CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 222

semana del 29 de septiembre al 5 de octubre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

10

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

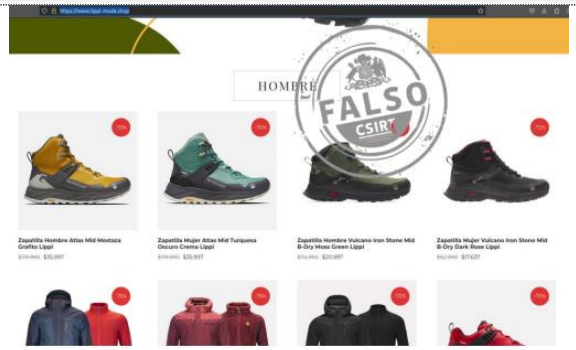
56

Las mitigaciones son útiles en productos de Android, Microsoft y Atlassian.

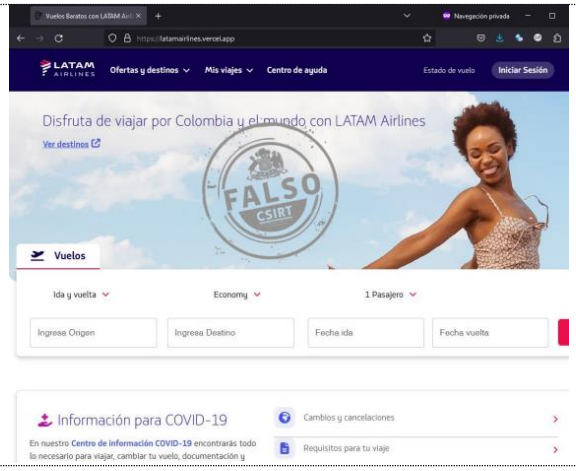
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

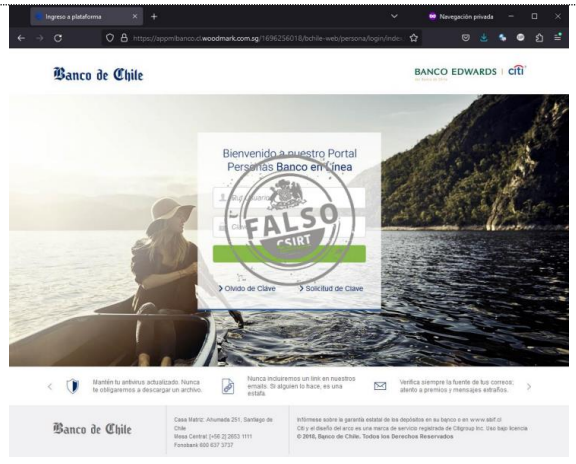
1. Sitios fraudulentos



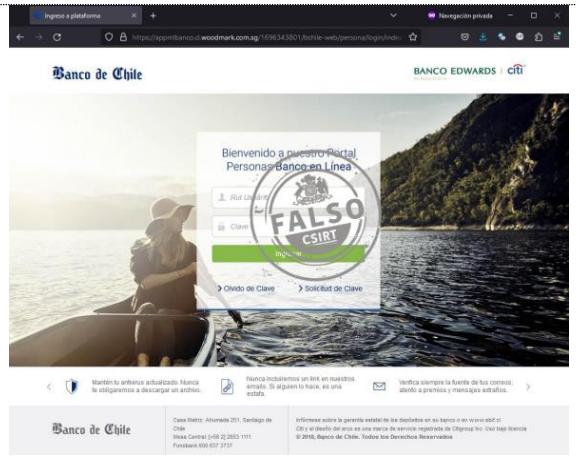
CSIRT alerta de nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01536-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 septiembre, 2023
Última revisión	29 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lippi-moda.shop/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01536-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Latam	
Alerta de seguridad cibernética	8FFR23-01537-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 octubre, 2023
Última revisión	2 octubre, 2023
Indicadores de compromiso	
URL sitio falso	
https://latamairlines.vercel.app/	
IP del sitio falso	
[76.76.21.142]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01537-01/	

