Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

05-03-2021 | Año 3 | N°87

Boletín de Seguridad Cibernética

Semana del 27 de Febrero al 4 de marzo de 2021

La semana en cifras

Hash

34

SHA

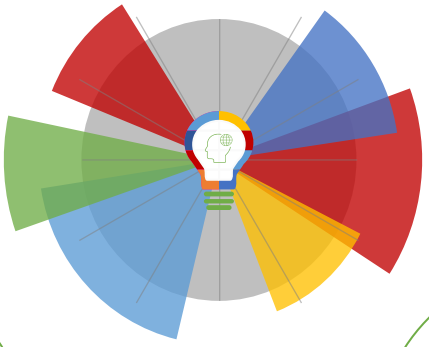
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

2

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

46

para vulnerabilidades

Las mitigaciones son útiles para productos de Microsoft, Google, Cisco, Red Hat y VMware.

IP

28

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.

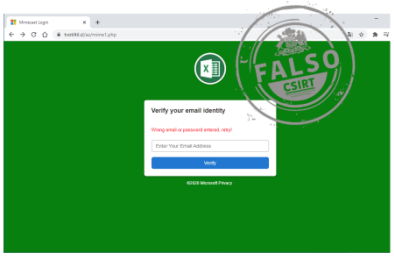
Contenido

Malware

CSIRT alerta campaña de malware suplantando a DocuSign	
Alerta de seguridad cibernética	2CMV21-00151-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2021
Última revisión	4 de marzo de 2021
Indicadores de compromiso	
SHA256	
859DDD9B0A93AB88C58C9B767A5533A9B5477DDE42456F2C946EA5D06072FB0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00151-01/	
https://www.csirt.gob.cl/media/2021/02/2CMV21-00151-01.pdf	

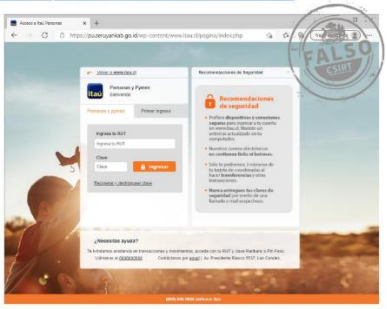
Sitios fraudulentos

Imagen del sitio



CSIRT alerta fraude que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR21-00910-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2021
Última revisión	4 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://tvotiltil[.]cl/az/mime1.php	
IP	
[131.72.237.67]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00910-01	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00910-01.pdf	

Imagen del sitio



CSIRT alerta web fraudulenta que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR21-00911-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2021
Última revisión	4 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://pu.seruyankab.go[.]id/wp-content/www.itau.cl/pagina/index.php	
IP	
[103.234.210.72]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00911-01	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00911-01.pdf	

Vulnerabilidades

CSIRT informa de vulnerabilidades en VMware	
Alerta de seguridad cibernética	9VSA21-00396-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de marzo de 2021
Última revisión	1 de marzo de 2021
CVE	
CVE-2021-21974	
Fabricante	
VMware	
Productos afectados	
vCenter Server, versiones 6.5 a 7.0 Cloud Foundation, versiones anteriores a la 3.10.1.2, 4.2. VMware ESXi.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00396-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00396-01.pdf	

CSIRT advierte vulnerabilidad en Cisco ACI MSO	
Alerta de seguridad cibernética	9VSA21-00397-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
CVE	
CVE-2021-1388	
Fabricante	
Cisco	
Productos afectados	
Cisco ACI Multi-Site Orchestrator (MSO) version 3.0, solo si está desplegado en un Cisco Application Services Engine.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00397-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00397-01.pdf	

