Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

03-09-2021 | Año 3 | N°113

Boletín de Seguridad Cibernética

Semana del 27 de agosto y el 3 de septiembre de 2021

La semana en cifras

Hash

4

SHA

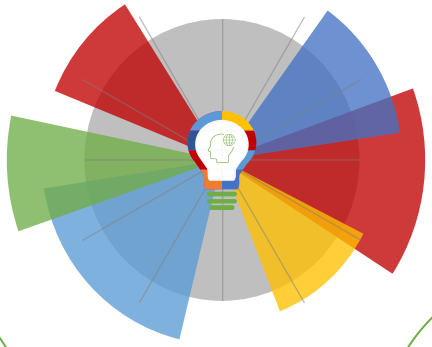
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

53

para vulnerabilidades

Las mitigaciones son útiles en productos de F5, Cisco y Red Hat.

IP

3

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.

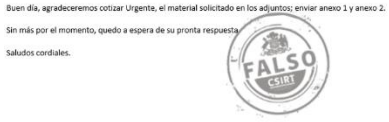
Contenido

Malware

Imagen del Mensaje

CSIRT alerta ante una nueva campaña de malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00218-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
SHA256	
CD2D7D1B1ACA9FC007E2911B8A44F2768056F4D532598E56EF1554B3D9F12D2C 4A0561537D58605334FAB6DDF66EB0140D9CFCE0B50C80338DD810511E519A28	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00218-01/	
https://csirt.gob.cl/media/2021/09/2CMV21-00218-01.pdf	

Imagen del Mensaje



CSIRT alerta ante campaña de malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00219-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
SHA256	
FEF392F98572CB50481B1A5613927743A2BD4C5E3B0F13844E52908564638A97 9828BFE3D475FCC606327F7F3340CE2BDABE44A5A5866903DAA21EE931F0FD42	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00219-01/	
https://csirt.gob.cl/media/2021/09/2CMV21-00219-01.pdf	

Sitios fraudulentos

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01009-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://5antand3r[.]xyz/1630675052/personas/index.asp	
IP	
[68.65.120.250]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01009-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01009-01.pdf	

Imagen del sitio

CSIRT alerta ante una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01010-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://santander.bancapersonas[.]xyz/1630675134/personas/index.asp	
IP	
[198.54.115.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01010-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01010-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante campaña de smishing que suplanta al banco Itaú	
Alerta de seguridad cibernética	8FPH21-00430-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de septiembre de 2021
Última revisión	2 de septiembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/38GLsb	
URL sitio falso	
https://it4ualertta[.]xyz/1630597935/bancochile-web/persona/login/index.html/login	
IP	
[162.213.255.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00430-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00430-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades graves en BIG-IP y BIG-IQ de F5	
Alerta de seguridad cibernética	9VSA21-00485-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2021
Última revisión	31 de agosto de 2021
CVE	
CVE-2021-23025 CVE-2021-23026 CVE-2021-23027 CVE-2021-23028 CVE-2021-23029 CVE-2021-23030 CVE-2021-23031 CVE-2021-23032 CVE-2021-23033 CVE-2021-23034 CVE-2021-23035 CVE-2021-23036 CVE-2021-23037 CVE-2021-23038 CVE-2021-23039 CVE-2021-23040 CVE-2021-23041 CVE-2021-23042 CVE-2021-23043 CVE-2021-23044 CVE-2021-23045 CVE-2021-23046 CVE-2021-23047 CVE-2021-23048 CVE-2021-23049 CVE-2021-23050 CVE-2021-23051 CVE-2021-23052 CVE-2021-23053	
Fabricante	
F5	
Productos afectados	
BIG-IP (todos los módulos) BIG-IP APM BIG-IQ	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00485-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00485-01.pdf	

CSIRT alerta de vulnerabilidades en productos de Red Hat	
Alerta de seguridad cibernética	9VSA21-00486-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2021
Última revisión	31 de agosto de 2021
CVE	
CVE-2020-8564 CVE-2021-2341 CVE-2021-2369 CVE-2021-2432 CVE-2021-3246 CVE-2021-31535	
Fabricante	
Red Hat	
Productos afectados	
Red Hat Enterprise Linux 8.1 Red Hat Enterprise Linux 8.2 Red Hat Enterprise Linux 7 Red Hat OpenShift Container Platform: 3.11.0 a 3.11.487 java-1.7.1-ibm (Red Hat package): 1.7.1.4.70-1jpp.1.el7, 1.7.1.4.75-1jpp.1.el7, 1.7.1.4.80-1jpp.1.el7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00486-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00486-01.pdf	

CSIRT alerta ante vulnerabilidades graves en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00487-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de agosto de 2021
Última revisión	26 de agosto de 2021
CVE	
CVE-2019-1727 CVE-2021-1518 CVE-2021-1578 CVE-2021-1579 CVE-2021-1580 CVE-2021-1581 CVE-2021-1582 CVE-2021-1587 CVE-2021-1588 CVE-2021-1590 CVE-2021-1591 CVE-2021-1592 CVE-2021-22156	

