Ministerio del Interior y Seguridad Pública

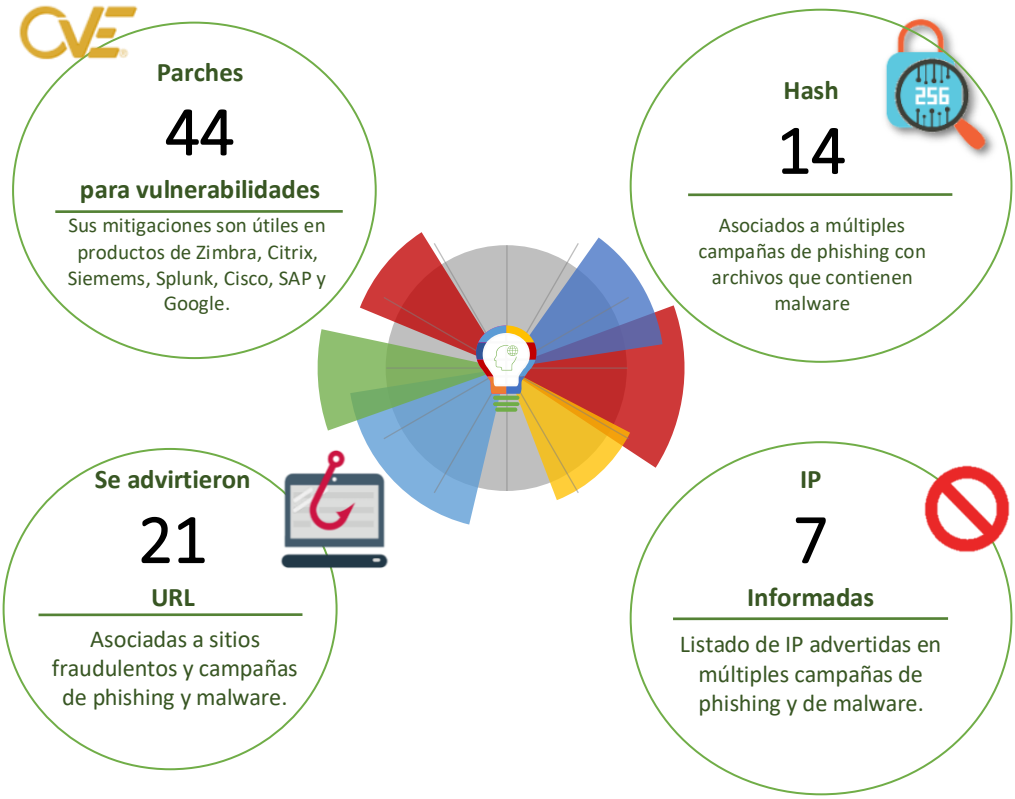
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

24-06-2022 | Año 4 | N°155

Boletín de Seguridad Cibernética

Semana del 17 al 23 de junio de 2022

La semana en cifras



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

Contenido

Malware

Imagen del mensaje

CSIRT advierte campaña de phishing con adjuntos que contienen malware	
Alerta de seguridad cibernética	2CMV21-00302-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022

Indicadores de compromiso

SHA256

Archivos que se encuentran en la amenaza

Nombre: documentación_14.zip
SHA256:
c3eaa48c45bb24774a2851df1b8bd72d239ab1be6ff8542ff65e8e53c72401a8
Nombre: documentación_14.xls
SHA256:
f9e265a7660e3d54b12c9ec9b7f9aff04e1217e705ae7c69809caf44170261b1
Nombre: tsGnq2vvf0l7ld5yVHYmlXyDn.dll
SHA256:
2b8d3693b5919bc17bda4da2a38afecd326e353e6d88ea1d3d99c1746d163ad9
Nombre: LXSdVoxctiTcU84j1SfqItxnM1Gbbxjb.dll
SHA256:
9b7d07a747c11957bd3bac5236dc8317ad9feb84cfb81ca6c8cbb0e7a548c20e
Nombre: mHJp0RsXn5l204BGHsgPJxqWZ4Y.dll
SHA256:
efac2bbbedb0ce1d4170d184ca471897f57eb8fc3d92ec253c9dafb4aeddb2ae
Nombre: 7PmU5TR2yOZ.dll
SHA256:
529d70448ed5cdc0e6bb89432214e880bd53f3fc2ea9117f5a9f9262d5bdd852