CSIRT advierte vulnerabilidades en Google Android	
Alerta de seguridad cibernética	9VSA21-00398-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero de 2021
CVE	
CVE-2021-0394	CVE-2020-11194
CVE-2021-0392	CVE-2020-11190
CVE-2021-0390	CVE-2020-11189
CVE-2021-0396	CVE-2020-11188
CVE-2021-0393	CVE-2020-11186
CVE-2021-0397	CVE-2020-11178
CVE-2021-0398	CVE-2020-11171
CVE-2021-0391	CVE-2020-11166
CVE-2021-0395	CVE-2020-11165
CVE-2017-14491	CVE-2020-11228
CVE-2020-11299	CVE-2020-11227
CVE-2020-11226	CVE-2020-11218
CVE-2020-11222	CVE-2020-11204
CVE-2020-11221	CVE-2020-11192
CVE-2020-11220	CVE-2020-11223
CVE-2020-11199	CVE-2020-11309
CVE-2020-11198	CVE-2020-11308
CVE-2020-11195	CVE-2020-11290
Fabricante	
Google	
Productos afectados	
Google Android, versiones 8.1, 9.0, 10.0 y 11.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00398-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00398-01.pdf	

CSIRT advierte vulnerabilidad en un producto Red Hat	
Alerta de seguridad cibernética	9VSA21-00399-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2021
Última revisión	2 de marzo de 2021
CVE	
CVE-2020-8625	
Fabricante	
Red Hat	
Productos afectados	
Red Hat Enterprise Linux Server Extended Life Cycle Support (para sistemas IBM z) 6.0 Red Hat Enterprise Linux Server Extended Life Cycle Support 6.0 BIND (Red Hat), versiones anteriores a la 9.8.2-0.68.rc1.el6_10.10	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00399-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00399-01.pdf	

CSIRT advierte vulnerabilidades en Microsoft Exchange	
Alerta de seguridad cibernética	9VSA21-00400-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2021
Última revisión	3 de marzo de 2021
CVE	
CVE-2021-26412 CVE-2021-26854 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2021-27078	
Fabricante	
Microsoft	
Productos afectados	
Microsoft Exchange Server: Versiones desde la 2013 a la 2019 Cumulative Update 8.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00400-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00400-01.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
495c923ab372a92360bc7241b16187ce60068f995c2182ed3d66ea55684b741f	2CMV21-00150-01
008dabc9c695a13d2be06645edc06956002a264c41fbe7c2d7da11727aba480a	2CMV21-00150-01
8222b412a8a528056fcd0f1f9c8085b9c3b2e9b05a3c90d7f95d532cbeb38321	2CMV21-00150-01
b3ff253a6bd7ff4512487b935d354479801b6b9500605128da84e9278fa2dc42	2CMV21-00150-01
536b2614d6a31099c53d636bf1c674c018d41f5b4e546a17257a4cde158a16f6	2CMV21-00150-01
b626c611e4a6668e75d1f4fd8ed4f9c1239b6de513eab0c574bfe48a45abb11f	2CMV21-00150-01
d1d7ec19c75c12f7cfe87024102c1ae061c0ec471b0114e03d91f2ddd07aba81	2CMV21-00150-01
870d263e3d5278e7542f8a0314a5c8f68f1115a7c5696e59fcbe653ac4c8b03f	2CMV21-00150-01
11f64f10b7a150ec728fbe3628aa4c8a335c09343d4d1840c0ef1dd91818e462	2CMV21-00150-01
daa3b4cc0a299b78de55f130a24eec67102c719cc4c0baa722b1bb144c60e3fc	2CMV21-00150-01
bf553553b9d47c5b57b4981129d2c1f55a067edc4e1dfcd51cca03b9600db851	2CMV21-00150-01
76e8e761aa37660d10828d263d04149c66ffe1c4967f5fb827010a123690bf1d	2CMV21-00150-01
093006fcbb64faa05356284b9d9bce6fb6b8fd594a54ad5e00c7808e4dca945a	2CMV21-00150-01
644da9a2b0cd1ae3cb04c5bfd85df07a419f1fd0dc5a29131375d06a87c89b96	2CMV21-00150-01
6665a54b927a5b5a8beeef07ef63b33682cb1e3857ab5448a114a6f663b1efd5	2CMV21-00150-01
bc692c42c9c300e9ea559d6cdd74239d85339b60918b1c712db7078c1298421a	2CMV21-00150-01
c2a91909b7087801b1ae7689e24623160221a7b165f5beb87ba03afa627524b9	2CMV21-00150-01
72c20dd7a67dedb3045e8aba8dc54462dafe916c95470102469aa43d72c93337	2CMV21-00150-01
0f0abe327cf4ba2a1ee7f1fbe9d65a55ed84e293918bd5618eccfbe18c2cbf26	2CMV21-00150-01
12f3ec372a3987ec834a44b589541a4a17770cd87d15779d11b21515266fc9c6	2CMV21-00150-01
127a0b3f86c6f5caa0d45cd1aa13d7bcdc56b12f30540942160e13f80bf7b595	2CMV21-00150-01
029bfd696b5089e18faf0bd5c25f43eb383a8bbaa9ee15da263f5d2b29e8e743	2CMV21-00150-01
9ae23c9941b43097d3af543cdd0f39a34da6e0d312262b7b517bdc15f701c180	2CMV21-00150-01
b3a9852041c31fa3080ca8a79f8b30507c66c6de67d005ca59ce2169bb155e40	2CMV21-00150-01
c17b1961a8f0f3de556f0c922e7cb18acd4c547065fedeef03bad58e662c3dfe	2CMV21-00150-01
d02b54ef9109101c5a3be848b612b9a187685c43320758c2a73667e9e18b78d0	2CMV21-00150-01
975acd33467a22af294bdd8a724d91bcc0f1247d7d52e64522b9ec9877be98b1	2CMV21-00150-01
86e3f0d3124fa55cd730e41a1cbb91ca1c5f9393f0b20eb333b955a042fe6f1e	2CMV21-00150-01
62c56b59eece87a7df77225ca143cf4830c727f71ca99f37af08832bf8cc712a	2CMV21-00150-01
a405aeb0d276dbc07ebef2be07064ae195f89bf4220e40668da72f97d85df69d	2CMV21-00150-01

