Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

20-05-2022 | Año 4 | N°150

Boletín de Seguridad Cibernética

Semana del 13 al 19 de mayo de 2022

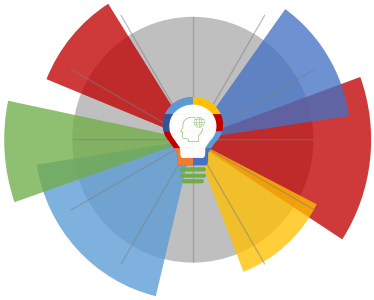
La semana en cifras

Parches

30

para vulnerabilidades

Sus mitigaciones son útiles en productos de Cisco, WordPress, VMware, Zyxel, SonicWall y Apple.



Se advirtieron

11

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

10

Informadas

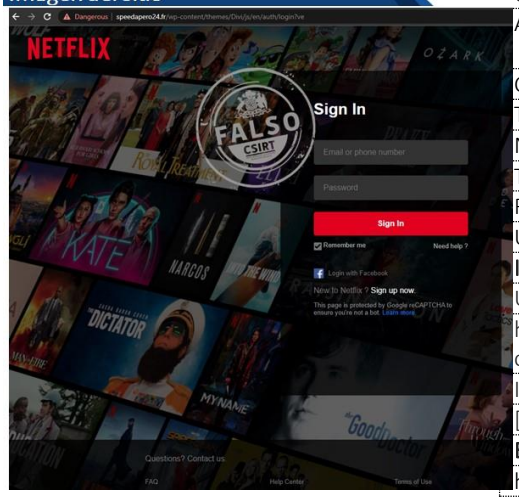
Listado de IP advertidas en múltiples campañas de phishing y de malware.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Sitios fraudulentos

Imagen del sitio



CSIRT advierte sitio falso de Netflix	
Alerta de seguridad cibernética	8FFR22-01082-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2022
Última revisión	29 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.speedapero24[.]fr/wp-content/themes/Divi/js/en/auth/login?ve	
IP	
[46.105.57.169]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01082-01/	
https://www.csirt.gob.cl/media/2022/05/8FFR22-01082-01.pdf	

Phishing

CSIRT advierte phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH22-00526-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de mayo de 2022
Última revisión	13 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
https://meatwhirl[.]com/cl/CPOST	
IP	
[94.182.146.253]	
[162.243.174.217]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00526-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00526-01.pdf	

CSIRT informa phishing que suplanta a Chilexpress	
Alerta de seguridad cibernética	8FPH22-00527-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2022
Última revisión	16 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/	
URL sitio falso	
hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[77.73.69.166]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00527-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00527-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00528-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
https://bit[.]ly/3wpolWy?l=www.bancoripley.cl	
http://luxeoconcept[.]com/wp-includes/certificates/enviar02.php?l=461885427	
https://zakajy[.]kz/activacion/cuenta-rbqj/	
https://www-bancoripley-cl.msdfilmsphotography[.]in/1652978613/login	
IP	
[185.21.117.20]	
[103.92.235.178]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00528-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00528-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00529-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
https://bamco-sanfander.cl-newra[.]buzz	
IP	
[64.44.101.173]	
[104.21.86.159]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00529-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00529-01.pdf	

Imagen del mensaje

CSIRT alerta phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00530-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
Indicadores de compromiso	
URL sitio redirección	
https://gestionvalpa[.]net/activacion/cuenta-wreo/	
URL sitio falso	
https://sgetyw.tarabgin[.]ir/bsgre/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.121.148]	
[185.51.202.58]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00530-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00530-01.pdf	

Vulnerabilidades

CSIRT alerta de nueva vulnerabilidad de día cero en productos Apple	
Alerta de seguridad cibernética	9VSA22-00638-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2022
Última revisión	16 de mayo de 2022
CVE	
CVE-2022-22675	
Fabricante	
Apple	
Productos afectados	
Macs con sistema operativo macOS Big Sur anteriores al 11.6. Apple Watch Series 3 o posteriores, con sistema operativo watchOS anteriores al 8.6. Apple TV HD y 4K de segunda generación, con sistemas operativos anteriores a tvOS 15.5.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00638-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00638-01.pdf	

CSIRT alerta vulnerabilidades en aparatos SonicWall SMA1000	
Alerta de seguridad cibernética	9VSA22-00639-01
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 2022
Última revisión	17 de mayo de 2022
CVE	
CVE-2022-22282 CVE-2022-1701 CVE-2022-1702	
Fabricante	
SonicWall	
Productos afectados	
Serie SMA1000 firmware versiones 12.4.0, 12.4.1-02965 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00639-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00639-01-1.pdf	

CSIRT alerta ante vulnerabilidad crítica que afecta dispositivos Zyxel	
Alerta de seguridad cibernética	9VSA22-00640-01
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 2022
Última revisión	17 de mayo de 2022
CVE	
CVE-2022-30525	
Fabricante	
Zyxel	
Productos afectados	
USG FLEX 100(W), 200, 500, 700, versiones firmware ZLD V5.00 a ZLD V5.21 Patch 1. USG FLEX 50(W) USG20(W)-VPN, versiones firmware ZLD V5.10 a ZLD V5.21 Patch 1. ATP series, versiones firmware ZLD V5.10 a ZLD V5.21 Patch 1. VPN series, versiones firmware ZLD V4.60 through ZLD V5.21 Patch 1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00640-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00640-01.pdf	

CSIRT alerta de vulnerabilidades en productos VMware	
Alerta de seguridad cibernética	9VSA22-00641-01
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 2022
Última revisión	17 de mayo de 2022
CVE	
CVE-2022-22972 CVE-2022-22973	
Fabricante	
VMware	
Productos afectados	
VMware Workspace ONE Access (Access) VMware Identity Manager (vIDM) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manager	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00641-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00641-01.pdf	

