Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

13-08-2021 | Año 3 | N°110

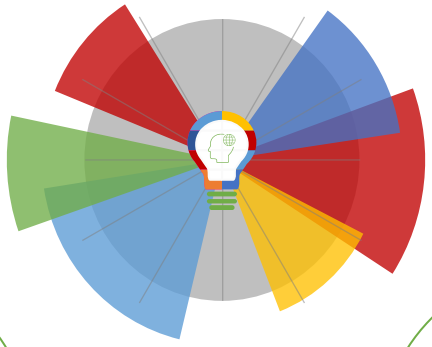
Boletín de Seguridad Cibernética

Semana del 06 al 12 de agosto 2021

La semana en cifras

Hash
14
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
5
URL
Asociadas a sitios fraudulentos y campañas de phishing



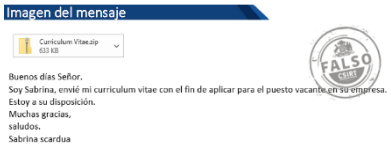
Parches
79
para vulnerabilidades
Las mitigaciones son útiles en productos de Microsoft y Red Hat.

IP
4
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

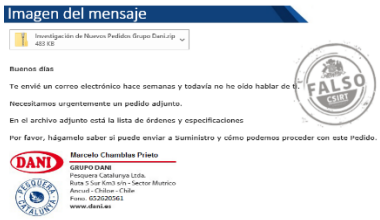
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Malware



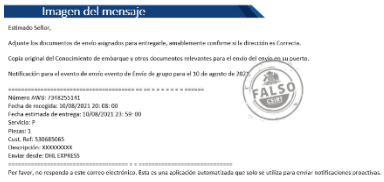
CSIRT alerta de campaña de malware con falso email	
Alerta de seguridad cibernética	2CMV21-00206-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2021
Última revisión	9 de agosto de 2021
Indicadores de compromiso	
SHA256	
C95430C28E718490FF42972961E854C573C17E631755F634F409DCD8E5998672 BD8E20864840F282FF01DB4854C9F4E1F29DBD61678A74492AD1F348C59F3B92	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00206-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00206-01.pdf	



CSIRT alerta de campaña de phishing con email falso	
Alerta de seguridad cibernética	2CMV21-00207-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2021
Última revisión	9 de agosto de 2021
Indicadores de compromiso	
SHA256	
C43D49B18B5F61A528E617C6153B832E710F5858F717C8EA9B048CB561EFC5A1 028BF9BA6655E79F036E2DE0ECCDCE5A121D63D902668350EB9CB3D094321597	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00207-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00207-01.pdf	

CSIRT alerta de campaña de malware que suplanta a la Universidad de Buenos Aires	
Alerta de seguridad cibernética	2CMV21-00208-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2021
Última revisión	9 de agosto de 2021
Indicadores de compromiso	
SHA256	
E9982B80E61AC3CE938CE597AEC312A3EA7D60FC8F600AA553FCAA0369D62079 028BF9BA6655E79F036E2DE0ECCDCE5A121D63D902668350EB9CB3D094321597	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00208-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00208-01.pdf	

CSIRT alerta ante campaña de malware que suplanta a la UBA	
Alerta de seguridad cibernética	2CMV21-00209-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021
Indicadores de compromiso	
SHA256	
38ba8bc874b39f5bf0b54728432d8c0f90cacfa05aaa3a6149b072b346a5f75b a33a5630510f65342fc12c6d68694d22398b2a20ac98f2edd8f606590e5dfddd	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00209-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00209-01.pdf	



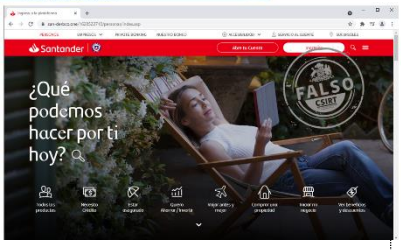
CSIRT alerta por campaña de malware que suplanta a DHL	
Alerta de seguridad cibernética	2CMV21-00210-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021
Indicadores de compromiso	
SHA256	
AE680810C7CE9D5415715CB2960828EB9BC4B3AD9494138CC1892B852E0B5112 42B4A1C6BB6C57B21540D10A07B8E94F282C75909D218734A6872137857A2E8F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00210-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00210-01.pdf	