551787674cc0a87019310e4c6ac2ff3b6c67ca6c579f15745916668c00fc31b5	2CMV21-00150-01
37537009160d5586c9d766111b85a4a577e3a394e008b6a3e700c14fcb0f7cdb	2CMV21-00150-01
e7d670158ed873ed9743b6cf3449fd9f5e323707ea08b62bf5c7e98ed8deb2f4	2CMV21-00150-01

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
45.133.203.222	Internet It Company Inc	2CMV21-00150-01
93.152.158.188	Online Direct Ltd	2CMV21-00150-01
103.141.138.124	Vietnam Posts and Telecommunications Group	2CMV21-00150-01
143.110.227.204	DIGITALOCEAN-ASN	2CMV21-00150-01
211.197.183.104	Korea Telecom	2CMV21-00150-01
103.245.210.68	HK Kwaifong Group Limited	2CMV21-00150-01
103.99.1.142	Vietnam Posts and Telecommunications Group	2CMV21-00150-01
103.99.2.5	Vietnam Posts and Telecommunications Group	2CMV21-00150-01
153.126.171.39	Sakura internet inc.	2CMV21-00150-01
157.230.113.9	Digitalocean-asn	2CMV21-00150-01
157.245.103.92	Digitalocean-asn	2CMV21-00150-01
172.93.194.116	Nexeon	2CMV21-00150-01
185.222.57.246	Rootlayer Web Services Ltd	2CMV21-00150-01
185.93.227.6	IPV6 informatica S.L.	2CMV21-00150-01
185.99.253.71	Uk dedicated servers limited	2CMV21-00150-01
45.137.22.36	Rootlayer web services ltd.	2CMV21-00150-01
45.137.22.77	Rootlayer web services ltd.	2CMV21-00150-01
64.227.7.198	Digitalocean-asn	2CMV21-00150-01
64.44.139.163	Nexeon	2CMV21-00150-01
64.44.139.179	Nexeon	2CMV21-00150-01
84.38.132.41	Dataclub S.A.	2CMV21-00150-01

