CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 202

semana del 12 al 18 de mayo de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

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

URL ADVERTIDAS

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

PARCHES COMPARTIDOS

16 Las mitigaciones son útiles en productos de Elementor (para Wordpress), Google (Chrome) y Cisco.

HASH REPORTADOS

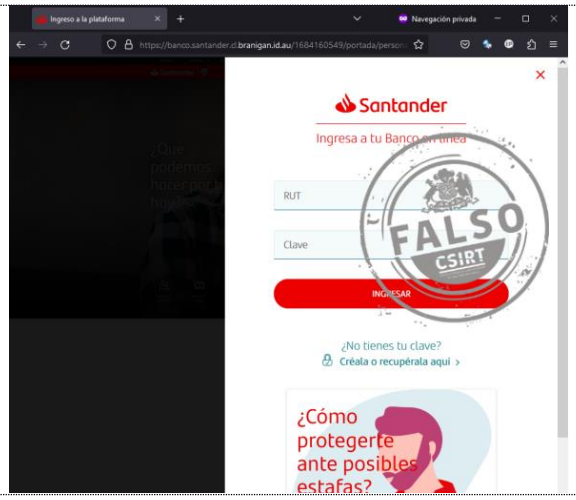
6 asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

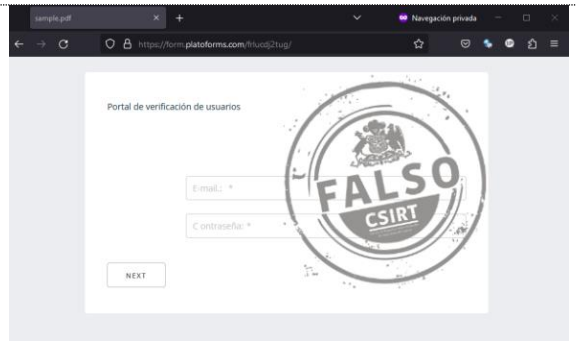
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

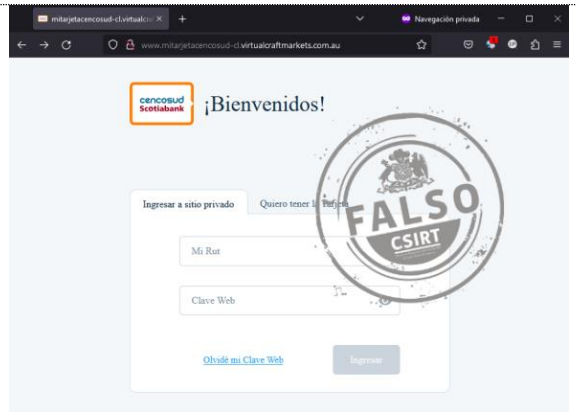
CSIRT alerta de sitio fraudulento que suplanta a Fonasa	
Alerta de seguridad cibernética	8FFR23-01320-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https://t[.]co/HkG1dGu25c https://iruccs[.]cn/u4gb8cq6/fonasa-v3/?_t=1684157041148#1684157049446	
Dirección IP	
[104.21.23.119]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01320-01	



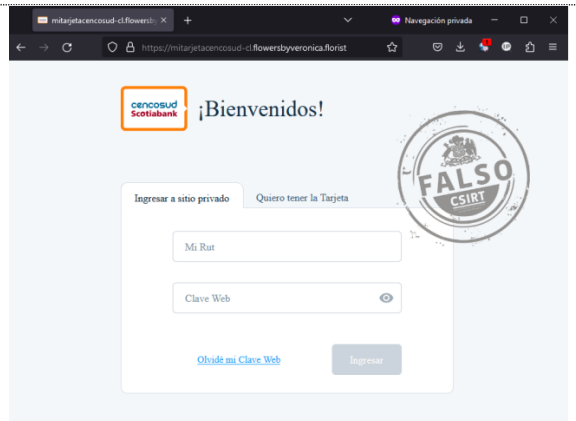
CSIRT alerta de un nuevo sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR23-01321-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//banco.santander.cl.branigan[.]id.au/1684160549/portada/personas/home.asp	
Dirección IP	
[116.0.23.203]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01321-01	