CSIRT alerta de nueva campaña de phishing para difundir malware	
Alerta de seguridad cibernética	2CMV21-00211-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2021
Última revisión	12 de agosto de 2021
Indicadores de compromiso	
SHA256	
6D51A37C2376F8AF9793B6F91B201E263B7356146C3FDFE9F49A8816B2030445 505CE8FCAA21B5FE5678571F794EAB2477FB4E0E7DEA90796E08CE1206AC4D1F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00211-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00211-01.pdf	

CSIRT alerta de campaña de malware que suplanta a Unilever Ecuador	
Alerta de seguridad cibernética	2CMV21-00212-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2021
Última revisión	12 de agosto de 2021
Indicadores de compromiso	
SHA256	
169A7CF8547051955CFCDEE93C5C0ED17BA09E1856C66C26C04081836685C755 15EE5A319FDEAAFD781E768C7DF3DF07FF1E4D55B57EB5D8E88C887409B76106	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00212-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00212-01.pdf	

Sitios fraudulentos

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01001-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2021
Última revisión	10 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://san-derbco[.]one/1628522710/personas/index.asp	
IP	
[198.54.114.195]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01001-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01001-01.pdf	

Imagen del sitio

CSIRT alerta ante sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR21-01002-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2021
Última revisión	10 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
http://francojunior[.]net/pagina/imagenes/comun2008/login.php#	
IP	
[149.56.241.97]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01002-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01002-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH21-00424-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://app.itau-att[.]com/choose.php	
IP	
[80.78.23.220]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00424-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00424-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de smishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH21-00425-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/2VJHum3	
URL sitio falso	
https://chileatiende-sms[.]xyz/?sms=Santander https://suertedeldia[.]store/1628785543/personas/index.asp	
IP	
[68.65.123.97]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00425-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00425-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades críticas en varios productos de Microsoft	
Alerta de seguridad cibernética	9VSA21-00480-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2021
Última revisión	10 de agosto de 2021

CVE

CVE-2021-36936	CVE-2021-36943	CVE-2021-26428	CVE-2021-36950
CVE-2021-26432	CVE-2021-36938	CVE-2021-26426	CVE-2021-34532
CVE-2021-26424	CVE-2021-36937	CVE-2021-34537	CVE-2021-26423
CVE-2021-34535	CVE-2021-36933	CVE-2021-34487	CVE-2021-36947
CVE-2021-34534	CVE-2021-36932	CVE-2021-34536	CVE-2021-36945
CVE-2021-34480	CVE-2021-36927	CVE-2021-34486	CVE-2021-36941
CVE-2021-34530	CVE-2021-36926	CVE-2021-34483	CVE-2021-36940
CVE-2021-36949	CVE-2021-26433	CVE-2021-34478	CVE-2021-36942
CVE-2021-36946	CVE-2021-26431	CVE-2021-34524	CVE-2021-26425
CVE-2021-34485	CVE-2021-26430	CVE-2021-33762	CVE-2021-34484
CVE-2021-36948	CVE-2021-26429	CVE-2021-34471	CVE-2021-34533

Fabricante

Microsoft

Productos afectados

.NET Core & Visual Studio	Windows Cryptographic Services
ASP .NET	Windows Defender
Azure	Windows Event Tracing
Azure Sphere	Windows Media
Microsoft Azure Active Directory Connect	Windows MSHTML Platform
	Windows NTLM
Microsoft Dynamics	Windows Print Spooler Components
Microsoft Graphics Component	Windows Services for NFS ONCRPC XDR Driver
Microsoft Office	
Microsoft Office SharePoint	Windows Storage Spaces Controller
Microsoft Office Word	Windows TCP/IP
Microsoft Scripting Engine	Windows Update
Microsoft Windows Codecs Library	Windows Update Assistant
Remote Desktop Client	Windows User Profile Service
Windows Bluetooth Service	

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00480-01

https://www.csirt.gob.cl/media/2021/08/9VSA21-00480-01.pdf

CSIRT alerta ante vulnerabilidades en productos Red Hat	
Alerta de seguridad cibernética	9VSA21-00481-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021

