Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

23-04-2021 | Año 3 | N°94

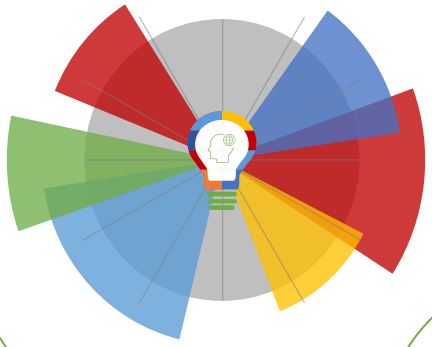
Boletín de Seguridad Cibernética

Semana del 16 al 22 de abril de 2021

La semana en cifras

Hash
29
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
9
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
20
para vulnerabilidades
Las mitigaciones son útiles para productos de Pulse, Google y Mozilla.

IP
23
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.

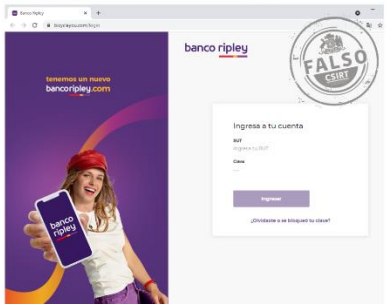
Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT alerta por sitio que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00933-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2021
Última revisión	19 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://159.65.153[.]113/1618842122/index.asp	
IP	
[159.65.153[.]113]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00933-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00933-01.pdf	

Imagen del sitio

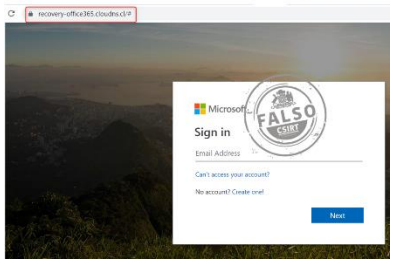


CSIRT alerta por sitio que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00934-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://bicycleyou[.]com/login	
IP	
[186.64.116.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00934-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00934-01.pdf	

Imagen del sitio

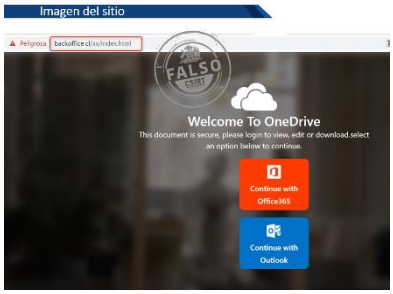
CSIRT alerta por sitio que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00935-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://sec.banco.santander.personas.chile.adu-experts[.]com/1619014963/index.asp	
IP	
[107.180.3.96]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00935-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00935-01.pdf	

Imagen del sitio



CSIRT alerta por sitio que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR21-00936-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://recovery-office365.cloudns[.]cl/#	
IP	
[46.166.184.102]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00936-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00936-01.pdf	

CSIRT alerta por sitio que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00937-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://login.clientescl[.]site/1619031808/index.asp	
IP	
[35.193.157.255]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00937-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00938-01.pdf	



CSIRT alerta de web fraudulenta que suplanta a OneDrive	
Alerta de seguridad cibernética	8FFR21-00938-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de abril de 2021
Última revisión	22 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://backoffice[.]cl/xx/index.html	
IP	
[162.241.157.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00938-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00938-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta por phishing con falso email del Banco Santander	
Alerta de seguridad cibernética	8FPH21-00393-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2021
Última revisión	17 de abril de 2021
Indicadores de compromiso	
URL sitio redirección	
http://143.110.242[.]241/	
URL sitio falso	
https://barco-santndrcl[.]xyz/1618584018/index.asp	
IP	
[157.245.96.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00393-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00393-01.pdf	

Imagen del mensaje

CSIRT alerta por phishing con email que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00394-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
wwwbancoripley.cl.asthamart[.]com/	
IP	
[162.213.196.78]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00394-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00394-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Mozilla Thunderbird y Firefox	
Alerta de seguridad cibernética	9VSA21-00425-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2021
Última revisión	20 de abril de 2021
CVE	
CVE-2021-23994	CVE-2021-29946
CVE-2021-23995	CVE-2021-29948
CVE-2021-23998	CVE-2021-23996
CVE-2021-23961	CVE-2021-23997
CVE-2021-23999	CVE-2021-24000
CVE-2021-24002	CVE-2021-24001
CVE-2021-29945	CVE-2021-29947
Fabricante	
Mozilla	
Productos afectados	
Mozilla Thunderbird: versiones de la 60.0 a la 78.9.1. Mozilla Firefox: versiones de la 8.0.1 a la 87.0. Mozilla Firefox ESR: versiones de la 60.0 a la 78.9.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00425-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00425-01.pdf	