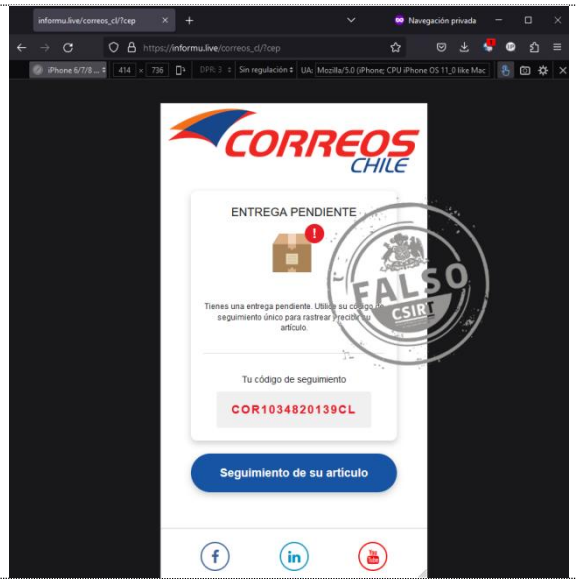
CSIRT alerta de sitio fraudulento que suplanta página de inicio de sesión de correo	
Alerta de seguridad cibernética	8FFR23-01322-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//form.platoforms[.]com/frlucdj2tug/	
Dirección IP	
[104.21.52.2]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01322-01	
CSIRT alerta de página fraudulenta que suplanta a Cencosud Scotiabank	



Alerta de seguridad cibernética	8FFR23-01323-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
http[:]//www.mitarjetacencosud-cl.virtualcraftmarkets[.]com.au/	
Dirección IP	
[103.20.202.161]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01323-01	

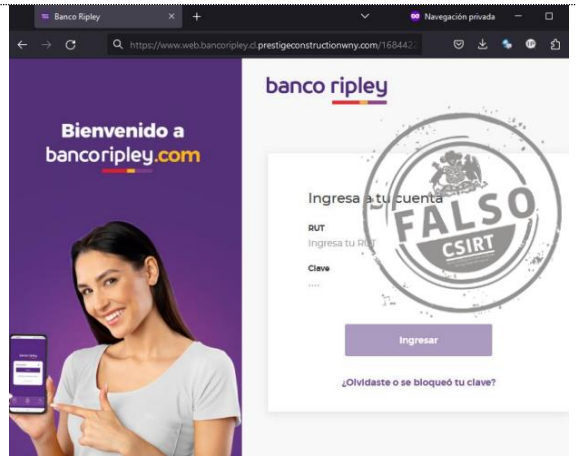


CSIRT alerta de sitio fraudulento que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FFR23-01324-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
http[:]//wordpress.zuliatec[.]com.ve/cuentas/cuenta-test/ https[:]//mitarjetacencosud-cl.flowersbyveronica[.]florist/	
Dirección IP	
[185.184.154.1]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01324-01	

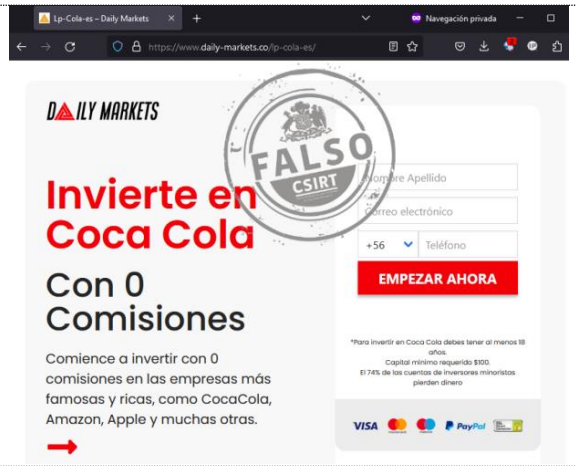


CSIRT alerta de página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01325-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2023
Última revisión	17 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
http[:]//pspa[.]me/ZE2cl4 https[:]//informu.live/correos_cl/?cep	
Dirección IP	
[93.95.227.126]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01325-01	

