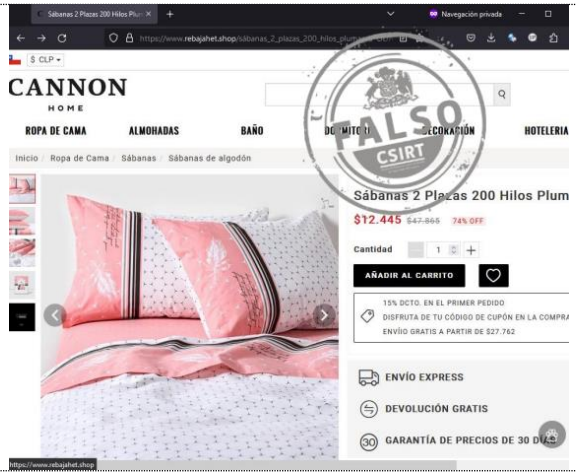
CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01340-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://web.bancoripley.cl.touchousindia[.]com/1685118958/login	
Dirección IP	
[162.222.225.160]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01340-01	



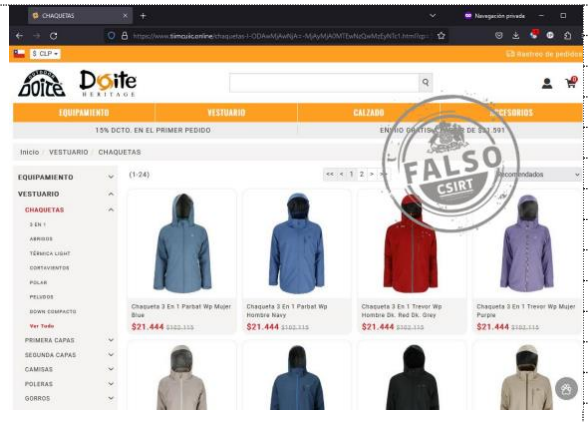
CSIRT alerta de sitio fraudulento que suplanta a STI San Antonio Terminal Internacional	
Alerta de seguridad cibernética	8FFR23-01341-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://stip0rt.com/	
Dirección IP	
[192.185.97.77]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01341-01	



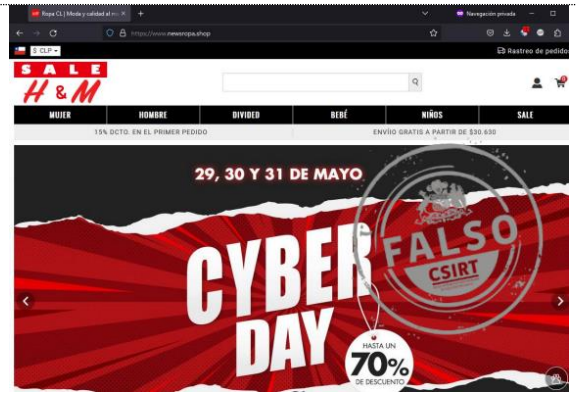
CSIRT alerta de sitio fraudulento que suplanta a Cannon	
Alerta de seguridad cibernética	8FFR23-01342-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://caconcl.godaddysites[.]com/	
Dirección IP	
[13.248.243.5]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01342-01	



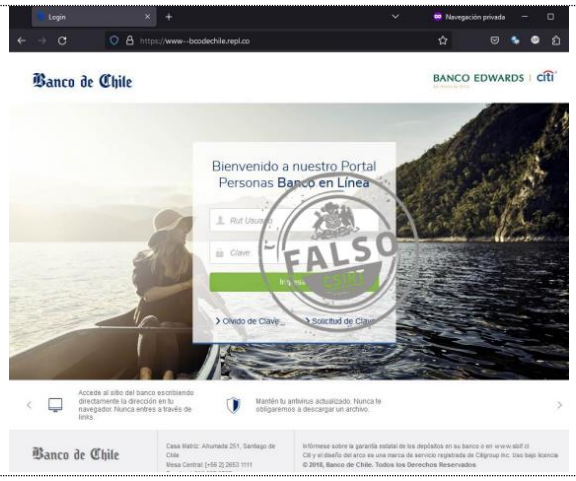
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cannon	
Alerta de seguridad cibernética	8FFR23-01343-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.rebajahet[.]shop	
Dirección IP	
[162.218.176.58]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01343-01	