CSIRT alerta de dos vulnerabilidades en plugins de WordPress	
Alerta de seguridad cibernética	9VSA22-00642-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
CVE	
CVE-2022-1654 CVE-2021-25094	
Fabricante	
WordPress	
Productos afectados	
Jupiter y Jupiter X Core. Tatsu Builder.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00642-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00642-01.pdf	

CSIRT informa sobre vulnerabilidades en productos de Cisco	
Alerta de seguridad cibernética	9VSA22-00641-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
CVE	
CVE-2022-20797 - CVE-2022-20806 - CVE-2022-20807 CVE-2022-20809 - CVE-2022-20802 - CVE-2022-20666 CVE-2022-20667 - CVE-2022-20668 - CVE-2022-20765 CVE-2022-20759 - CVE-2022-20681 - CVE-2022-20677 CVE-2022-20718 - CVE-2022-20719 - CVE-2022-20720 CVE-2022-20721 - CVE-2022-20722 - CVE-2022-20723 CVE-2022-20724 - CVE-2022-20725 - CVE-2022-20726 CVE-2022-20727	
Fabricante	
Cisco	
Productos afectados	
Cisco Secure Network Analytics anteriores a 7.4.1. Cisco Expressway Series y Cisco TelePresence VCS 14.0 y anteriores. Cisco Enterprise Chat and Email (ECE) anteriores a 12.6(1) ES2. Cisco CSPC 2.10.0.2 y anteriores. Cisco ASA software anteriores a 9.12.4.38, 9.14.4, 9.15.1.21, 9.16.2.14 y 9.17.7. Cisco FMC y FTD software anteriores a 6.4.0.15, 6.6.5.2, 7.0.2 y 7.1.0.1. 800 Series Industrial Integrated Services Routers (Industrial ISRs)	

800 Series Integrated Services Routers (ISRs) 1000 Series Connected Grid Router (CGR1000) Compute Modules IC3000 Industrial Compute Gateways Industrial Ethernet (IE) 4000 Series Switches IOS XE-based devices configured with IOx IR510 WPAN Industrial Routers
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00643-01/
https://www.csirt.gob.cl/media/2022/05/9VSA22-00643-01.pdf

Actualidad

Uso de vulnerabilidades en Active Directory como vector del ransomware Conti en ataques con troyano Emotet

El CSIRT de Gobierno insta a los encargados de ciberseguridad del país a implementar los parches publicados por Microsoft para dos vulnerabilidades (CVE-2021-42278 y CVE-2021-42287) dadas a conocer en la actualización mensual de la compañía (conocidas como "Update Tuesday") correspondiente a noviembre de 2021, la cual también fue en su momento publicada por el CSIRT de Gobierno en nuestro sitio web: https://csirt.gob.cl/vulnerabilidades/9vsa21-00519-01/

Ambas vulnerabilidades permiten el escalamiento de privilegios en Active Directory, y están siendo aprovechadas por ciberdelincuentes en Chile y otros países de Latinoamérica para inyectar el ransomware Conti, usando como vector al troyano Emotet.

Por lo anterior, es clave que no solo ambas vulnerabilidades sean parchadas a la brevedad, sino que el parchado de vulnerabilidades sea realizado regularmente y cuan pronto como sea posible luego de que estas sean dadas a conocer. Por nuestra parte, compartimos regularmente las vulnerabilidades más relevantes en https://www.csirt.gob.cl/vulnerabilidades/

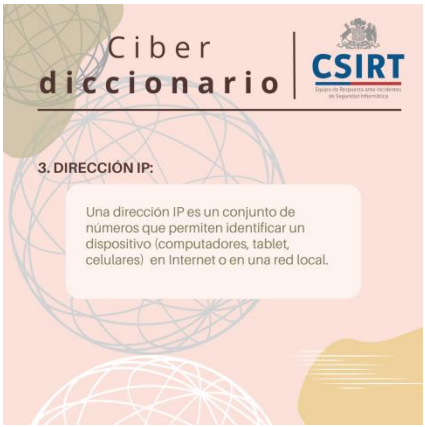
Día Mundial de Internet: Hitos de la llegada de internet a Chile

El 17 de mayo se celebra el Día Mundial de Internet (oficialmente "Día Mundial de las Telecomunicaciones y de la Sociedad de la Información"), que tiene como fin promover el uso de Internet, dar a conocer la importancia que tienen las TIC en el mundo y disminuir la brecha digital.

Internet comienza su historia en nuestro país a mediados de los años 80, con el envío del primer correo electrónico. Desde entonces, su evolución y crecimiento en Chile ha dependido de una serie de eventos cruciales, los que detallamos como CSIRT de Gobierno y que pueden leer también aquí: https://www.csirt.gob.cl/recomendaciones/dia-mundial-de-internet/.

Ciberdiccionario Volumen 6

El CSIRT de Gobierno comparte el volumen n°6 del Ciberdiccionario. En esta ocasión, explicamos en qué consisten los ataques de DDoS, Servicio de Nombre de Dominio (DNS), direcciones IP y HTTP. Pueden encontrarlo también aquí: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-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 los sitios web que se ingresen sean los oficiales.

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Catalina Caimanque
- Rubén Contreras
- Rachel Tapia
- Javier Martínez
- Cristián Arancibia
- Carlos Aguirre
- Elena Jerez
- Carlos Arriagada
- Cristián Chávez
- Juan Pablo Berríos
- Cristián Acuña
- Carlos Escalona
- Andrés Sepúlveda