CSIRT alerta de sitio fraudulento que suplanta a Banco Ripley

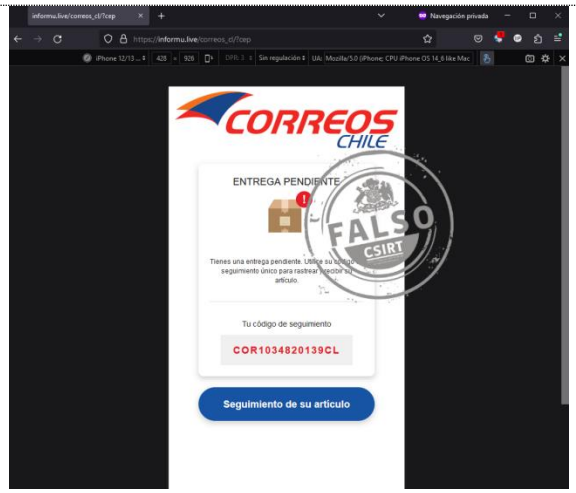


Alerta de seguridad cibernética	8FFR23-01326-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//www.web.bancoripley.cl.prestigeconstructionwny[.]com/1684422767/login	
Dirección IP	
[192.185.21.172]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01326-01	

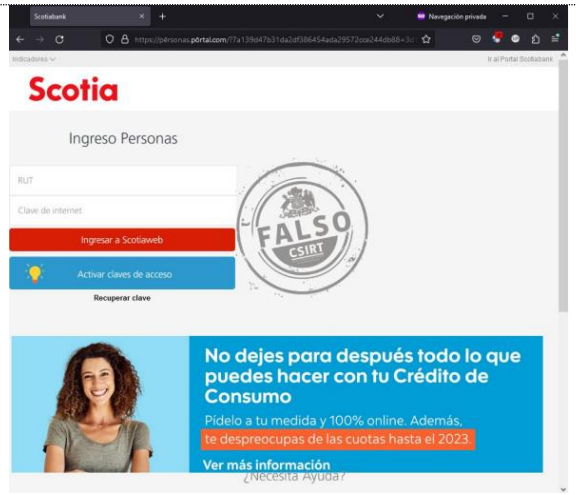


CSIRT alerta ante sitio fraudulento que suplanta a Coca-Cola	
Alerta de seguridad cibernética	8FFR23-01327-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//www.daily-markets[.]co/lp-cola-es/	
Dirección IP	
[172.67.176.187]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01327-01	

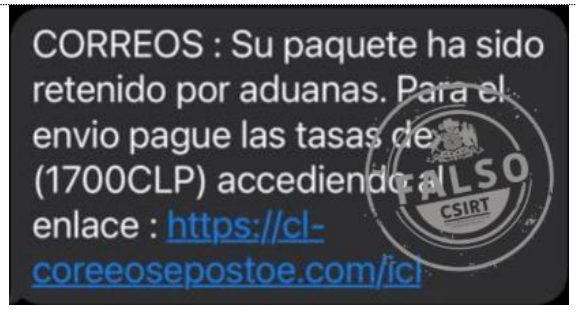
2. Phishing



CSIRT alerta de nueva campaña de phishing, que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00808-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2023
Última revisión	12 de mayo de 2023
URL redirección	
http[:]//eaaa[.]me/ZEE3Hy	
URL sitio falso	
https[:]//informu.live/correos_cl/?cep	
Dirección IP	
[93.95.227.126]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00808-01/	