CSIRT alerta de sitio fraudulento que suplanta a Doite	
Alerta de seguridad cibernética	8FFR23-01344-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2023
Última revisión	27 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.tiimcuiic[.]online	
Dirección IP	
[162.218.176.58]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01344-01	



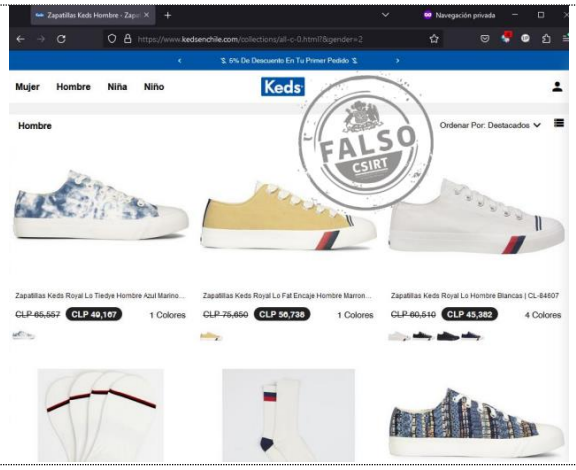
CSIRT alerta de sitio fraudulento que suplanta a H&M	
Alerta de seguridad cibernética	8FFR23-01345-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2023
Última revisión	27 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.newsropa[.]shop/	
Dirección IP	
[107.150.177.15]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01345-01	



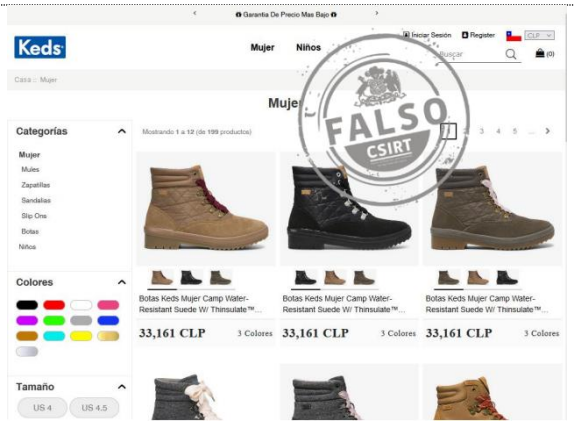
CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01346-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de mayo de 2023
Última revisión	29 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www–bcodechile.repl[.]co/	
Dirección IP	
[34.149.204.188]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01346-01	

CSIRT alerta ante varios sitios fraudulentos que suplantan a numerosas marcas presentes en el CyberDay 2023	
Alerta de seguridad cibernética	8FFR23-01347-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de mayo de 2023
Última revisión	29 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.deportescalzado[.]online/	https://www.dukepet[.]shop/
https://www.myshoespromo[.]online/	https://www.jupefemme[.]online/
https://www.clothsalesit[.]online/	https://www.modahandm[.]shop/
https://www.rustinlowe[.]shop/	https://www.sapatiofers[.]shop/
https://www.saleousontius[.]online/	https://www.lipmies[.]online/
https://www.uniedoudoune[.]online/	https://www.babyropaa[.]shop/
https://www.saptofers[.]online/	https://www.melichinelos[.]shop/
https://www.vetemcam[.]online/	https://www.neudones[.]online/
https://www.saleshkalmgr[.]online	https://www.skersapatos[.]shop/
https://www.borseitalias[.]online/	

	Dirección IP		
	[199.21.150.24]	[162.222.89.177]	[23.252.66.113]
	[23.252.71.150]	[167.160.3.13]	[107.150.166.236]
	[107.150.166.243]	[23.252.68.234]	[107.150.173.210]
	[107.150.173.206]	[23.252.68.239]	[107.150.166.229]
	[199.21.150.25]	[167.160.3.5]	[162.222.89.176]
	[23.252.68.235]	[167.160.3.20]	
	Enlace para revisar el informe:		
	https://www.csirt.gob.cl/alertas/8ffr23-01347-01		



