CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 203

semana del 19 al 25 de mayo de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

19

IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

34

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

100

Las mitigaciones son útiles en productos de Samsung, Apple, GitLab y Zyxel.

HASH REPORTADOS

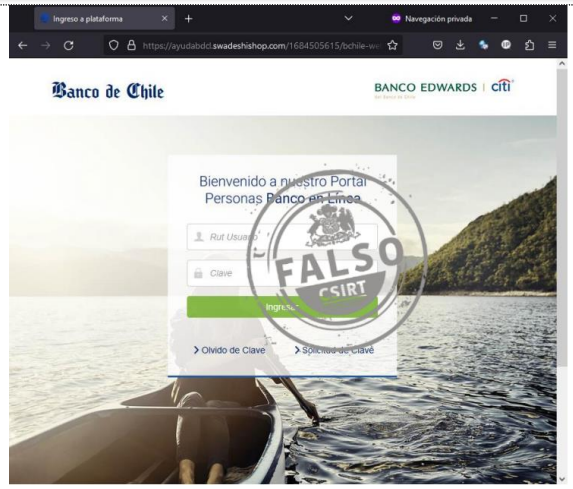
3

asociadas a múltiples campañas de phishing con archivos que contienen malware

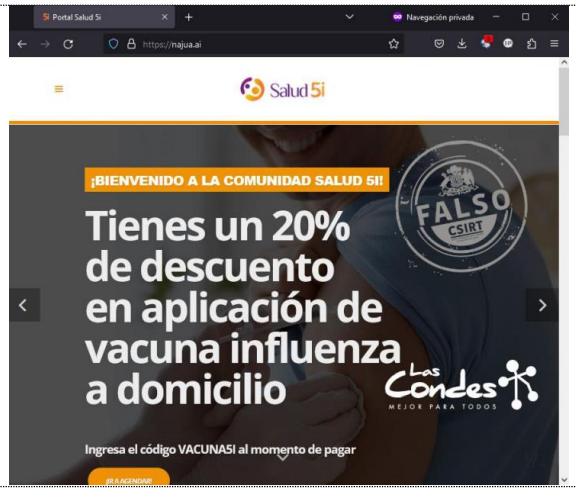
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

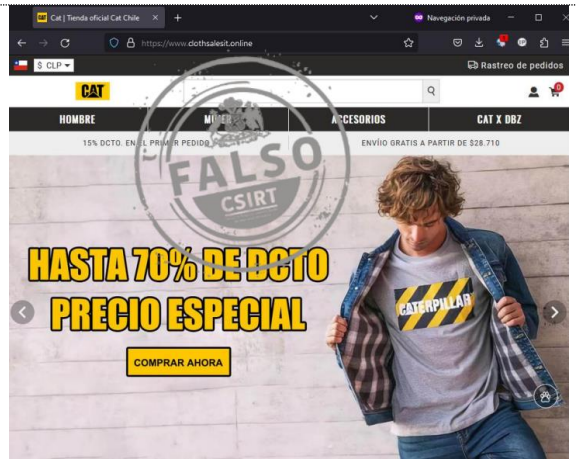
1. Sitios fraudulentos



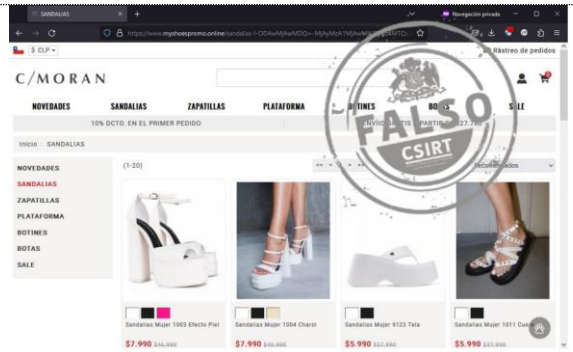
CSIRT alerta ante sitio fraudulento que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01328-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2023
Última revisión	19 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://ayudabdcl.swadeshishop[.]com/1684505615/bchile-web/persona/login/index.html/login	
Dirección IP	
[85.187.128.31]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01328-01	