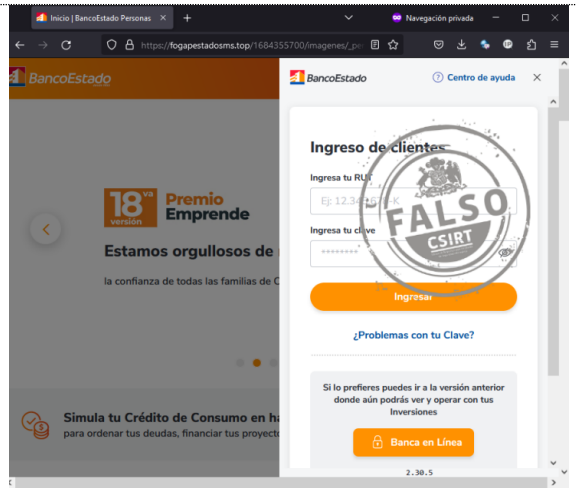
CSIRT alerta de nueva campaña de phishing, que suplanta al banco Scotia	
Alerta de seguridad cibernética	8FPH23-00809-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2023
Última revisión	12 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//qrco[.]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=OBMSXPTVMK https[:]//qrco[.]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=ISESLXOVHB	
URL redirección:	
https[:]//pērsonas.pōrtal[.]com/?7a139d47b31da2df386454ada29572cce244db88=3d1dd3a2e1ab9329b4ffc31f3d98ab92&p=login&country=CL&lang=es	
Dirección IP sitio falso	
[3.0.200.196]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00809-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00810-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https[:]//cl-coreeosepostoe[.]com/icl	
URL sitio falso	
https://cl-coreeosepostoe[.]com/cll/parcel/	
Dirección IP sitio falso	
[3.0.200.196]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00810-01/	

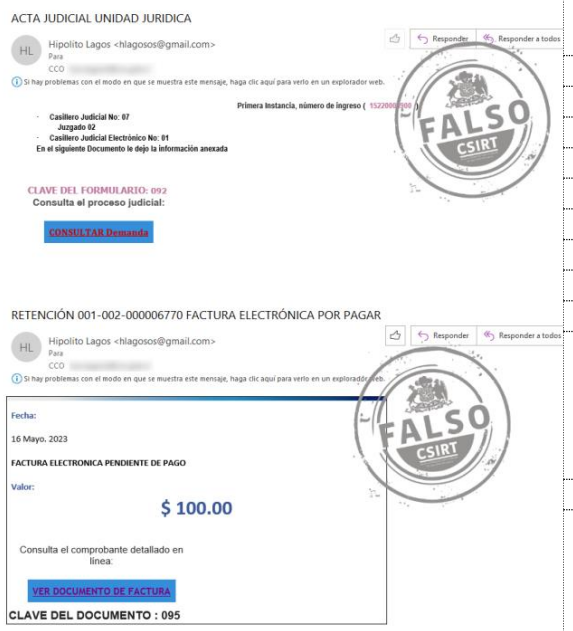
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00811-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https[:]//hopgia[.]vn/module/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//homepatitostado[.]bio/1684159549/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[172.67.202.214]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00811-01/	

CSIRT alerta de campaña de phishing por SMS que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00812-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023
Indicadores de compromiso	
URL redirección	
http[:]//jxfs[.]me/ZEWYVN	
URL sitio falso	
https[:]//informu[.]live/correos_cl?cep=	
Dirección IP sitio falso	
[93.95.227.126]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00812-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00813-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023
Indicadores de compromiso	
URL redirección	
https[:]//hopgia[.]vn/module/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//fogapestadosms[.]top/1684355700/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[172.67.140.95]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00813-01/	

3. Malware



CSIRT alerta de nueva campaña de phishing con malware, difundido via una falsa acta judicial y una supuesta retención de factura	
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	17 de mayo de 2023
Última revisión	17 de mayo de 2023
Indicadores de compromiso	
URL-Dominio	
https://acortar[.]link/NCMHbI https://acortar[.]link/zlbaw7 Iessecuador[.]con-ip.com:2434 178.237.33[.]50 186.169.64[.]87	
SHA256	
40e7707233efd5935367b041f8dbfdd5237b3efbdde7dec15ce38f1152bd6a16 e803b7421aa3bd70991445974558ef0955cc84e260222e5cac8b28a4ebb7e6b0 9a50e8852c21875b333fa210d814be7f0acc096afab6d06cc438d1ace3f42993 e803b7421aa3bd70991445974558ef0955cc84e260222e5cac8b28a4ebb7e6b0 5e908c1a0f74bc26d9f2dd21bcfb4b3ff077b39d4296763eb251889435790f78ae3 dba8130c56c7373e63b7f1b2cb0d89baa536f418173cf59a4db928d02db6e	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00413-01/	