Otros IoC en relación a la amenaza

001d8f7352fd43acf6f276d72571cac4548b540376bbf847036fdbf0e9ce10db
004f0dd54445f9f6c5fe3008bfa719dbd80d5d12e70d8d8ad562b6aae5bee207
016b2d6b86488f15baeba646286aca46566f5cf3d4e787a3cb03af8af99fb2bf
02db3b7e6c7eeff23217a73a9672e84edbc0defac0104881804f4cf41c20ae0a
04e0e78e22e7d486960861504e9c6c1306a698d7944c4a541d87cf47e470885e
1edc6f712e2d7670f8ec65f6f03e3ebb0ab8b59f861cd48ba0f382f2daf2e750
2b8d3693b5919bc17bda4da2a38afecd326e353e6d88ea1d3d99c1746d163ad9
2e53404f8f2098e8608b46ccb485caacc404b12ea0c7f49e405faa714e3ce53

IoC URL

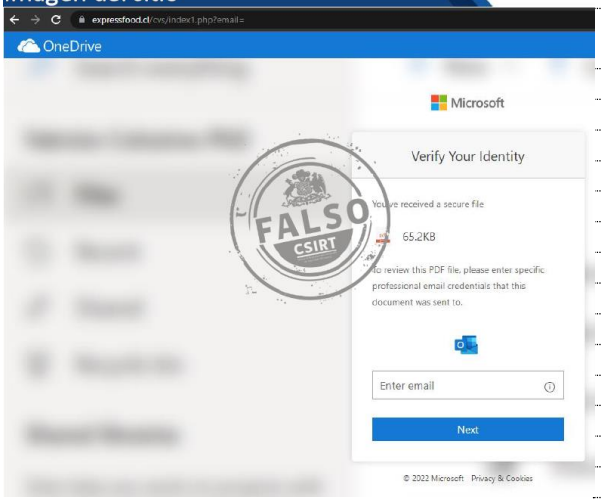
upscalifornia[.]us
yourbankruptcypartner[.]com
webbandi[.]hu
com[.]mx
http://upscalifornia[.]us/libraries/VDu9kaMu/
http://ftp.yourbankruptcypartner[.]com/wp-content/ksdtjfFji/
http://webbandi[.]hu/image/m7IzjWQftQ1Jyw6/
http://zarzamora.com[.]mx/cgi-bin/hAuGj65SuKr

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-0302-01/
https://www.csirt.gob.cl/media/2022/06/2CMV22-00302-01.pdf

Sitios fraudulentos

Imagen del sitio



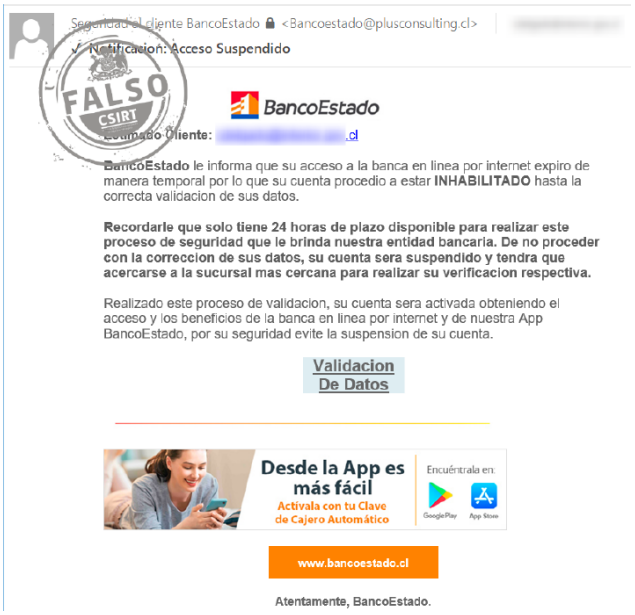
CSIRT informa de sitio web falso que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01089-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de junio de 2022
Última revisión	23 de junio de 2022
Indicadores de compromiso	
URL sitio falso	
https://expressfood[.]cl/cvs/index1.php?email=	
IP	
[162.214.114.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01089-01/	
https://www.csirt.gob.cl/media/2022/06/8FFR22-01089-01.pdf	