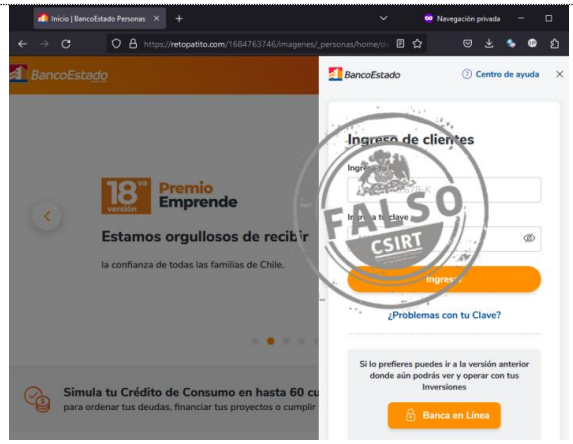
CSIRT alerta ante sitio falso que suplanta a Salud 5i	
Alerta de seguridad cibernética	8FFR23-01329-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://najua[.]ai/	
Dirección IP	
[104.21.44.112]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01329-01	



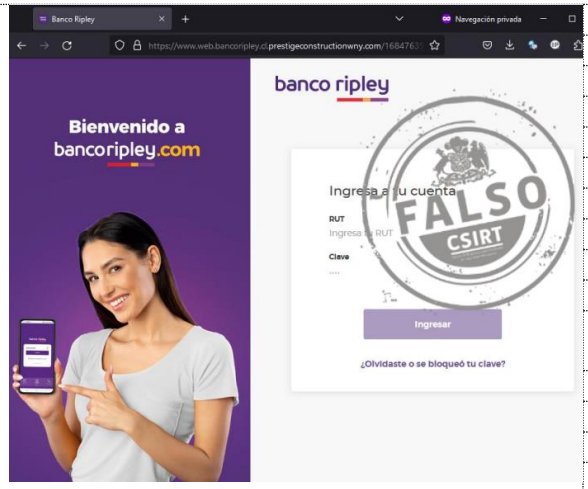
CSIRT alerta de sitio fraudulento que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01330-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://shoescat.mystrikingly.com/ https://www.clothsalesit.online/	
Dirección IP	
[107.150.166.243]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01330-01	



CSIRT alerta de sitio fraudulento que suplanta a C/Moran	
Alerta de seguridad cibernética	8FFR23-01331-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.myshoespromo[.]online/	
Dirección IP	
[23.252.71.150]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01331-01	

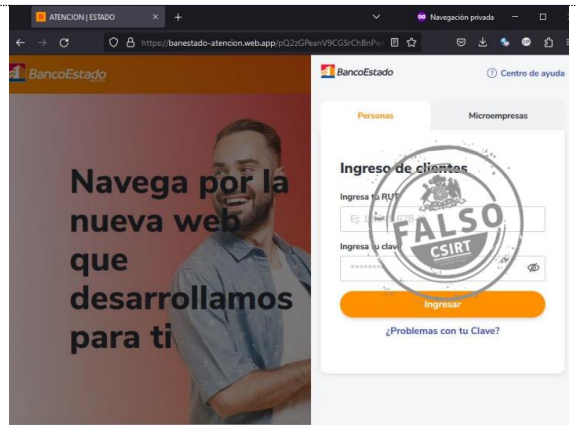


CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01332-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://retopatito[.]com/1684763746/imagenes/_personas/home/default.asp	
Dirección IP	
[98.142.101.90]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01332-01	

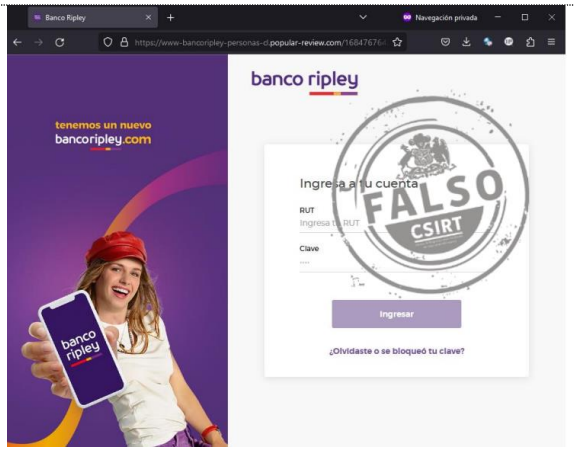


CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01333-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.web.bancoripley.cl.prestigeconstructionwny[.]com/1684763984/login	
Dirección IP	
[192.185.21.172]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01333-01	