CVE-2021-34732 CVE-2021-34733 CVE-2021-34746 CVE-2021-34759 CVE-2021-34765
Fabricante
Cisco
Productos afectados
Cisco Nexus 9500 Series. Cisco UCS 6400 Series Fabric Interconnects si están corriendo una version vulnerable del Cisco UCS Manager software. Nexus 3000 Series Switches, Nexus 7000 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, si corren una version vulnerable de Cisco NX-OS y tienen la función MPLS OAM activada. Nexus 3000 Series Switches y Nexus 9000 Series Switches si corren una version vulnerable de Cisco NX-OS y tienen la función NGOAM activada. QNX SDP 6.5.0SP1 y anteriores, QNX OS for Medical 1.1 y anteriores y QNX OS for Safety 1.0.1 y anteriores Cisco Nexus Insights. Cisco Identity Services Engine (ISE) Cisco Prime Collaboration Provisioning Cisco Prime Infrastructure Cisco Evolved Programmable Network Manager Cisco Enterprise NFV Infrastructure Software (NFVIS) Cisco Firepower Device Manager (FDM) Cisco NX-OS Software Cisco Application Policy Infrastructure Controller (APIC) Cisco Cloud APIC
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00487-01
https://www.csirt.gob.cl/media/2021/09/9VSA21-00487-01.pdf

Actualidad

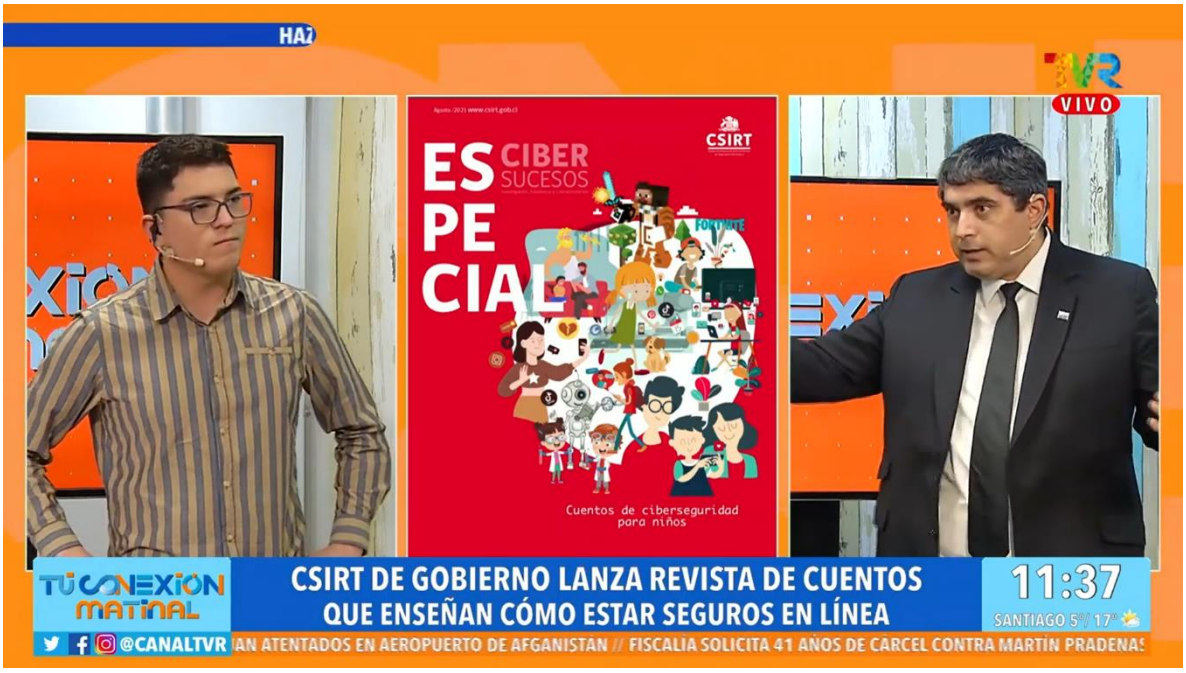
Gobierno presenta proyecto de ley para crear el Ministerio de Seguridad Pública, que incorpora a la futura Agencia Nacional de Ciberseguridad

El Presidente de la República, Sebastián Piñera, acompañado de los Ministros del Interior y Seguridad Pública, Rodrigo Delgado, y de Justicia y Derechos Humanos, Hernán Larraín, presentó el proyecto de ley que busca crear el Ministerio de Seguridad Pública. A la ceremonia también asistieron el General Director de Carabineros, Ricardo Yáñez, y el Director General de la Policía de Investigaciones (PDI), Sergio Muñoz, y los subsecretarios del Interior, Juan Francisco Galli, y de Prevención del Delito, María José Gómez.

El proyecto pone bajo dependencia jerárquica de este nuevo ministerio a Carabineros y la PDI, además de la futura Agencia Nacional de Ciberseguridad. Con él, además, colaborará la Agencia Nacional de Inteligencia (ANI), cuando se trate de materias de seguridad pública. Todas estas instituciones deben funcionar como un sistema de seguridad pública, explicó el Presidente.