Phishing

Imagen del sitio

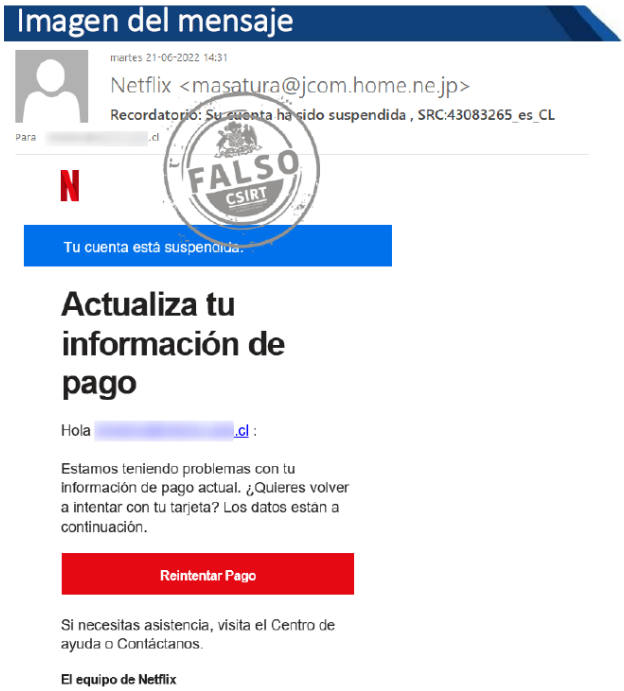
CSIRT advierte phishing con falso IFE laboral disponible	
Alerta de seguridad cibernética	8FPH22-00542-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3zBhhrK	
URL sitio falso	
https://app.cl-estado[.]ru/uuGqCWpRwBVk987Qm7evpdvdN/Imaggeness/comun2008/banca-en-linea-personas.html	
IP	
[104.21.76.201]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00542-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00542-01.pdf	

Imagen del mensaje



CSIRT advierte phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00543-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://anticontaweb[.]com/activacion/cuenta-nzvd/	
URL sitio falso	
https://comuntrans[.]info/procard/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[192.141.51.210]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00543-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00543-01.pdf	

CSIRT informa phishing con falsa cuenta bloqueada	
Alerta de seguridad cibernética	8FPH22-00544-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
Indicadores de compromiso	
URL Redirección	
http://asedl[.]am/Servicio_Estado/cuenta-iddb/	
URL sitio falso	
https://sixthstartech[.]com/Conoce/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[101.53.141.67]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00544-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00544-01.pdf	



CSIRT alerta de phishing que suplanta a Netflix	
Alerta de seguridad cibernética	8FPH22-00545-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2022
Última revisión	22 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://qrco[.]de/63a2a3e25620f5e43a74d4c9a2e13401bf4a7f6b?fbid=8A7AB20EC0AB3262CE329C7DCB399A4E	
URL sitio falso	
https://reactiva.netflix.obcfrs[.]com/CL-es/signin.php?cmd=_update-information&account_update=13b29965a7b6fedfa9dbc58d893bc740&lim_session=99eac1d2641b8c49bf5ee03559a038f4f6302cd9	
IP	
[20.2.82.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00545-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00545-01.pdf	

CSIRT alerta phishing con falsa cuenta inhabilitada	
Alerta de seguridad cibernética	8FPH22-00546-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de junio de 2022
Última revisión	23 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://menheadpro[.]com/ganador2/cuenta-uwnh/	
URL sitio falso	
https://judge2wincamp[.]com/1655998529/Login	
IP	
[198.12.225.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00546-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00546-01.pdf	

CSIRT alerta phishing con falsa cuenta inhabilitada	
Alerta de seguridad cibernética	8FPH22-00547-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de junio de 2022
Última revisión	23 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://cutt[.]ly/sKpM0b2 https://gocloudasiaacademe[.]com/	
URL sitio falso	
https://login.acceso-bancochlle.cl.luisorlandini[.]cl/1656013825/bcochile-web/persona/login/index.html/login	
IP	
[200.63.97.55]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00547-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00547-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidad en Zimbra	
Alerta de seguridad cibernética	9VSA22-00659-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
CVE	
CVE-2022-27924	
Fabricante	
Zimbra	
Productos afectados	
Zimbra 8.8.x y 9.x, versiones open source y comerciales.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00659-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00659-01.pdf	