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

Dirección
auah@metalplessparts.net
accounts@marakishexpress.com
Ahmed.Abdelfattah@tui.ru
axu@metalplessparts.net
Bob@shrmbz.com
bwynsi@metalplessparts.net
chris@sinoglory-group.com
commonality@pak.com.cn
cwhite@dwnameplate.com
derry@kavatdintl.gq
Disha.sachin@beijerref.co.in
dwompoi@metalplessparts.net
engy.ahmed@razorslord.com
hyaxotu@metalplessparts.net
info@midwaywholesalebz.com
jpt@jptagri.de
karena@yorkshiretrading.com
mangchann@dreamgames.com.kh
operation@arkon-shipping.de
operation2@sawaby.com
pfidye@metalplessparts.net
pkpbear@acsalaska.net
purchase1.sal@suprajit.com
purchase1@aquavalv.com
shmwops@cmhk.com
squyq@metalplessparts.net
submissions@researchopenworld.com
tyvolei@metalplessparts.net
wuvujie@metalplessparts.net
zyjjiph@metalplessparts.net

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
45,142,120,147	UAB Host Baltic, LT	4IIA21-00031-01
2.57.122.16	PPTECHNOLOGY LIMITED	4IIA21-00031-01
103,133,111,129	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	4IIA21-00031-01
210.92.18.169	EHOSTICT	4IIA21-00031-01
5.188.206.235	KREZ 999 EOOD	4IIA21-00032-01
141.98.80.134	NFORCE - NForce Entertainment B.V	4IIA21-00032-01
103.153.183.25	SNTHOSTINGS-AS-AP - SnTHostings, IN	4IIA21-00032-01
37.49.225.123	PEENQ - PEENQ.NL, NL	4IIA21-00032-01
87.246.7.102	Internet Hosting LTD	4IIA21-00032-01

Actualidad

Ciberconsejos para una conexión segura a las clases virtuales

Vuelve marzo y como la pandemia continúa, así también lo hacen las clases online. Por eso elegimos, para el primer Ciberconsejos del mes, hacer un resumen de las principales recomendaciones para estar más protegidos en las clases virtuales.

Mencionamos los principales riesgos de exponer demasiada información en internet, cómo reducirlos, e incluimos una comparativa con aspectos de la seguridad de las plataformas más usadas: Zoom, Google Classroom y Microsoft Teams.

La infografía completa la pueden encontrar en el siguiente enlace de nuestro sitio web: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-conexion-segura-a-las-clases-virtuales/


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS
PARA UNA CONEXIÓN SEGURA A LAS CLASES VIRTUALES
RECOMENDACIONES PARA UNA CONEXIÓN SEGURA
CONFIGURA la privacidad de las cuentas de tus hijos, o conversa con el colegio para saber qué información puedes controlar.
INTENTA conocer a compañeros y profesores, para saber con quienes interactúan tus hijos.
NUNCA compartas claves ni el número de identificación de una reunión con desconocidos o en las redes sociales.
MANTÉN actualizada las plataformas y el equipo.


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS
PARA UNA CONEXIÓN SEGURA A LAS CLASES VIRTUALES
COMPARATIVA DE SEGURIDAD
CIFRADO
AUTENTICACIÓN DE DOS PASOS
GRABACIÓN DE REUNIONES
Google Classroom
Durante el tránsito de la información
Configurable por cada alumno o apoderado para su propia cuenta de Google.
Posible para los asistentes, a menos que el anfitrión o administrador desactive la opción
Microsoft Teams
Configurable por el colegio o, de no hacerlo este, por el usuario para su propia cuenta
zoom
De extremo a extremo
Configurable por el anfitrión de la reunión


Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS
PARA UNA CONEXIÓN SEGURA A LAS CLASES VIRTUALES
¿CÓMO CREAR UNA CLAVE SEGURA?
Usa una extensión mínima de9 caracteres
Mezcla letras mayúsculas, minúsculas, números y símbolos
Utiliza frases fáciles de recordar como pedazos de canciones
Nunca uses datos personales, nombres de familiares, RUT, direcciones o teléfonos, etc.
Ejemplo contraseña segura:
MI.C4ncion(Favor7Ta)

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.

- Julio López Saa
- Maurice André Poirrier Chuden
- Yasna Ivette Andrade Mascareña
- Aldo Esteban Valladares Horta
- Ewald Beekman
- Camilo Iván Mix Vásquez
- Ricardo Andrés Monreal Llop

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.05 16:25:43 -03'00'