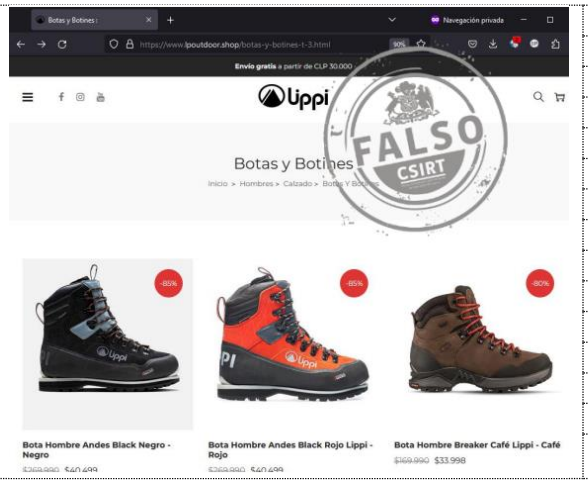
CSIRT alerta de nuevo sitio fraudulento que suplanta a Keds	
Alerta de seguridad cibernética	8FFR23-0148-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de mayo de 2023
Última revisión	29 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.kedsenchile[.]com/	
Dirección IP	
[196.196.194.131]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01348-01	



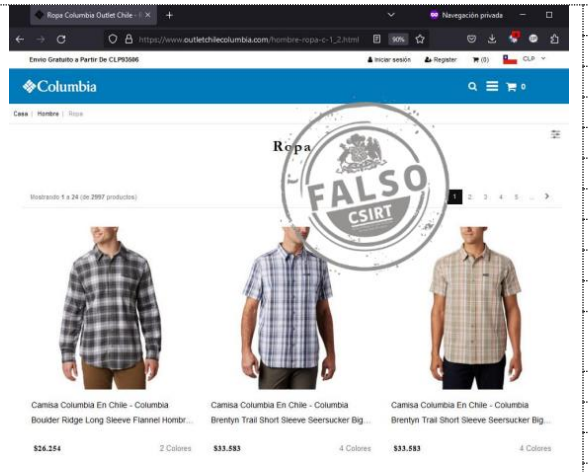
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Keds	
Alerta de seguridad cibernética	8FFR23-01349-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2023
Última revisión	30 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.kedscl[.]com/	
Dirección IP	
[196.245.249.72]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01349-01	

Nota: la alerta 8FFR23-01350-01 fue publicada con un error, fue eliminada y por eso no es parte de este boletín. Sus consejos, especialmente lo relativo a bloqueos de IP y direcciones web, contenían errores y no deben ser considerados.

CSIRT alerta de la activación de una página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01351-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://informu[.]live/correos_cl/?cep	
Dirección IP	
[93.95.227.126]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01351-01	

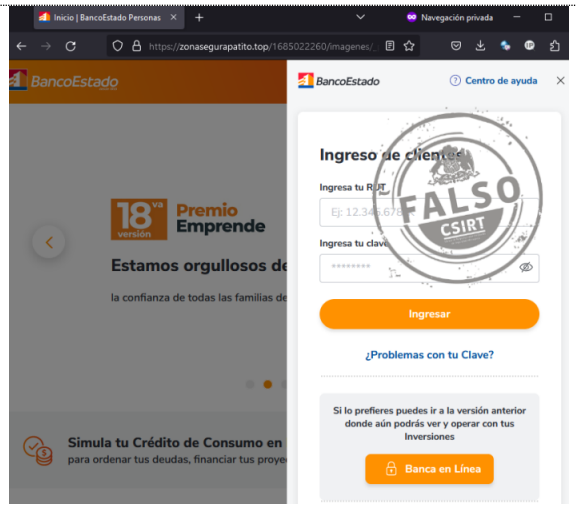


CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01352-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lpoutdoor[.]shop	
Dirección IP	
[172.67.188.191]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01352-01	