CSIRT alerta de vulnerabilidad en Citrix ADM	
Alerta de seguridad cibernética	9VSA22-00660-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
CVE	
CVE-2022-27511	
Fabricante	
Citrix	
Productos afectados	
Citrix Application Delivery Management (ADM): Citrix ADM 13.0 anteriores al 13.0-85.19 y Citrix ADM 13.1 anteriores al 13.1-21.53	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00660-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00660-01.pdf	

CSIRT advierte de vulnerabilidad crítica en Splunk Enterprise	
Alerta de seguridad cibernética	9VSA22-00660-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022
CVE	
CVE-2022-32158	
Fabricante	
Splunk	
Productos afectados	
Splunk Enterprise anteriores a la versión 9.0. La Splunk Cloud Platform (SCP) no es afectada por esta vulnerabilidad.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00660-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00660-01.pdf	

CSIRT alerta ante vulnerabilidades en Siemens SINEC NMS		
Alerta de seguridad cibernética	9VSA22-00662-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	20 de junio de 2022	
Última revisión	20 de junio de 2022	
CVE		
CVE-2021-33722	CVE-2021-33727	CVE-2021-33732
CVE-2021-33723	CVE-2021-33728	CVE-2021-33733
CVE-2021-33724	CVE-2021-33729	CVE-2021-33734
CVE-2021-33725	CVE-2021-33730	CVE-2021-33735
CVE-2021-33726	CVE-2021-33731	CVE-2021-33736
Fabricante		
Siemens		
Productos afectados		
Siemens SINEC NMS, todas las versiones anteriores a la V1.0 SP2 Update 1.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00662-01/		
https://www.csirt.gob.cl/media/2022/06/9VSA22-00662-01.pdf		

CSIRT alerta de nuevas vulnerabilidades en productos de Cisco	
Alerta de seguridad cibernética	9VSA22-00663-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2022
Última revisión	20 de junio de 2022

CVE		
CVE-2022-20798 CVE-2022-20825 CVE-2022-20664	CVE-2022-20819 CVE-2022-20817	CVE-2022-20736 CVE-2022-20733

Fabricante
Cisco

Productos afectados
Cisco Secure Email and Web Manager, Cisco Email Security Appliance Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Cisco Identity Services Engine (ISE) Teléfonos Cisco Unified IP Cisco AppDynamics Controller Software

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00663-01/
https://www.csirt.gob.cl/media/2022/06/9VSA22-00663-01.pdf

CSIRT advierte de vulnerabilidades en productos SAP	
Alerta de seguridad cibernética	9VSA22-00664-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2022
Última revisión	22 de junio de 2022

CVE		
CVE-2022-27668 CVE-2022-31590 CVE-2022-29611 CVE-2022-29618	CVE-2022-29612 CVE-2022-31589 CVE-2022-31595	CVE-2022-29614 CVE-2022-29615 CVE-2022-31594

Fabricante
SAP

Productos afectados
SAP NetWeaver y ABAP Platform, Versions -KERNEL 7.49 a 7.88, 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22 SAP PowerDesigner Proxy 16.7, Versions -16.7High7.8 SAP NetWeaver Application Server for ABAP and ABAP Platform,Version -700 a 788 SAP 3D Visual Enterprise Viewer, Version -9.0 SAP NetWeaver Development Infrastructure (Design Time Repository), Versions -7.30, 7.31, 7.40, 7.50

SAP NetWeaver, ABAP Platform and SAP Host Agent, Versions -KERNEL 7.22, a 8.04, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, 8.04, SAPHOSTAGENT 7.22 SAPERP, localization forCEEcountries, Versions -C-CEE110_600, 110_602, 110_603, 110_604, 110_700 SAP Financials, Versions -SAP_FIN 618, 720 SAP S/4Hana Core, Versions -S4CORE 100 a 108 SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53 SAP NetWeaverASABAP,ASJava, ABAP Platform and HANA Database, Versions -KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, SAPHOSTAGENT 7.2 SAP NetWeaver Developer Studio (NWDS), Versions -7.50 SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53Low3.2
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00664-01/
https://www.csirt.gob.cl/media/2022/06/9VSA22-00664-01-1.pdf