CSIRT alerta de vulnerabilidad crítica en Pulse Connect Secure	
Alerta de seguridad cibernética	9VSA21-00426-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril de 2021
CVE	
CVE-2021-22893	
Fabricante	
Pulse	
Productos afectados	
Pulse Connect Secure (PCS) 9.0R3 y superior.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00426-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00426-01.pdf	

CSIRT alerta por vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00427-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de abril de 2021
Última revisión	22 de abril de 2021
CVE	
CVE-2021-21222 CVE-2021-21223 CVE-2021-21224	CVE-2021-21225 CVE-2021-21226
Fabricante	
Google	
Productos afectados	
Google Chrome	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00419-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00419-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos	Documento web
014091ccf1da83017db74482e8ba23ac09c9d3be83db0cde6acf7ce501b33158	2CMV21-00172-01
02521f0bb91b4c74d1590b85254f26f0d258cd780393010593ae6daaa5993753	2CMV21-00172-01
0b703762face2a9e4e471d7552928c04e5c689979d4577f2fca545c618e93f92	2CMV21-00172-01
0cd5a024136300d04da07a59d2809c4de9490101d39cdc0f1d626f0bd8d7e222	2CMV21-00172-01
1c7f3a2e122fb7bc063f2ac2569e0efc40cb692ca851951c7ad75459bf1ef946	2CMV21-00172-01
20a1ef617f8e7d88f053d8a0413d2314fab10b201f10fb9ca68781451d915ab2	2CMV21-00172-01
2b403d2296c588bf2df893e68032aa7e08d961b8381fbde633e33ba0f3a6229d	2CMV21-00172-01
3f166bca73a1ce8ac5a413d202c62f066b6ad30fac79efa72c27e126608f1168	2CMV21-00172-01
40a9ca2ac0d094d2920a9bcec0667053e8021f7cc8fa46c8db69d9c620c8cf97	2CMV21-00172-01
5089d4f46e3d770269a9f6aff7ffee885c58b0e6a7a5782ef937a51b8d858611	2CMV21-00172-01
5b1f24d4df73a4b7030f827e2ac416691b4bfd3fe8f1bd7e08d9a066b46fb9b7	2CMV21-00172-01
669bc3853206dc70db65ff9328a08f2acebeb53968842b64edd2c65a7fabbdb6	2CMV21-00172-01
66ae87b3a3b395219b730ce1cf8dccfe3ccf78872979bd6100a14571df61bc6c	2CMV21-00172-01
6db1ff8c8165ce025e4a0ed40d3898b44775d9d6149156a1b1a6c750f4b5ff60	2CMV21-00172-01
97307bd8eb2823df5bed1ec7877544c7c5a171ce43d4bbb8214fe31bf6b9595c	2CMV21-00172-01
9c46d85d692df86280e483d3d3814b0d46f14e9469df7f4f0e53253a1e8f8e98	2CMV21-00172-01
e4fc12ad05311be83b981d6ede545f691b484adb0e0ec3ff99451555691545f5	2CMV21-00172-01
e9e5b02aedb7b8b2dcc2b5911cd3d6231a0f3a4f106cd7b3e34df73d14e8d3d0	2CMV21-00172-01
f5eba0dabaf2f683f7db6367e1fef245968870d76211dd46dcd57ded0d25d7cd	2CMV21-00172-01
fa67ef0fb5b5675fcc95cad44e4debbc4eb093dfb9038429124be44af0dd8ab3	2CMV21-00172-01
fdd5611526089bf08eee93b73b19b07091674f0760017619cf7f5d851885eaae	2CMV21-00172-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
92.118.190.80	23media GmbH	2CMV21-00172-01
45.143.223.147	ABC Consultancy	2CMV21-00172-01
45.137.22.84	RootLayer Web Services Ltd.	2CMV21-00172-01
45.137.22.71	RootLayer Web Services Ltd.	2CMV21-00172-01
31.210.20.217	Des Capital B.V.	2CMV21-00172-01
27.71.121.184	Viettel Group	2CMV21-00172-01
216.194.166.202	INMOTION	2CMV21-00172-01
185.222.58.156	RootLayer Web Services Ltd.	2CMV21-00172-01
159.203.121.138	DIGITALOCEAN-ASN	2CMV21-00172-01
141.98.10.239	UAB Host Baltic	2CMV21-00172-01
139.162.7.170	Linode, LLC	2CMV21-00172-01
134.209.149.84	DIGITALOCEAN-ASN	2CMV21-00172-01
134.119.177.15	Host Europe GmbH	2CMV21-00172-01
109.70.236.32	M247 Ltd	2CMV21-00172-01
103.133.105.111	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00172-01