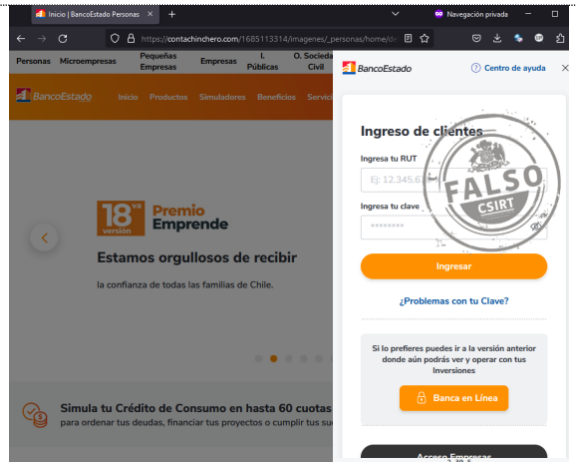


CSIRT alerta de nueva página fraudulenta que suplanta a Columbia	
Alerta de seguridad cibernética	8FFR23-01353-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.tiendacolumbiachile[.]com/ https://www.outletchilecolumbia[.]com/	
Dirección IP	
[172.67.188.191]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01353-01	

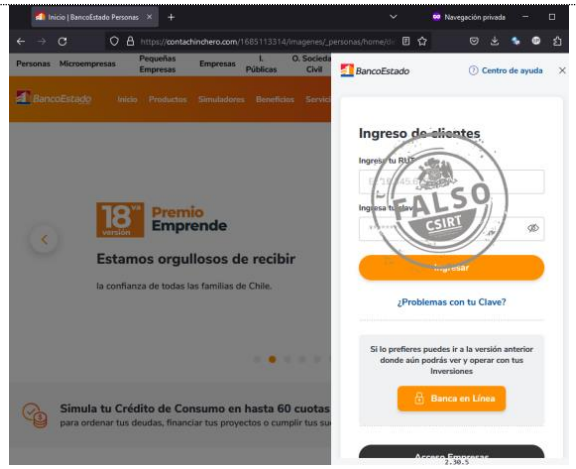
2. Phishing



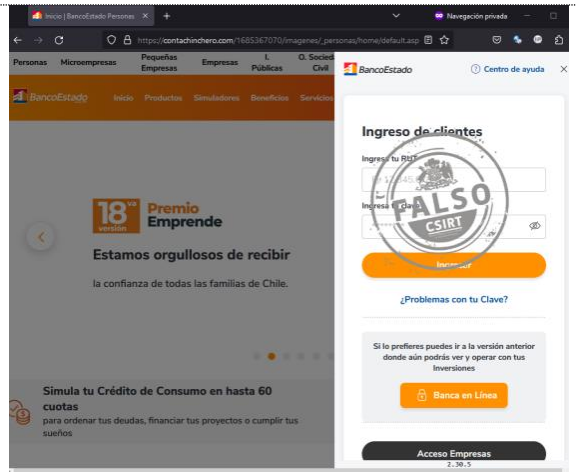
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00822-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023
URL redirección	
https://zoomcontactdoor[.]com/activacion/cuenta-dzqa/	
URL sitio falso	
https://zonasegurapatito[.]top/1685022260/imagenes/_personas/home/default.asp	
Dirección IP	
[98.142.101.90]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00822-01/	



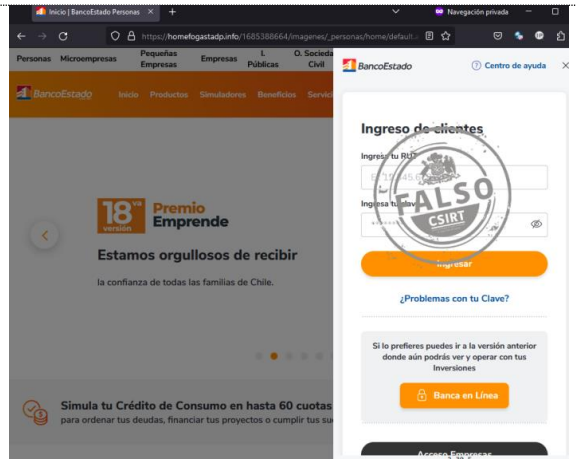
CSIRT alerta ante nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00823-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-sdbg/	
URL sitio falso	
https://contachinchero[.]com/1685113314/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[138.128.170.234]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00823-01/	