CSIRT alerta de nuevas vulnerabilidades en Google Chrome		
Alerta de seguridad cibernética	9VSA22-00665-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	22 de junio de 2022	
Última revisión	22 de junio de 2022	
CVE		
CVE-2022-2156	CVE-2022-2160	CVE-2022-2163
CVE-2022-2157	CVE-2022-2161	CVE-2022-2164
CVE-2022-2158	CVE-2022-2162	CVE-2022-2165
Fabricante		
Google		
Productos afectados		
Chrome 102, actualizar a Chrome 103 (Chrome 103.0.5060.53).		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00665-01/		
https://www.csirt.gob.cl/media/2022/06/9VSA22-00665-01.pdf		

Actualidad

La nueva Ley de Delitos Informáticos entró en vigor

Esta semana ha entrado en vigor la nueva Ley de Delitos Informáticos, legislación que reemplaza a la existente desde 1993 en búsqueda de una mejor adaptación a los tiempos que corren.

Nota completa:
https://www.csirt.gob.cl/noticias/nueva-ley-de-delitos-informaticos-entro-en-vigor/

Se trata de la Ley N° 21.459, «que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest», su denominación oficial. Como su nombre lo indica, se buscó actualizar los tipos legales y facilitar la persecución de los delitos informáticos a través de las fronteras internacionales.

Pueden encontrar la ley en PDF como apareció publicada en el Diario Oficial, aquí: https://www.diariooficial.interior.gob.cl/publicaciones/2022/06/20/43283/01/2145558.pdf.

DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 43.283 | Lunes 20 de Junio de 2022 | Página 1 de 5

Normas Generales

CVE 2145558

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

LEY NÚM. 21.459

ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

"TÍTULO I
DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1°.- Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Artículo 2°.- Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Artículo 4°.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

CVE 2145558 | **Director Interino: Jaime Sepúlveda O.** | **Mesa Central:** 600 712 0001 | **Email:** consultas@diariooficial.cl
Sitio Web: www.diariooficial.cl | **Dirección:** Dr. Torres Boonen N°511, Providencia, Santiago, Chile

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

El Control del Mes | No. 20 Aseguramiento de servicios de aplicación en redes públicas

Regresó el antiguo Control de la Semana, aunque ahora con periodicidad mensual. En esta ocasión presentamos la Ficha de Control Normativo A.14.1.2. «Aseguramiento de servicios de aplicación en redes públicas». Aquí: csirt.gob.cl/estadisticas/el-control-del-mes-no-20-aseguramiento-de-servicios-de-aplicacion-en-redes-publicas/.

Ciberconsejos | Cómo protegernos contra los stealers

Un tipo de programa malicioso (malware) dedicado a robar nuestra información es el conocido como stealer o infostealer. En los ciberconsejos de esta semana te mostramos cómo trabajan estos programas y cómo prevenir su accionar en nuestros celulares y computadores.

La nota aquí: https://www.csirt.gob.cl/recomendaciones/actualizacion/

Ciberdiccionario Volumen 9

Esta semana explicamos qué son los red team y blue team, las vulnerabilidades zero day o día cero, los captcha y Malware as a Service: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-9/.

Especialista del CSIRT Sabina Torres entrevistada en TrendTIC Live

"Análisis de vulnerabilidades y desarrollo seguro de proyectos" fue el tema de la conversación de nuestra especialista del área de Vulnerabilidades Sabina Torres con Pablo Antillanca, conductor de TrendTIC Live. Revisa la entrevista, aquí: https://www.youtube.com/watch?v=9jB193XKHCo

Hernán Espinoza, asesor especialista en el CSIRT de Gobierno, participa en conversatorio de la Cybersecurity Week Conference 2022 Usach

Espinoza fue parte de un panel titulado "Desafíos de los Equipos de Respueta a Insidentes" del Diplomado Blue Team de la Universidad de Santiago de Chile (Usach).

Pueden ver la participación de Hernán aquí: https://www.youtube.com/watch?v=pf4hDJfNI_Y.

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 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Carolina Isabel Correa Fenick
- César
- Dina Silva Castillo
- Marina Becerra
- Sofía Soledad Zaravia Matamala
- Carlos Aguirre
- Rodrigo Gallardo Flores
- Pablo Araya del Pino
- Matías González
- Alexis Bustos
- Jorge Romero Arancibia