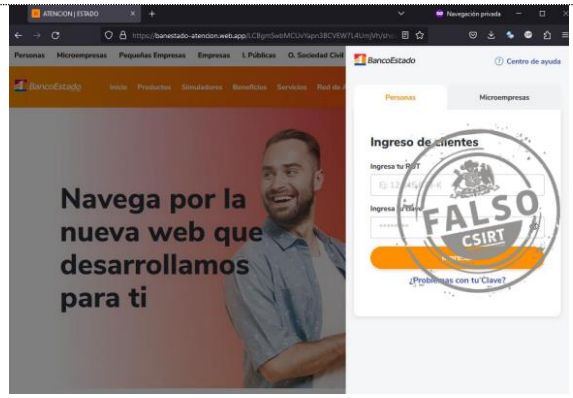
CSIRT alerta de página fraudulenta que suplanta al Gobierno de Chile con la oferta de falsos bonos	
Alerta de seguridad cibernética	8FFR23-01334-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://gobchile.canalformacion[.]site/	
Dirección IP	
[157.245.227.78]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01334-01	



CSIRT alerta de la activación de web fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01335-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://banestado-atencion.web[.]app/	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01335-01	



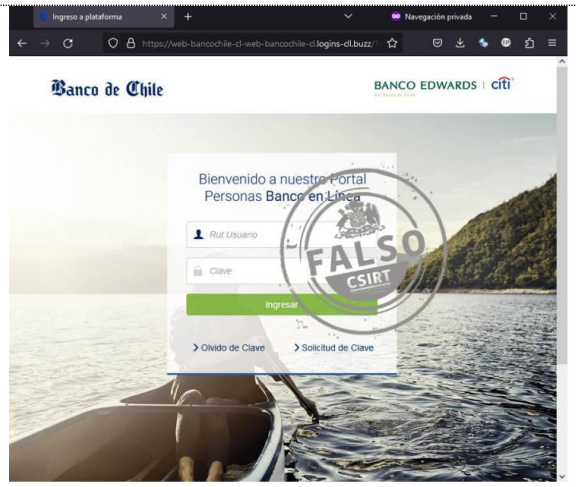
CSIRT alerta ante página falsa que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01336-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2023
Última revisión	22 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www-bancoripley-personas-cl.popular-review[.]com/1684767642/login/index.html	
Dirección IP	
[198.54.116.184]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01336-01	



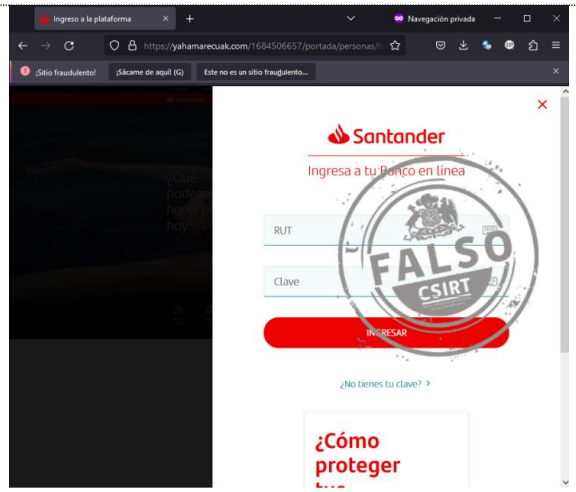
CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01337-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2023
Última revisión	24 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://banestado-atencion.web[.]app/	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01337-01	

