Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

15-07-2021 | Año 3 | N°106

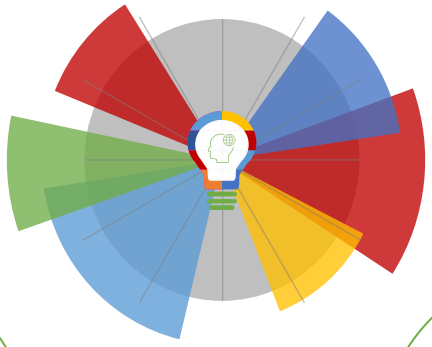
Boletín de Seguridad Cibernética

Semana del 9 al 14 de julio de 2021

La semana en cifras

Hash
2
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
6
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
152
para vulnerabilidades
Las mitigaciones son útiles en productos de Microsoft, Adobe y Cisco.

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....2
Sitios fraudulentos....3
Phishing....4
Vulnerabilidades....5
Actualidad....8
Recomendaciones y buenas prácticas....10
Muro de la Fama....14

Malware

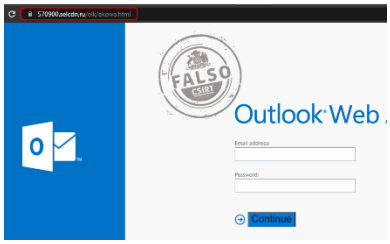
CSIRT alerta ante campaña de malware que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00202-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021
Indicadores de compromiso	
SHA256	
40b42995ff3b6060af72d7929532c86e3428d28f8641f48fc5e1d224dd87cc2d 2a96a10441d437dc80f91db82571eb7a84cf8c500006eb2c2a358b1953b74c31	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00202-01/	
https://csirt.gob.cl/media/2021/07/2CMV21-00202-01.pdf	

Sitios fraudulentos

Imagen del sitio

CSIRT advierte de página fraudulenta que suplanta a Apple	
Alerta de seguridad cibernética	8FFR21-00989-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
https://sandalci.com[.]tr/3r/final/c559da2ba967eb820766939a658022c8/	
IP	
[176.236.107.10]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00989-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00989-01.pdf	

Imagen del sitio



CSIRT alerta ante página fraudulenta que suplanta a Outlook Web	
Alerta de seguridad cibernética	8FFR21-00990-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
https://570900.selcdn[.]ru/elk/ekowa.html	
IP	
[92.53.68.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00990-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00990-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de campaña de smishing que suplanta al banco Santander	
Alerta de seguridad cibernética	8FPH21-00418-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/Santandeer	
URL sitio falso	
https://bnc0-xxsamtamdeerxx[.]com/1626113046/index.asp	
IP	
[66.29.132.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00418-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00418-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de smishing que suplanta al banco Santander	
Alerta de seguridad cibernética	8FPH21-00419-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021
Indicadores de compromiso	
URL de SMS	
https://smsverific[.]app/?sms=santander	
URL sitio falso	
https://validatu-clave[.]app/1626113851/personas/index.asp	
IP	
[66.29.141.3]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00419-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00419-01.pdf	

Vulnerabilidades

CSIRT alerta ante distintas vulnerabilidades en productos Cisco	
Alerta de seguridad cibernética	9VSA21-00465-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de julio de 2021
Última revisión	9 de julio de 2021

CVE

CVE-2021-1562	CVE-2021-1576
CVE-2018-0155	CVE-2021-3449
CVE-2021-1359	CVE-2021-3450
CVE-2021-1574	

Fabricante

Cisco

Productos afectados

Cisco BroadWorks Application Server
Cisco Catalyst 4500 Series Switches
Cisco Catalyst 4500-X Series Switches
Cisco Web Security Appliance (WSA)

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00465-01
https://www.csirt.gob.cl/media/2021/07/9VSA21-00465-01.pdf

CSIRT alerta de vulnerabilidades críticas en productos de Microsoft	
Alerta de seguridad cibernética	9VSA21-00466-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio de 2021

CVE

CVE-2021-31183	CVE-2021-33767	CVE-2021-34449	CVE-2021-34493
CVE-2021-31196	CVE-2021-33768	CVE-2021-34450	CVE-2021-34494
CVE-2021-31206	CVE-2021-33771	CVE-2021-34451	CVE-2021-34496
CVE-2021-31947	CVE-2021-33772	CVE-2021-34452	CVE-2021-34497
CVE-2021-31961	CVE-2021-33773	CVE-2021-34454	CVE-2021-34498
CVE-2021-31979	CVE-2021-33774	CVE-2021-34455	CVE-2021-34499
CVE-2021-31984	CVE-2021-33775	CVE-2021-34456	CVE-2021-34500
CVE-2021-33740	CVE-2021-33776	CVE-2021-34457	CVE-2021-34501
CVE-2021-33743	CVE-2021-33777	CVE-2021-34458	CVE-2021-34503
CVE-2021-33744	CVE-2021-33778	CVE-2021-34459	CVE-2021-34504
CVE-2021-33745	CVE-2021-33779	CVE-2021-34460	CVE-2021-34507
CVE-2021-33746	CVE-2021-33780	CVE-2021-34461	CVE-2021-34508
CVE-2021-33749	CVE-2021-33781	CVE-2021-34462	CVE-2021-34509
CVE-2021-33750	CVE-2021-33782	CVE-2021-34464	CVE-2021-34510

