CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 246

semana del 15 al 21 de marzo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

12

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

13

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

28

Las mitigaciones son útiles en productos de Cisco, Google y Mozilla.

CONTENIDO

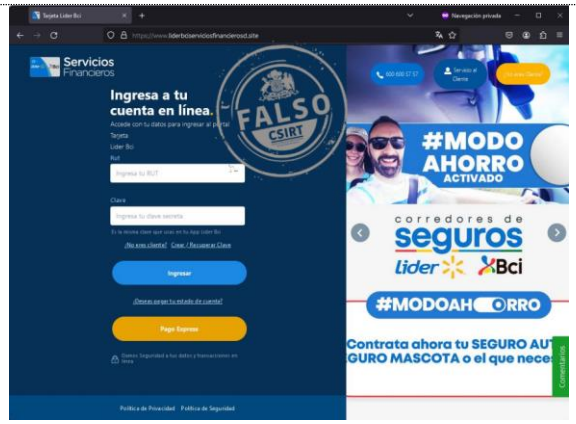
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

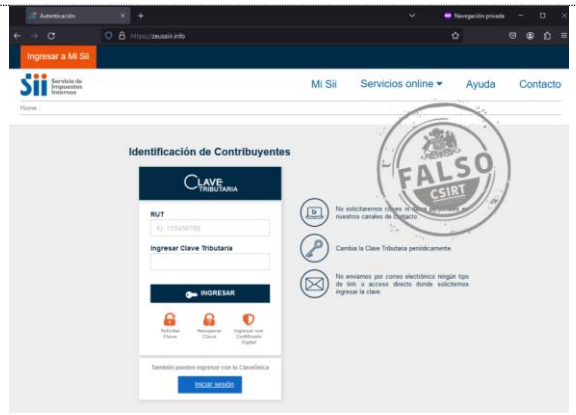
CSIRT informa de una nueva campaña de phishing que suplanta a CorreosChile	
Código de alerta	8FPH24-00940-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://correos-cl-seguimiento.correos-cl[.]sbs/seguimiento/seguimiento.html	
URL de redirección	
https://del-norte[.]autos/correos?https://www.correos.cl/documents/20123/33943275/	
Dirección IP sitio falso	
[104.21.4.92]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00940-01/	

CSIRT alerta de una nueva campaña de phishing que suplanta al Servicio de Salud Metropolitana Oriente	
Código de alerta	8FPH24-00941-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo, 2024
Última revisión	21 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://share.hsforms[.]com/1Ju6hrp76Rcu_DAz1E5bN1gr3lwd	
Dirección IP sitio falso	
[104.18.176.125]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00941-01/	