CSIRT alerta de sitios fraudulentos que suplantan a Copec	
Alerta de seguridad cibernética	8FFR23-01338-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2023
Última revisión	24 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://www.facebook[.]com/ads/library/?id=633629151994254 https://www.facebook[.]com/ads/library/?id=255028966903103 https://www.facebook[.]com/ads/library/?id=1152089978792182	
URL sitio falso	
https://conduitgrenades[.]com/optio/?px=2129228548710 49&ac=ageyap2&c=orencl33 https://aktivmemory[.]com/quo/?px=257452091262524&ac=age2&c=2 https://aktivmemory[.]com/quo/?px=3439185366295760&ac=age1&c=1 https://aktivmemory[.]com/quo/thanks/index.php	
Dirección IP	
[165.22.79.159] [104.21.51.211] [172.67.186.89]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01338-01	

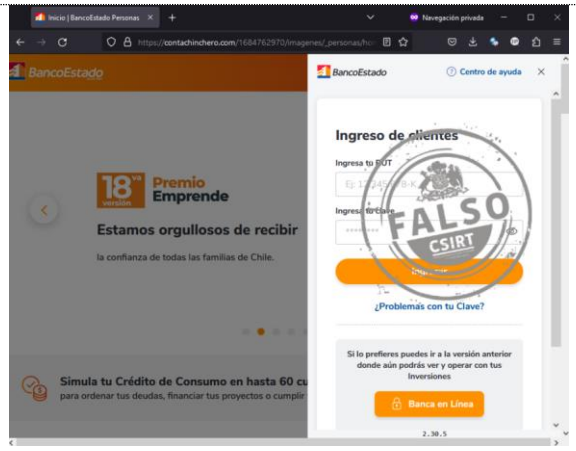
2. Phishing



CSIRT alerta de una nueva campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH23-00814-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2023
Última revisión	19 de mayo de 2023
URL redirección	
https://tarjeta-cl[.]top/	
URL sitio falso	
https://web-bancochile-cl-web-bancochile-cl.logins-cll[.]buzz/1684504981/bancochile-web/persona/login/index.html/login	
Dirección IP	
[104.21.82.172]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00814-01/	



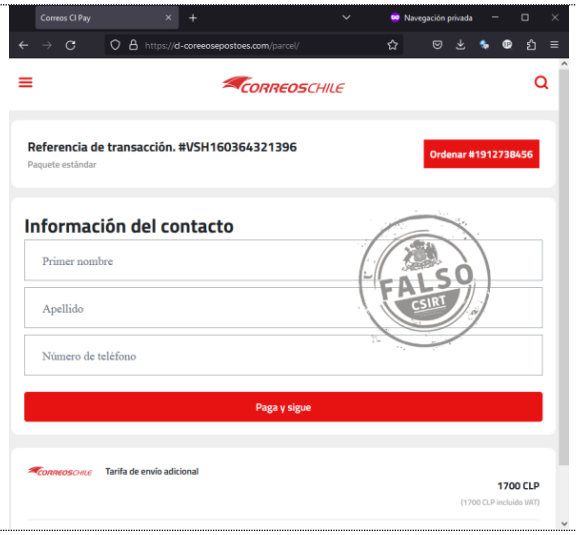
CSIRT alerta de nueva campaña de phishing que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00815-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2023
Última revisión	19 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://yahamarecuak[.]com/1684506657/portada/personas/home.asp	
URL redirección:	
https://lidercolor.com[.]br/consulta/beneficio/ https://yahamarecuak[.]com/?cid=UsuarioRestaurar&cat=cgiRestaurar&gClic=b1a59b315fc9a3002ce38bbe070ec3f5&valueValidar	
Dirección IP sitio falso	
[98.142.101.90]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00815-01/	