CVE

CVE-2020-0543	CVE-2020-8696	CVE-2021-31162	CVE-2021-33910
CVE-2020-0548	CVE-2020-8698	CVE-2021-31525	CVE-2021-34558
CVE-2020-0549	CVE-2021-20271	CVE-2021-31799	CVE-2021-3516
CVE-2020-24489	CVE-2021-27292	CVE-2021-31810	CVE-2021-3517
CVE-2020-24511	CVE-2021-28875	CVE-2021-32066	CVE-2021-3518
CVE-2020-24512	CVE-2021-28876	CVE-2021-33195	CVE-2021-3520
CVE-2020-36323	CVE-2021-28877	CVE-2021-33196	CVE-2021-3537
CVE-2020-36327	CVE-2021-28878	CVE-2021-33197	CVE-2021-3541
CVE-2020-8695	CVE-2021-28879	CVE-2021-33198	

Fabricante

Red Hat

Productos afectados

microcode_ctl (Red Hat package): 20210216-1.20210525.1.el8_4
Red Hat OpenShift Jaeger anteriores a la version 1.24.0
Red Hat Enterprise Linux Server 7 x86_64
Red Hat Enterprise Linux Workstation 7 x86_64
Red Hat Enterprise Linux Desktop 7 x86_64
Red Hat Enterprise Linux for Scientific Computing 7 x86_64
Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server – TUS: 8.4 y AUS: 8.4
Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.4
Red Hat Enterprise Linux for x86_64: 8.0
Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server (para IBM Power LE) – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.4
Red Hat Enterprise Linux for IBM z Systems – Extended Update Support: 8.4
Red Hat Enterprise Linux for x86_64: 8.0
Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.4
Red Hat Enterprise Linux for ARM 64 Extended Update Support: 8.4
Red Hat Enterprise Linux for ARM 64: 8
Red Hat Enterprise Linux for Power, little endian: 8
Red Hat Enterprise Linux for IBM z Systems: 8
go-toolset-1.15-golang (Red Hat package): 1.15.13-1.el7_9
go-toolset-1.15 (Red Hat package): 1.15.13-1.el7_9
Red Hat Developer Tools (RHEL Workstation) 1 x86_64
Red Hat Developer Tools (RHEL Server) 1 x86_64
Red Hat Developer Tools (RHEL Server for System Z) 1 s390x
Red Hat Developer Tools (RHEL Server for IBM Power LE) 1 ppc64le
Red Hat Developer Tools (RHEL Server for IBM Power) 1 ppc64

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00481-01
https://www.csirt.gob.cl/media/2021/08/9VSA21-00481-01.pdf

«Aceleran la ciberseguridad» | Columna en El Mercurio sobre la labor del CSIRT de Gobierno

OPINIÓN

Aceleran la ciberseguridad

Llama un amigo: "¡Me 'hackearon' mi teléfono! ¡Ojo con lo que te llegue!".

Gracias; no abriré *e-mails*, ni responderé, ni nada. ¿Qué más hacer?

Puedo matricularme en una charla sobre ciberseguridad.

El senador por Valparaíso, Kenneth Pugh, moderó una conversación con dos expertos que me podrían serenar. Uno, Santiago Paz, a cargo de la ciberseguridad por el grupo del Banco Interamericano de Desarrollo, el BID. Llegó allí desde Uruguay, donde logró activar medidas de protección. El otro, Carlos Landeros, es el jefe en redes y seguridad informática en nuestro Ministerio del Interior. Viejos amigos de lides compartidas.

Quedé con las ganas de que describieran a los criminales, habituado a los noticiarios, que se concentran en el morbo.

Quería saber de robos, de las amenazas, de los secuestros de información y los asaltos que se producen en el mundo digital. Hay un prontuario espantoso que recorrer. Sí, se refirieron a la "infraestructura crítica" (un listado que comprende los servicios de salud, los de agua potable, electricidad, los oleoductos, los bancos…).

Hablaron más de lo positivo.

Pensé en mis nietos que discurren sobre su vocación profesional cuando Carlos Landeros habló de las oportunidades de servicios y de negocios en ciberseguridad. Faltan especialistas. Peor todavía, no hay suficientes profesores, investigadores, profesionales en el tema. Santiago Paz se refirió a alianzas internacionales de instituciones de educación superior en la materia.