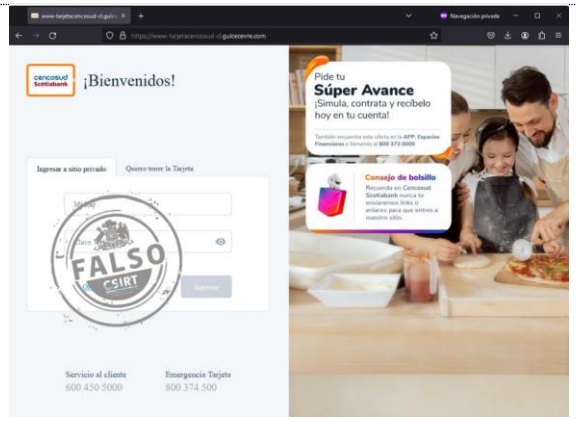
2. Sitios fraudulentos



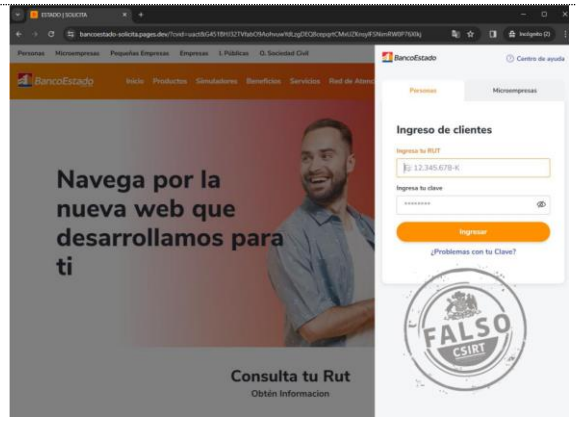
CSIRT alerta de nuevo sitio fraudulento que suplanta a Líder BCI	
Código de alerta	8FFR24-01664-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de marzo, 2024
Última revisión	19 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.liderbciserviciosfinancieroscl[.]site/	
Dirección IP sitio falso	
[154.41.250.28]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01664-01/	



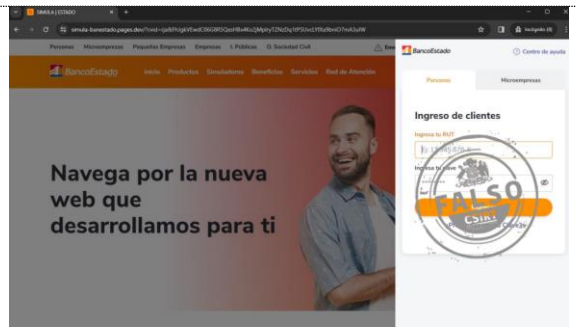
CSIRT informa de nuevo sitio fraudulento que suplanta al Servicio de Impuestos Internos (SII)	
Código de alerta	8FFR24-01665-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://zeussiir[.]info/	
Dirección IP sitio falso	
[104.21.53.84]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01665-01/	



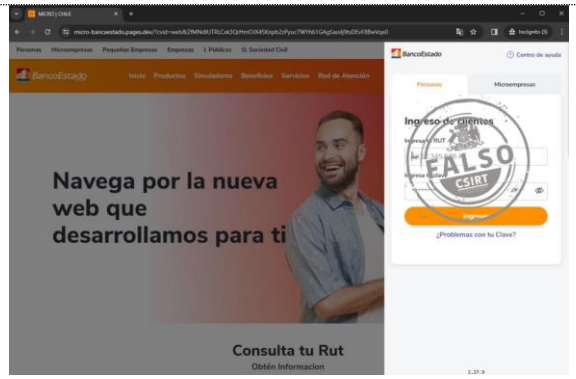
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Código de alerta	8FFR24-01666-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www-tarjetacencosud-cl.gulcecevre[.]com/	
Dirección IP sitio falso	
[94.199.206.206]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01666-01/	



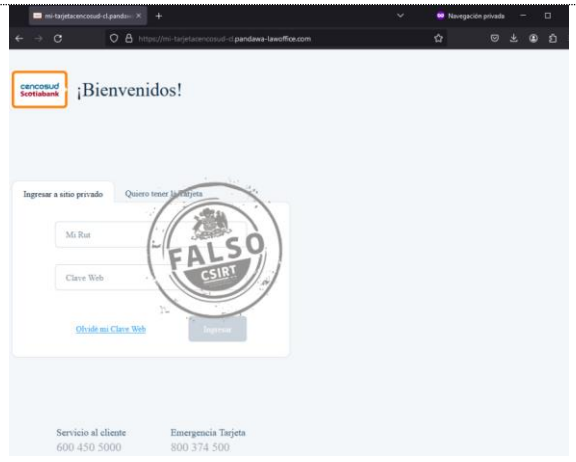
CSIRT alerta de un nuevo sitio fraudulento que suplanta a BancoEstado	
Código de alerta	8FFR24-01667-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://bancoestado-solicita[.]pages.dev/fr7pr|94	
Dirección IP sitio falso	
[172.66.44.183]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01667-01/	