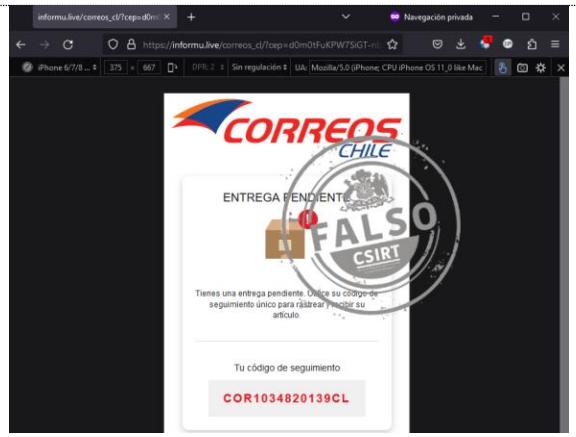
CSIRT alerta ante nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00816-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2023
Última revisión	23 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-sdbg/	
URL sitio falso	
https://contachinchero.com/1684762970/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[138.128.170.234]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00816-01/	

CSIRT alerta de nueva campaña de phishing via email, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00817-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2023
Última revisión	23 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-sdbg/	
URL sitio falso	
https://contachinchero[.]com/1684852963/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[138.128.170.234]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00817-01/	

CSIRT alerta de campaña de phishing que engaña con falso aviso para actualizar cuenta de email	
Alerta de seguridad cibernética	8FPH23-00818-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2023
Última revisión	23 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.landpagepreview.com/f599b73a-f936-11ed-b3a9-a6da6f1d126b	
Dirección IP sitio falso	
[157.53.227.1]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00818-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00820-01
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
Indicadores de compromiso	
URL sitio falso	
https://cl-coreeosepostoes[.]com/parcel/	
Dirección IP sitio falso	
[149.100.151.191]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00820-01/	



CSIRT alerta ante nueva campaña de phishing que se hace pasar por CorreosChile	
Alerta de seguridad cibernética	8FPH23-00821-01
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
Indicadores de compromiso	
URL redirección:	
http://sgqo[.]me/ZmYgoK	
URL sitio falso	
https://cl-coreeosepostoes[.]com/parcel/	
Dirección IP sitio falso	
[93.95.227.126]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00821-01/	

3. Malware

CSIRT alerta de campaña de phishing con el malware Grandoeiro, difundido via falsa notificación judicial	
Alerta de seguridad cibernética	2CMV23-00413-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2023
Última revisión	24 de mayo de 2023
Indicadores de compromiso	
URL-Dominio	
https://atlinkwifiprogramado.australiacentral.cloudapp.azure[.]com/ https://www.dropbox[.]com/s/aagvp0fccnb8sk8/AttatchmentFacturQEDGDCLYXHEEAYDdqjvo.zip http://ip-api[.]com/json 20.54.89[.]15:443 208.95.112[.]1 67.27.158[.]126	
SHA256	
3a053c761405b390b821dcfa246aef4e77f9bfa991ec5980ae58150793c1a8ba 9a8bff65411c24aa7df8cb56053f21aad2868613fc84cf44bae06692bae0da06 0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00413-01/	

4. Vulnerabilidades

CSIRT comparte vulnerabilidad que afecta algunos celulares Samsung con Android 11, 12 y 13	
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	22 de mayo de 2023
Última revisión	22 de mayo de 2023
CVE	
CVE-2023-21492	
Fabricantes	
Samsung	
Productos afectados	
Algunos aparatos Android 11, 12 y 13.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00835-01/	

CSIRT comparte vulnerabilidades parchadas por Apple, incluyendo tres de día cero		
Alerta de seguridad cibernética	9VSA23-00833-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	23 de mayo de 2023	
Última revisión	23 de mayo de 2023	
CVE		
CVE-2023-23532	CVE-2023-32391	CVE-2023-32373
CVE-2023-27930	CVE-2023-32392	CVE-2023-32376
CVE-2023-27940	CVE-2023-32394	CVE-2023-32380
CVE-2023-27945	CVE-2023-32395	CVE-2023-32382
CVE-2023-28181	CVE-2023-32397	CVE-2023-32384
CVE-2023-28191	CVE-2023-32398	CVE-2023-32387
CVE-2023-28202	CVE-2023-32399	CVE-2023-32388
CVE-2023-28204	CVE-2023-32400	CVE-2023-32391
CVE-2023-32403	CVE-2023-32402	CVE-2023-32392
CVE-2023-32352	CVE-2023-32403	CVE-2023-32394
CVE-2023-32354	CVE-2023-32404	CVE-2023-32395
CVE-2023-32355	CVE-2023-32405	CVE-2023-32386
CVE-2023-32357	CVE-2023-32407	CVE-2023-32397
CVE-2023-32360	CVE-2023-32408	CVE-2023-32398
CVE-2023-32363	CVE-2023-32409	CVE-2023-32399
CVE-2023-32365	CVE-2023-32410	CVE-2023-32400
CVE-2023-32367	CVE-2023-32411	CVE-2023-32402
CVE-2023-32368	CVE-2023-32412	CVE-2023-32403
CVE-2023-32369	CVE-2023-32413	CVE-2023-32404
CVE-2023-32371	CVE-2023-32415	CVE-2023-32405
CVE-2023-32372	CVE-2023-32417	CVE-2023-32407
CVE-2023-32373	CVE-2023-32419	CVE-2023-32408
CVE-2023-32375	CVE-2023-32420	CVE-2023-32409
CVE-2023-32376	CVE-2023-32422	CVE-2023-32410