CVE-2021-33751	CVE-2021-33783	CVE-2021-34466	CVE-2021-34511
CVE-2021-33752	CVE-2021-33784	CVE-2021-34467	CVE-2021-34512
CVE-2021-33753	CVE-2021-33785	CVE-2021-34468	CVE-2021-34513
CVE-2021-33754	CVE-2021-33786	CVE-2021-34469	CVE-2021-34514
CVE-2021-33755	CVE-2021-33788	CVE-2021-34470	CVE-2021-34516
CVE-2021-33756	CVE-2021-34438	CVE-2021-34473	CVE-2021-34517
CVE-2021-33757	CVE-2021-34439	CVE-2021-34474	CVE-2021-34518
CVE-2021-33758	CVE-2021-34440	CVE-2021-34476	CVE-2021-34519
CVE-2021-33759	CVE-2021-34441	CVE-2021-34477	CVE-2021-34520
CVE-2021-33760	CVE-2021-34442	CVE-2021-34479	CVE-2021-34521
CVE-2021-33761	CVE-2021-34444	CVE-2021-34488	CVE-2021-34522
CVE-2021-33763	CVE-2021-34445	CVE-2021-34489	CVE-2021-34523
CVE-2021-33764	CVE-2021-34446	CVE-2021-34490	CVE-2021-34525
CVE-2021-33765	CVE-2021-34447	CVE-2021-34491	CVE-2021-34528
CVE-2021-33766	CVE-2021-34448	CVE-2021-34492	CVE-2021-34529

Fabricante

Microsoft

Productos afectados

.NET Education Bundle SDK Install Tool
.NET Install Tool for Extension Authors
HEVC Video Extensions
Microsoft 365 Apps for Enterprise
Microsoft Bing Search for Android
Microsoft Dynamics 365 Business Central 2020
Microsoft Dynamics 365 Business Central 2021
Microsoft Excel 2013, 2013 RT, 2015
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2013, 2016, 2019
Microsoft Malware Protection Engine
Microsoft Office 2013, 2013 RT, 2016, 2019
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013
Microsoft SharePoint Enterprise Server 2013
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013
Microsoft SharePoint Server 2019
Microsoft Word 2016
Open Enclave SDK
Power BI Report Server
Visual Studio Code
Windows 10
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2004, 2008, 2012, 2012 R2, 2016, 2019, 20H2

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00466-01
https://www.csirt.gob.cl/media/2021/07/9VSA21-00466-01.pdf

CSIRT alerta de vulnerabilidades en varios productos de Adobe	
Alerta de seguridad cibernética	9VSA21-00467-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de julio de 2021
Última revisión	14 de julio de 2021

CVE	
CVE-2021-35981	CVE-2021-28636
CVE-2021-35983	CVE-2021-28637
CVE-2021-35984	CVE-2021-28638
CVE-2021-35985	CVE-2021-28639
CVE-2021-35986	CVE-2021-28640
CVE-2021-35987	CVE-2021-28641
CVE-2021-35988	CVE-2021-28642
CVE-2021-35989	CVE-2021-28643
CVE-2021-35990	CVE-2021-28644
CVE-2021-35991	CVE-2021-28591
CVE-2021-35992	CVE-2021-28592
CVE-2021-35980	CVE-2021-28593
CVE-2021-28624	CVE-2021-28595
CVE-2021-28634	CVE-2021-28596
CVE-2021-28635	