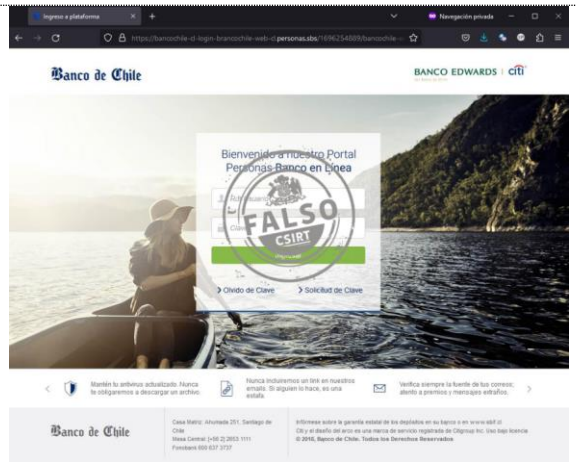


CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01538-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 octubre, 2023
Última revisión	2 octubre, 2023
Indicadores de compromiso	
URL sitio falso	
https://appmlbanco.cl.woodmark[.]com.sg/1696256018/bchile-web/persona/login/index.html/login	
IP del sitio falso	
[85.187.128.38]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01538-01/	

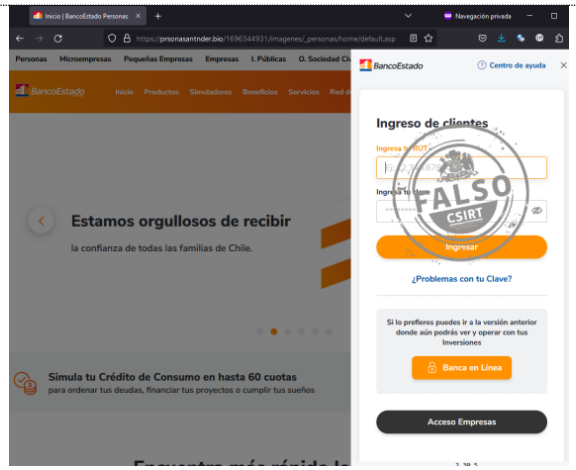


CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01539-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 octubre, 2023
Última revisión	5 octubre, 2023
Indicadores de compromiso	
URL sitio falso	
https://appmlbanco.cl.woodmark.com.sg/1696343801/bchile-web/persona/login/index.html/login	
IP del sitio falso	
[85.187.128.38]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01539-01/	

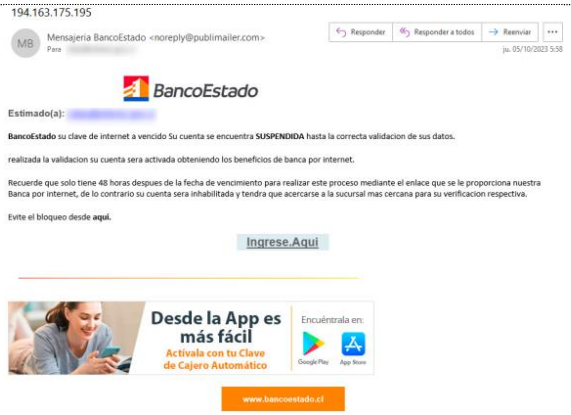
2. Phishing



CSIRT advierte de nueva campaña de phishing que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FPH23-00894-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 octubre, 2023
Última revisión	3 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://prsonasantnder[.]bio/1696344931/imagenes/_personas/home/default.asp	
URL de redirección	
https://codeundestado[.]com/activacion/cuenta-padw/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00894-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00895-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 octubre, 2023
Última revisión	3 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://prsonasantnder[.]bio/1696344931/imagenes/_personas/home/default.asp	
URL de redirección	
https://codeundestado[.]com/activacion/cuenta-padw/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00895-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00896-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 octubre, 2023
Última revisión	5 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://prsonasantnder[.]bio/1696509264/imagenes/_personas/home/default.asp	
URL de redirección	
https://codeundestado[.]com/activacion/cuenta-padw/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00896-01/	