María Florencia Attademo-Hirt, jefa del grupo BID en Chile, dio las cifras en EE.UU.: hay 900 mil profesionales, pero faltan 450 mil. Y ofreció el apoyo de su organización para la formación de expertos. Ojalá no se los robe después EE.UU.

Ella hizo ver cómo el cibercrimen demolía la confianza en los sistemas digitales que hoy sustentan la vida en sociedad. Es uno de los cinco riesgos que más amenazan a las empresas, según el BID.

Santiago Paz, el uruguayo, mostró cómo esta no es una cuestión solo de ingenieros o de políticos. Como siempre, el tema es cultural. Tal como en el tránsito urbano, no basta con demarcar las calles, instalar semáforos, peajes, cámaras de seguridad, la policía, los tribunales… La cosa es que los choferes manejen a la defensiva.

NICOLÁS LUCO

Hay que rediseñar todo, teniendo presente desde los cimientos, la ciberseguridad y la cooperación.

Carlos Landeros apuntó a los altos ejecutivos. Los llamó a invertir en ciberseguridad. La gente preferirá a las empresas en las que tiene confianza. "No tenemos que esperar más ciberataques, ya hay experiencia suficiente", dijo.

El senador agradeció las sugerencias prácticas. Espera que el Senado saque adelante las leyes, de gobernanza de la ciberseguridad, de infraestructura crítica de la nación. Estamos a punto. Landeros habló de la ley de delitos informáticos y la ley de datos. Agradeció al BID los 27 millones de dólares entregados para educar sobre el tema. Hasta motiva a los padres para que entrenen a sus hijos en la materia.

Para sufrir menos "hackeos".

Este lunes, «El Mercurio» compartió en su sección Vida, Ciencia y Tecnología, una columna de Nicolás Luco que versa sobre la charla entre el Director Nacional del CSIRT de Gobierno, Carlos Landeros y el Especialista Sectorial de Ciberseguridad del BID, Santiago Paz, con la moderación del Senador Kenneth Pugh, realizada la semana anterior.

Queremos compartir con ustedes esta interesante columna, disponible para su lectura en el siguiente enlace: https://www.csirt.gob.cl/noticias/columna-aceleran-la-ciberseguridad/.

El Comando de la Semana | No. 12 SHCHECK

En la sección El Comando de la Semana les traemos a SHCHECK, herramienta en lenguaje Python para escanear los encabezados de seguridad de cualquier sitio web, sin importar el websever o sistema operativo sobre el que esté construido. Verificar la presencia de estos encabezados es importante, ya que permiten evitar que actores maliciosos puedan efectuar una técnica conocida como clickjacking para robar información de los usuarios que ingresan a sitios web vulnerables.

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.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/media/2021/08/Comando-de-la-semana-12-SHCHECK_v1.pdf.

El Control de la Semana | No. 6 Políticas de acceso a las redes y a los servicios de la red

La Ficha de Control Normativo que compartimos esta semana trata sobre las mejores formas de establecer políticas de acceso a las redes y a los servicios de la red, algo clave al definir un Sistema de Gestión de la Seguridad de la Información. En el documento encontrarán requisitos y elementos que resulta esencial considerar al momento de definir los controles de acceso a los datos de su organización.

Pueden descargar esta quinta ficha semanal, aquí: https://www.csirt.gob.cl/media/2021/08/El-Control-de-la-semana-N%C2%B06-A.9.1.2_v1.pdf.

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.

- Claudia Inostroza Castillo
- C4t[.]py_01
- Victor Cofré
- Fátima Fleitas Suárez
- Greta Emperatriz Gómez Cornejo
- Gabriel Huenulaf
- Sergio Vega Castillo
- Olivia Véliz Copa
- Cinthya Gabriela Miranda Terrazas
- Andrés Aldana F.
- Jorge Rodrigo Muñoz Ubilla
- Rodrigo Machado Villegas
- Nicolás Carrasco
- Patricio Quezada
- Javier Ignacio Candia Tapia

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.08.16 10:38:28 -04'00'