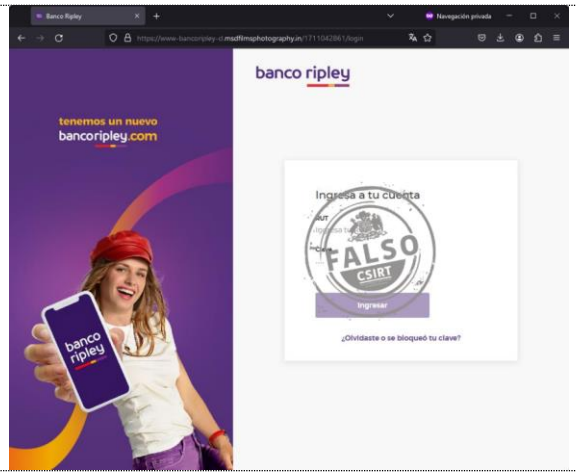
CSIRT advierte de un nuevo sitio fraudulento que suplanta a BancoEstado	
Código de alerta	8FFR24-01668-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://simula-banestado.pages[.]dev/LTypron	
Dirección IP sitio falso	
[172.66.47.176]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01668-01/	



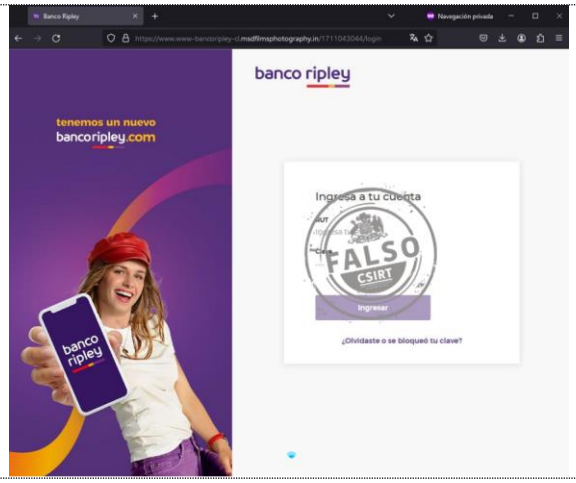
CSIRT alerta de una nueva página fraudulenta que suplanta a BancoEstado	
Código de alerta	8FFR24-01669-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://micro-bancaestado.pages[.]dev/fr7prl94	
Dirección IP sitio falso	
[172.66.44.146]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01669-01/	



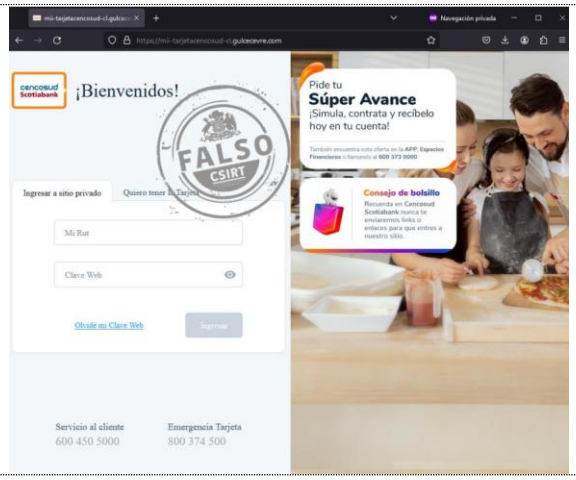
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Código de alerta	8FFR24-01670-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo, 2024
Última revisión	20 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://mi-tarjetacencosud-cl.pandawa-lawoffice[.]com/	
Dirección IP sitio falso	
[172.66.44.146]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01670-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Banco Ripley	
Código de alerta	8FFR24-01671-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo, 2024
Última revisión	21 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www-bancoripley-cl.msdfilmsphotography[.]in/1711042861/login	
Dirección IP sitio falso	
[103.92.235.178]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01671-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Código de alerta	8FFR24-01672-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo, 2024
Última revisión	21 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.www-bancoripley-cl.msdfilmsphotography[.]in/1711043044/login	
Dirección IP sitio falso	
[103.92.235.178]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01672-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Código de alerta	8FFR24-01673-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo, 2024
Última revisión	21 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://mii-tarjetacencosud-cl.gulcecevre[.]com/	
Dirección IP sitio falso	
[94.199.206.206]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01673-01/	