4. Vulnerabilidades

CSIRT comparte información de una vulnerabilidad crítica que afecta al plugin Essential Addons for Elementor, de WordPress	
Alerta de seguridad cibernética	9VSA23-00832-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023
CVE	
CVE-2023-32243	
Fabricantes	
Elementor	
Productos afectados	
Plugin Essential Addons for Elementor de WordPress posteriores a la 5.4.0 y anteriores a la versión 5.7.2, que parcha la vulnerabilidad.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00832-01/	

CSIRT comparte información de vulnerabilidades parchadas en actualización a Google Chrome 113		
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	17 de mayo de 2023	
Última revisión	17 de mayo de 2023	
CVE		
CVE-2023-2721	CVE-2023-2723	CVE-2023-2725
CVE-2023-2722	CVE-2023-2724	CVE-2023-2726
Fabricantes		
Google		
Productos afectados		
Google Chrome		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00833-01/		

CSIRT comparte vulnerabilidades informadas por Cisco para varios de sus switches		
Alerta de seguridad cibernética	9VSA23-00834-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	18 de mayo de 2023	
Última revisión	18 de mayo de 2023	
CVE		
CVE-2023-20159	CVE-2023-20189	CVE-2023-20157
CVE-2023-20160	CVE-2023-20024	CVE-2023-20158
CVE-2023-20161	CVE-2023-20156	CVE-2023-20162
Fabricantes		
Cisco		
Productos afectados		
250 Series Smart Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, and 550X Series Stackable Managed Switches (fixed in firmware version 2.5.9.16). Business 250 Series Smart Switches and Business 350 Series Managed Switches (fixed in firmware version 3.3.0.16). Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches, Small Business 500 Series Stackable Managed Switches (no patch available).		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00834-01/		

5. Concientización

Ciberdiccionario Volumen 37

Con la intención de seguir sumando conceptos a nuestro Ciberdiccionario, esta semana les traemos definiciones de bot, VLAN, VoIP y lo que son las llaves pública y privada en el concepto de la criptografía. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están en: http://csirt.gob.cl/recomendaciones.

El CSIRT de Gobierno alerta ante resurgimiento de Remcos, malware difundido a través de archivos de Word

Como CSIRT de Gobierno hemos visto con mayor frecuencia, entre las campañas de phishing que detectamos, el uso del troyano Remcos, un peligroso virus informático que permite a un ciberdelincuente tomar total control del teléfono o computador de la víctima. También vemos que las campañas apuntan principalmente a empresas e instituciones públicas de nuestro país.

En vista de esta situación, y para ampliar el conocimiento de la ciudadanía respecto de las amenazas que enfrentamos en el ciberespacio, compartimos algunas de las características que hacen peligroso a Remcos, y algunas formas en que podemos evitar ser sus víctimas. Están disponibles en el siguiente enlace: https://www.csirt.gob.cl/noticias/10cnd23-00100-01/.

Ciberconsejos en el Día Mundial de Internet

El 17 de mayo se celebró el Día Mundial de las Telecomunicaciones y de la Sociedad de la Información, con el objetivo de promover el uso de Internet, dar a conocer la importancia que tienen las TIC en el mundo y disminuir la brecha digital. Para navegar seguros y evitar ser víctima de una estafa o robo de información, entregamos algunos ciberconsejos generales sobre el uso más seguro de internet: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-en-el-dia-mundial-de-internet/.

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.

- Diego Ignacio Concha de la Fuente.
- Sugy Nam.
- Juan Eduardo Báez.
- Marly Robles.
- Rigoberto Cancino.
- Marcelo Esteban Rodríguez Kong.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.19 17:42:54 -04'00'