CSIRT alerta de una nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00824-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://hopgia[.]vn/module/activacion/cuenta-kzho/	
URL sitio falso	
https://homefogastadp.info/1685118087/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[213.136.93.171]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00824-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00825-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de mayo de 2023
Última revisión	29 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-zksc/	
URL sitio falso	
https://contachinchero[.]com/1685367070/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[138.128.170.234]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00825-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00826-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de mayo de 2023
Última revisión	29 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://hopgia[.]vn/module/activacion/cuenta-kzho/	
URL sitio falso	
https://homefogastadp[.]info/1685388664/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[213.136.93.171]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00826-01/	

CSIRT alerta ante nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00827-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3oMxl6V?l=www.bancoripley.cl	
URL sitio falso	
https://web.bancoripley-cl.grfer[.]com.br/1685557879/login/index.html	
Dirección IP sitio falso	
[108.167.171.58]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00827-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Conaset	
Alerta de seguridad cibernética	2CMV23-00415-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2023
Última revisión	26 de mayo de 2023
Indicadores de compromiso	
URL-Dominio	
https://psdasyogapathy[.]org/images/conaset/ https://montao.com.pe/adslink/ 50.116.72[.]199 89.116.255[.]59:9999	
SHA256	
00b8b72c1353a2a6646e20bdddad58318dab20ade02151ce3864ff04c912a2cc c8c6ff192502979e1a1983919bd3cadfb8e0c7409f02476c540a6802397222f6 14cef33c97ba660caca4bb0552caa4e68bfa3f117111a10b8d3a3addab7b06b5 c8c6ff192502979e1a1983919bd3cadfb8e0c7409f02476c540a6802397222f6 c09d0790e550694350b94ca6b077c54f983c135fab8990df5a75462804150912 e1cba56f20dbad484273f58df3d672b4b07f36d237e4cb16dcedd9fba0a720a1 a5a770b8d64d757f8894e551ace0627dbe60c3b4e5032d2ccb8ca56f0d0ee352 de87c8713fac002b0b0a0f9b02c4e3ebcccf65282a22f5ab5912a9da00f35c2a	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00415-01/	

CSIRT alerta de nueva campaña de phishing con malware, difundido a través de falso aviso de pago	
Alerta de seguridad cibernética	2CMV23-00416-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo de 2023
Indicadores de compromiso	
URL-Dominio	
23.72.32[.]173	
SHA256	
7c8967960ad84f41435692215c414f6b21f804a6679b4754be52e866cd9bfec8 8ba3f2678bd2622e665539d20ba61643782d2e99ee0f9cd703221fae5d49e2c0 f004c568d305cd95edbd704166fcd2849d395b595dff814bcc2012693527ac37 9c22043cc1b16fcbcbd6cc8d478420779437a04626f82c4ba4345add0a025caa d76f82f670ae983c553ecac05ca77958e9c761e05f3e0e6d741372d34348a340 30612f5a43f9cb99f90f87fa6b63bf0f886f6acf2ef0ddddc2663437e9ec0261	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00416-01/	

4. Vulnerabilidades

CSIRT informa de vulnerabilidad crítica en Barracuda ESG	
Alerta de seguridad cibernética	9VSA23-00835-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2023
Última revisión	30 de mayo de 2023
CVE	
CVE-2023-2868	
Fabricantes	
Barracuda	
Productos afectados	
Barracuda Email Security Gateway versiones 5.1.3.001 a 9.2.0.006	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00835-01/	