3. Vulnerabilidades

CSIRT informa de nuevas vulnerabilidades parchadas por Cisco en IOS RX			
Código de alerta	9VSA24-00988-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	19 marzo, 2024		
Última revisión	19 marzo, 2024		
CVE			
CVE-2024-20320 CVE-2024-20327 CVE-2024-20318	CVE-2023-20236 CVE-2024-20262	CVE-2024-20315 CVE-2024-20322	CVE-2024-20266 CVE-2024-20319
Fabricante			
Cisco			
Productos afectados			
Cisco IOS XR Software SSH Privilege Escalation Vulnerability Cisco IOS XR Software for ASR 9000 Series Aggregation Services Routers PPPoE Denial of Service Vulnerability Cisco IOS XR Software Layer 2 Services Denial of Service Vulnerability Cisco IOS XR Software iPXE Boot Signature Bypass Vulnerability Cisco IOS XR Software Authenticated CLI Secure Copy Protocol and SFTP Denial of Service Vulnerability Cisco IOS XR Software MPLS and Pseudowire Interfaces Access Control List Bypass Vulnerabilities Cisco IOS XR Software DHCP Version 4 Server Denial of Service Vulnerability Cisco IOS XR Software SNMP Management Plane Protection ACL Bypass Vulnerability			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00988-01/			

CSIRT comparte información de vulnerabilidades parchadas en Google Chrome 123			
Código de alerta	9VSA24-00989-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	21 marzo, 2024		
Última revisión	21 marzo, 2024		
CVE			
CVE-2024-2625 CVE-2024-2626	CVE-2024-2627 CVE-2024-2628	CVE-2024-2629 CVE-2024-2630	CVE-2024-2631
Fabricante			
Google			
Productos afectados			
Google Chrome, todas las versiones anteriores a 123.0.6312.58/.59 para Mac y Windows, y 123.0.6312.58 para Linux.			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00989-01/			

CSIRT comparte información de vulnerabilidades parchadas en Firefox 124			
Código de alerta	9VSA24-00990-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	21 marzo, 2024		
Última revisión	21 marzo, 2024		
CVE			
CVE-2024-2605	CVE-2024-2608	CVE-2024-2610	CVE-2024-2613
CVE-2024-2606	CVE-2023-5388	CVE-2024-2611	CVE-2024-2614
CVE-2024-2607	CVE-2024-2609	CVE-2024-2612	CVE-2024-2615
Fabricante			
Mozilla			
Productos afectados			
Firefox, versiones anteriores a la 124.			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00990-01/			

4. Noticias y concientización

Ciberconsejos | Protege tu información biométrica

Tus datos biométricos son inalterables. Si los entregas sin razón, o por unas pocas monedas, podrías arrepentirte para siempre. Por eso te recomendamos que cuides tu información, en este caso no solo tus contraseñas o PIN, también elementos biométricos como tus huellas dactilares y los patrones de tus iris. Disponibles también aquí: https://csirt.gob.cl/recomendaciones/ciberconsejos-biometrica/.

Ciberconsejos | Cinco recomendaciones básicas de protección personal en ciberseguridad (III)

El tercer y final post recordatorio de los principales #ciberconsejos contenidos en "Cinco recomendaciones básicas de protección personal en #ciberseguridad" del CSIRT de Gobierno, charlas que publicamos en video y PDF aquí: https://csirt.gob.cl/noticias/ultimas-charlas-mes-de-la-ciberseguridad-2023/.

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.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.03.22 17:04:43 -03'00'