3. Vulnerabilidades

CSIRT informa de parches de Microsoft para vulnerabilidades en libwebp y libvpx	
Alerta de seguridad cibernética	9VSA23-00911-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 octubre, 2023
Última revisión	5 octubre, 2023
CVE	
CVE-2023-4863 CVE-2023-5217	
Fabricante	
Microsoft	
Productos afectados	
Microsoft Edge Microsoft Teams for Desktop Skype for Desktop Webp Image Extensions (Released on Windows and updates through Microsoft Store)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00911-01/	

CSIRT informa de parche publicado por Atlassian para vulnerabilidad crítica en Confluence Data Center and Server	
Alerta de seguridad cibernética	9VSA23-00912-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 octubre, 2023
Última revisión	5 octubre, 2023
CVE	
CVE-2023-22515	
Fabricante	
Atlassian	
Productos afectados	
Confluence Data Center and Server 8.0.0 y posteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00912-01/	

CSIRT comparte información de actualización de seguridad mensual de Android correspondiente a octubre 2023			
Alerta de seguridad cibernética		9VSA23-00913-01	
Clase de alerta		Vulnerabilidad	
Tipo de incidente		Sistema y/o Software Abierto	
Nivel de riesgo		Alto	
TLP		Blanco	
Fecha de lanzamiento original		27 septiembre, 2023	
Última revisión		27 septiembre, 2023	
CVE			
CVE-2023-21266	CVE-2023-40117	CVE-2023-4211	CVE-2023-21673
CVE-2023-40116	CVE-2023-40129	CVE-2023-33200	CVE-2023-22385
CVE-2023-40120	CVE-2023-40125	CVE-2023-34970	CVE-2023-24843
CVE-2023-40131	CVE-2023-40128	CVE-2023-20819	CVE-2023-24844
CVE-2023-40140	CVE-2023-40130	CVE-2023-32819	CVE-2023-24847
CVE-2023-40121	CVE-2023-40123	CVE-2023-32820	CVE-2023-24848
CVE-2023-40136	CVE-2023-40127	CVE-2023-40638	CVE-2023-24849
CVE-2023-40134	CVE-2023-40133	CVE-2023-33029	CVE-2023-24850
CVE-2023-40137	CVE-2023-40135	CVE-2023-33034	CVE-2023-24853
CVE-2023-40138	CVE-2023-21252	CVE-2023-33035	CVE-2023-33026
CVE-2023-40139	CVE-2023-21253	CVE-2023-24855	CVE-2023-33027
CVE-2023-21291	CVE-2022-28348	CVE-2023-28540	CVE-2023-4863
CVE-2023-21244	CVE-2021-44828	CVE-2023-33028	
Fabricante			
Google			
Productos afectados			
Android			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00913-01/			

4. Noticias y concientización

CSIRT recibe interesante ciclo de charlas para funcionarios públicos sobre ciberseguridad y respuesta a incidentes, presentado por Google Cloud y Mandiant

Con la asistencia de un centenar de encargados de ciberseguridad provenientes de Santiago y regiones tuvo lugar un ciclo de charlas sobre ciberseguridad y respuesta a incidentes, presentada por especialistas de Mandiant y Google Cloud. La instancia contó con una positiva respuesta de los presentes, quienes entregaron sus visiones y sugerencias para similarias instancias al CSIRT a través de una encuesta.

Mes de la ciberseguridad | Ciberconsejos para identificar un phishing

El phishing es una de las técnicas de ingeniería social más utilizada por los delincuentes para engañar a las víctimas, haciéndose pasar por una persona, empresa o servicio de confianza. Se realiza por correo electrónico, SMS o apps de mensajería, en los que los delincuentes presionan a las personas a ingresar a un link con el objetivo de dirigirlos a una web fraudulenta y así robar su información.

Revísalos aquí: https://www.csirt.gob.cl/recomendaciones/mes-ciberseguridad-phishing/.

5. 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.

6. 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.

- Milton Reyes Hernández
- Enzo Samir Avendaño Chozas
- Francisco Javier Gutiérrez
- Christian Ferrando
- OSI VTI Universidad de Chile
- Richard von Moltke Necochea
- Maximiliano Barrera Montenegro

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.06 17:07:57 -03'00'