	CVE-2023-32382	CVE-2023-32423	CVE-2023-32411
	CVE-2023-32384	CVE-2023-32352	CVE-2023-32412
	CVE-2023-32385	CVE-2023-32357	CVE-2023-32413
	CVE-2023-32386	CVE-2023-32367	CVE-2023-32414
	CVE-2023-32387	CVE-2023-32368	CVE-2023-32415
	CVE-2023-32388	CVE-2023-32369	CVE-2023-32420
	CVE-2023-32389	CVE-2023-32371	CVE-2023-32422
	CVE-2023-32390	CVE-2023-32372	CVE-2023-32423
	Fabricantes		
	Apple		
	Productos afectados		
	macOS Big Sur y macOS Monterey Apple Watch Series 4 y versiones posteriores Apple TV 4K (todos los modelos) y Apple TV HD iPhone 8 y modelos posteriores, iPad Pro (todos los modelos), iPad Air (tercera generación y modelos posteriores), iPad (quinta generación y modelos posteriores), y iPad mini (quinta generación y modelos posteriores) iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (primera generación), iPad Air 2, iPad mini (cuarta generación) y iPod touch (séptima generación) macOS Big Sur macOS Ventura macOS Monterey		
	Enlaces para revisar el informe:		
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00836-01/		

CSIRT comparte datos de vulnerabilidad crítica parchada por GitLab	
Alerta de seguridad cibernética	9VSA23-00837-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023
CVE	
CVE-2023-2825	
Fabricantes	
GitLab	
Productos afectados	
GitLab Community Edition (CE) y Enterprise Edition (EE) desde la versión 16.0.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00837-01/	

CSIRT comparte información de vulnerabilidades críticas parchadas por Zyxel	
Alerta de seguridad cibernética	9VSA23-00838-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023
CVE	
CVE-2023-33009 CVE-2023-33010	
Fabricantes	
Zyxel	
Productos afectados	
Zyxel ATP firmware versiones ZLD V4.32 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2) Zyxel USG FLEX firmware versiones ZLD V4.50 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2) Zyxel USG FLEX50(W) / USG20(W)-VPN firmware versiones ZLD V4.25 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2) Zyxel VPN firmware versiones ZLD V4.30 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2) Zyxel ZyWALL/USG firmware versiones ZLD V4.25 a V4.73 Patch 1 (parchado en ZLD V4.73 Patch 2)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00838-01/	

5. Concientización

Ciberconsejos para el CyberDay de mayo 2023

Mantener conductas seguras al comprar por internet es siempre un requisito, pero más aún cuando se trata de un evento de ventas online tan grande como un CyberDay. Por eso queremos recordarles los principales consejos para mantenernos más seguros al hacer transacciones en línea.

Estas recomendaciones están disponibles en PDF, aquí: 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.

- Jaime Ricardo Uribe Guzmán
- María Francisca Villouta Porcile
- Carlos Román
- Felipe Cortés
- Migdalis Mago
- Carolina Andrea Morales García
- Roberto Salas
- Alonso Ignacio Villalobos González

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.26 16:52:25 -04'00'