Fabricante
Adobe

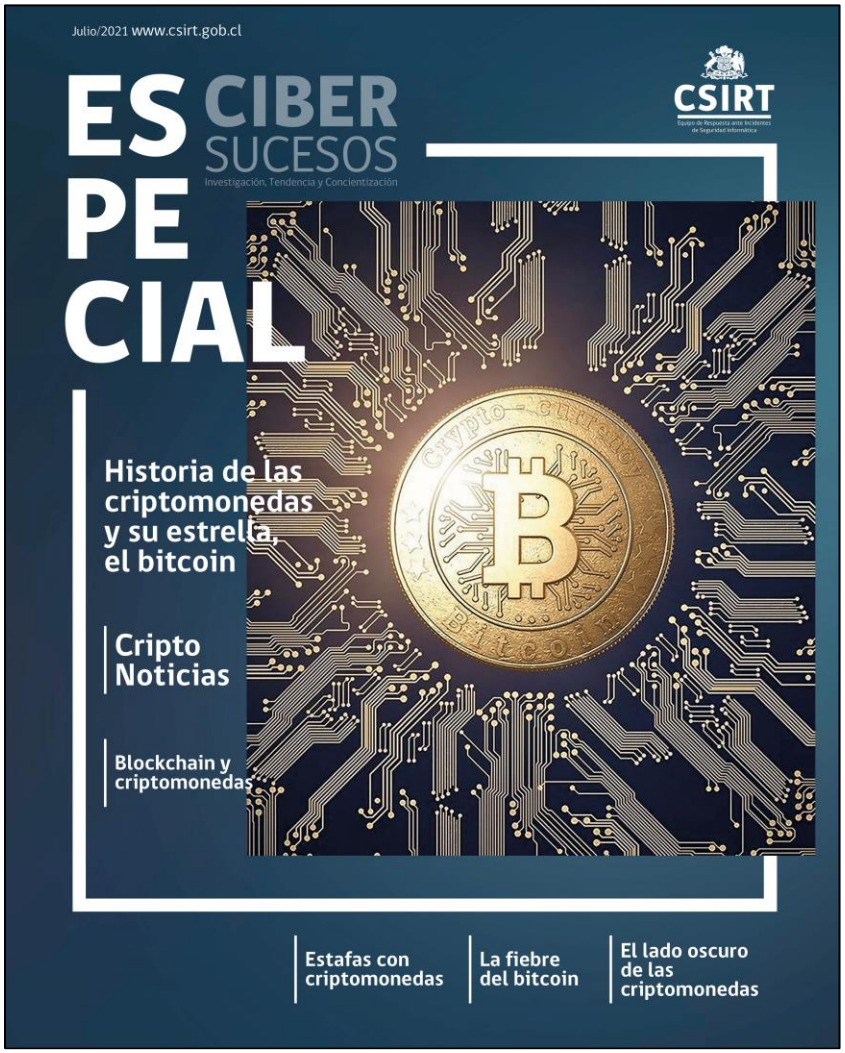
Productos afectados
Adobe Dimension 3.4 y anteriores
Adobe Illustrator 2021 25.2.3 y anteriores.
Adobe Framemaker 2019 Release Update 8 (hotfix) y 2020 Release Update 2.
Adobe Acrobat DC y Reader DC 2021.005.20054 y anteriores.
Adobe Acrobat 2020 y Acrobat Reader 2020 2020.004.30005 y anteriores
Adobe Acrobat 2017 y Acrobat Reader 2017, 2017.011.30197 y anteriores.
Adobe Bridge 11.0.2 y anteriores.

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00467-01
https://www.csirt.gob.cl/media/2021/07/9VSA21-00467-01.pdf

Actualidad

CiberSucesos Especial Criptomonedas

Viendo cómo dominan las noticias y las redes sociales, este mes en nuestra revista CiberSucesos decidimos hacer un especial dedicado enteramente al Bitcoin y otras criptomonedas ¿El futuro del dinero o catalizador del ciberdelito? Decídelo tras leer nuestra revista, aquí:
https://csirt.gob.cl/recomendaciones/cibersucesos-especial-criptomonedas/



Ciberconsejos | Cómo evitar que tu hijo sea víctima del grooming

Se denomina descubrimiento pasivo a las formas de encontrar datos personales o información delicada de una organización a través de fuentes abiertas disponibles en internet. Es importante controlar la información que ponemos en línea, siguiendo los consejos que compartimos en: csirt.gob.cl/recomendaciones/ciberconsejos-cuida-lo-que-compartes-y-evita-el-descubrimiento-pasivo.

El Comando de la Semana | No. 8: UNISCAN

Esta publicación, con la que buscamos compartir información de herramientas útiles para los encargados de ciberseguridad de todo tipo de instituciones, tuvo como protagonista esta semana al comando Uniscan, un simple escáner de vulnerabilidad de inclusión de archivos remotos, inclusión de archivos locales y ejecución de comandos remotos.

Encuéntralo aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-8/.

El Control de la Semana | No. 3 Concientización, educación y formación en seguridad de la información

Este documento, denominado “Ficha de Control Normativo", tiene como objetivo ilustrar sobre los diferentes controles normativos que se estima son prioritarios para todo Sistema de Gestión de Seguridad de la Información. https://www.csirt.gob.cl/estadisticas/la-implementacion-del-mes-no-1-seguridad-aplicada

Encuentra la tercera ficha aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-3.

La Implementación de la Semana | No. 1 SYSLOGSERVER

Este julio debuta una nueva publicación llamada La Implementación de la Semana, cuya primera edición está dedicada SYSLOGSERVER.

Encuéntrala aquí: https://www.csirt.gob.cl/estadisticas/la-implementacion-del-mes-no-1.

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.

- Mr. H
- Natán Finol Bencomo
- Diego Javier González Figueroa
- Alfonso Adauy
- Rodrigo Cortés
- Robinson Cáceres

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.15 15:26:09 -04'00'