CSIRT comparte vulnerabilidades parchadas en Google Chrome 114		
Alerta de seguridad cibernética	9VSA23-00840-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	31 de mayo de 2023	
Última revisión	31 de mayo de 2023	
CVE		
CVE-2023-2929	CVE-2023-2934	CVE-2023-2938
CVE-2023-2930	CVE-2023-2935	CVE-2023-2939
CVE-2023-2931	CVE-2023-2936	CVE-2023-2940
CVE-2023-2932	CVE-2023-2937	CVE-2023-2941
CVE-2023-2933		
Fabricantes		
Apple		
Productos afectados		
Google Chrome		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00840-01/		

5. Concientización

Gobierno presentó su nueva Política Nacional de Ciberseguridad

Este viernes 26 de mayo, en una ceremonia en el Palacio de La Moneda, el Subsecretario del Interior, Manuel Monsalve, y la Subsecretaria de Ciencia, Carolina Gainza, presentaron la nueva Política Nacional de Ciberseguridad del Gobierno de Chile (PNCS). Esta es una actualización de la primera PNCS, presentada en 2017.

Para que entre en vigor solo falta que el Presidente Gabriel Boric firme el correspondiente decreto y la Contraloría tome razón.

Durante la presentación, el Subsecretario Monsalve señaló que «esta política es para proteger a las personas y al país, y destacó que con esta política, Chile podría lograr estar dentro de los puestos más altos de los rankings mundiales de ciberseguridad, al lograr, entre otras cosas, que «las empresas que invierten también tomen en cuenta la ciberseguridad».

Más información: https://www.csirt.gob.cl/noticias/gobierno-presento-su-nueva-politica-nacional-de-ciberseguridad/

CSIRT realiza nuevamente exposición ante el Curso de Estado Mayor de la Academia de Guerra Aérea

Los expositores fueron Carlos Silva, jefe del CSIRT, y Juan Moraga, analista del mismo. En primer lugar, Silva presentó un resumen de las funciones del CSIRT y el proceso que se sigue desde que la institución toma conocimiento de un evento o incidente. Además, agradeció la invitación y destacó la importancia de continuar con instancias de colaboración entre instituciones del Estado, como la presente.

Más información: https://www.csirt.gob.cl/noticias/csirt-academia-de-guerra-aerea-2023/.

Exitosa tercera edición de la simulación de ciberataque presentada por el CSIRT y Microsoft a empleados públicos

Este viernes 26 de mayo tuvo lugar la tercera convocatoria organizada por el CSIRT de Gobierno a la presentación realizada por Microsoft de cómo es vivir un ciberataque en tiempo real, instancia exclusiva para funcionarios públicos de todo el país y que permite a los asistentes ponerse en el lugar de una organización que está siendo atacada, debatiendo entre ellos y con los representantes de Microsoft la conveniencia de distintos cursos de acción. Más información disponible aquí: https://www.csirt.gob.cl/noticias/tercera-simulacion-microsoft-2023/.

La próxima edición de esta simulación tendrá lugar el 22 de junio de 2023 y será virtual, buscando la participación de empleados públicos de todas las regiones del país. Las inscripciones pueden realizarse en el siguiente formulario: https://forms.gle/E3f38ZGtvnD78GKAA.

Ciberdiccionario Volumen 37

Con la intención de seguir sumando conceptos a nuestro Ciberdiccionario, esta semana les traemos definiciones de data broker, prompt, spear phishing y passkey. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están contenidas siempre en: http://csirt.gob.cl/recomendaciones.

6. 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 que los sitios web a los que se ingrese sean los oficiales.

7. 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.

- Juan Pablo Berríos.
- Francisca Orellana Cartes.
- Francisco Javier Flores Varela.
- Óscar Videla.
- Ivanna Janet López Serrano.
- Carlos Alberta Pinto Mora.
- Sugy Nam.
- Rigoberto Cancino.
- María Angélica Bosch Cartagena.
- Elizabeth Uribe Barría.
- Catalina Inés Sanhueza Rivera.
- Vaitiare García
- Paul Helbig Soto.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.02 16:16:05 -04'00'