Correos electrónicos de donde son enviados los archivos adjunto con malware.

Dirección	Documento web
abdullah-jallad@veniciaco.com	2CMV21-00172-01
alexander.rivera@berriospr.com	2CMV21-00172-01
colivieri@curbellmedical.com	2CMV21-00172-01
GVIJ@un.org	2CMV21-00172-01
headoffice@karlstorz.com	2CMV21-00172-01
madha@technogroupllc.com	2CMV21-00172-01
martini3@o3.e.notification.intuit.com	2CMV21-00172-01
MENA_MARKETING@MEDICOM-GRP.COM	2CMV21-00172-01
ofertas@bombasideal.com	2CMV21-00172-01
rawinox@via-gmail.com	2CMV21-00172-01
sales@gmdsa.com	2CMV21-00172-01
sales@hbxfgj.com	2CMV21-00172-01

sales@padministracja.com.pl	2CMV21-00172-01
sales-06@minewe.com	2CMV21-00172-01
smith@maerskline.com	2CMV21-00172-01
tiwarikk@bhansaliabs.com	2CMV21-00172-01

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
45.227.253.115	Global Layer B.V.	4IIA21-00035-01
5.188.206.236	Krez 999 Eood	4IIA21-00035-01
141.98.10.235	UAB Host Baltic	4IIA21-00035-01
141.98.10.40	UAB Host Baltic	4IIA21-00035-01
141.98.10.132	UAB Host Baltic	4IIA21-00035-01
141.98.10.232	UAB Host Baltic	4IIA21-00035-01
185.24.233.98	Sternforth Ltd	4IIA21-00035-01
170.231.195.192	COMETA TELECOMUNICACOES E SERVICOS LTDA	4IIA21-00035-01

Actualidad

Alerta ante explotación de varias vulnerabilidades por parte de actores relacionados a un servicio de inteligencia ruso

El 15 de abril de 2021, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS) de Estados Unidos y el Buró Federal de Investigaciones (FBI) compartieron una alerta conjunta sobre la explotación de varias vulnerabilidades conocidas por parte actores del Servicio de Inteligencia Exterior de Rusia (SVR), entre los que se incluyen aquellos conocidos como APT29, Cozy Bear y The Dukes) con el objetivo de comprometer redes de EE.UU. y sus aliados, incluyendo sistemas de gobierno y seguridad nacional.

El CSIRT de Gobierno decidió compartir esta alerta, las vulnerabilidades involucradas y su mitigación, con la comunidad. Los detalles de esta publicación pueden ser encontrados aquí: https://www.csirt.gob.cl/noticias/alerta-ante-explotacion-de-varias-vulnerabilidades-por-svr/.

Ciberconsejos | El Bitcoin y las estafas que lo rodean

Junto al aumento en notoriedad de las denominadas criptomonedas, como siempre ocurre, al interés de inversionistas y redes sociales se ha sumado el de los criminales, que aprovechan de generar nuevas estafas.

Para concientizar a la población respecto de los riesgos asociados al Bitcoin y las criptomonedas, publicamos consejos esta semana en nuestra web: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-el-bitcoin-y-las-estafas-que-lo-rodean/.

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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Nelson Collao
- Nicolás Osorio Guzmán
- Romel Rivas
- Felipe Zúñiga
- Michael Hudson
- Eduardo Juan Barra Guzmán

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.23 12:48:36 -04'00'