De acuerdo con el Jefe de Estado, la creación de este nuevo ministerio busca "alejar la figura del ministro jefe de gabinete de las contingencias propias de la seguridad pública, otorgándole en consecuencia mayor estabilidad política y permitiendo un enfoque específico y técnico en materia de seguridad que no pugne con las urgencias políticas propias del Ministerio del Interior". El nuevo ministerio comprenderá dos subsecretarías: de Seguridad Pública y de Prevención del Delito.

Director del CSIRT de Gobierno presenta cuentos de ciberseguridad para niños en Tu Conexión Matinal de TVR



El último viernes de agosto el director nacional del CSIRT de Gobierno, Carlos Landeros, asistió a la invitación que hizo Tu Conexión Matinal del canal TVR (22 en televisión abierta, https://www.tvr.cl para su streaming en línea), para compartir con la comunidad los cuentos de ciberseguridad para niños, niñas y adolescentes que escribió el propio personal del CSIRT (y que pueden leer aquí: https://www.csirt.gob.cl/recomendaciones/cibersucesos-especial-cuentos-mes-del-nino/).

En el programa, Landeros explicó la importancia de educar a nuestros niños, niñas y adolescentes para que conozcan los riesgos de internet y cómo evitarlos, anticipándose a los delitos y riesgos que acechan en el mundo online.

El video: https://www.youtube.com/watch?v=jNb6vLEWWbw&.

Pueden encontrar más información en csirt.gob.cl/noticias/director-del-csirt-de-gobierno-presenta-cuentos-de-ciberseguridad-para-ninos-en-tu-conexion-matinal-de-tvr/.

Ciberconsejos | El riesgo que suponen los keyloggers, espías que pueden infectar nuestros dispositivos

Un keylogger puede suponer tal pérdida de privacidad y riesgos para el usuario, que debemos conocer cómo funcionan y en qué fijarse para no ser víctima de ellos. Léalo aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-el-riesgo-que-suponen-los-keyloggers-espias-que-pueden-infectar-nuestros-dispositivos/.


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD
para prevenir la amenza del keylogger
Espías digitales en tu dispositivo
Formatos de keyloggers
- Digitales (software):
Basados en API: Interceptan los datos entre el teclado y los programas en los que estamos tipeando.
Ladrones de formularios: Roban todos los datos que se ingresan en formularios web.
Basados en el kernel: Ingresan al núcleo del sistema obteniendo permisos de Administrador, teniendo a su disposición toda la información que se ha ingresado al sistema.


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD
para prevenir la amenza del keylogger
Espías digitales en tu dispositivo
Precauciones contra los keyloggers
1.- Usar programas de seguridad que escaneen tu equipo en busca de este tipo de software.
2.- Mantener tus equipos actualizados, para que detecten los keyloggers más modernos.
3.- Emplear administradores de contraseñas, que rellenan las claves en lugar de tener que tipearlas cada vez.


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD
para prevenir la amenza del keylogger
Espías digitales en tu dispositivo
Precauciones contra los keyloggers
4.- Hacer una revisión física del aparato, para chequear que no haya conexiones extrañas entre el teclado y el resto del equipo.
5.- Activar la autenticación de dos pasos en las cuentas y apps que lo permitan.
6.- Evitar el uso de pendrives desconocidos o discos de almacenamiento externos en los que no se tenga confianza.
Es muy difícil detectar un keylogger, se recomienda tener actitudes de seguridad en internet para evitar estos programas maliciosos.

El Comando de la Semana | No. 15 Nikto

Esta vez, la sección El Comando de la Semana trata sobre Nikto, un escáner de servidor web de código abierto (GPL) que realiza pruebas exhaustivas contra servidores web para varios elementos, incluidos más de 6.700 archivos potencialmente peligrosos, verifica versiones desactualizadas de más de 1.250 servidores y problemas específicos de la versión en más de 270 servidores. También comprueba los elementos de configuración del servidor, como la presencia de varios archivos de índice, las opciones del servidor HTTP e intentará identificar los servidores web y el software instalados. Los elementos de escaneo y los complementos se actualizan con frecuencia y se pueden actualizar automáticamente.

El objetivo de estos comandos que compartimos semanalmente no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Descarga el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-14/.

El Control de la Semana | No. 9 Protección contra amenazas externas y del ambiente

La Ficha de Control Normativo de esta semana trata sobre cómo definir políticas de Seguridad Física y del Ambiente, parte de la implementación de la Política General de Seguridad de la Información en una organización.

En el documento descargable a continuación, encontrarán restos consejos y otras consideraciones, parte de nuestra serie de fichas de control normativo.

Pueden descargar esta nueva ficha semanal, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-9/.

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- José Ignacio Parra
- Gonzalo Andrés Ramírez Cabrera
- Francisco Javier Gutiérrez
- Jorge Muñoz
- Eliú Figueroa Albarrán
- Romel Rivas
- Andrés Aldana F.
- SIOC Ecomsur
- Luis Catrilef

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.03 17:15:54 -04'00'