Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

30-07-2021 | Año 3 | N°108

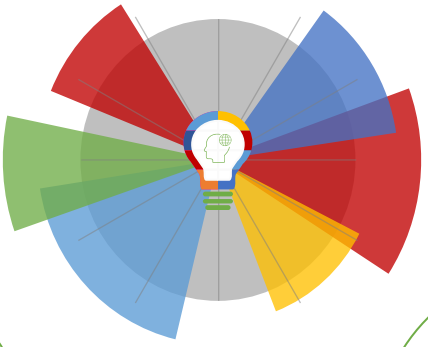
Boletín de Seguridad Cibernética

Semana del 23 al 29 de julio de 2021

La semana en cifras

Hash
24
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
8
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
5
para vulnerabilidades
Las mitigaciones son útiles en productos de Apple, Zimbra y Trend Micro.

IP
72
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

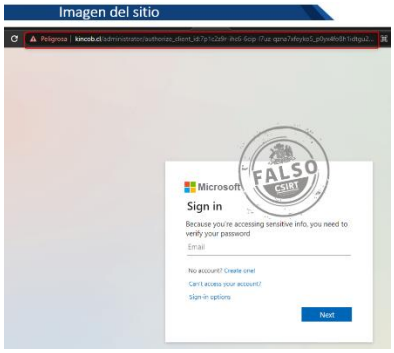
IoC Ataques de Fuerza Bruta

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.

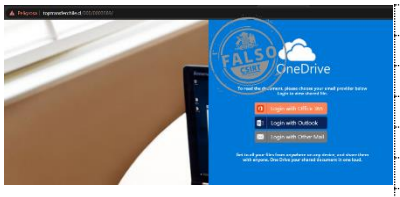
IP	Etiqueta de sistema autónomo	Documento web
37.0.10.7	Serverion BV	4IIA21-00041-01
5.188.206.234	Technology Advanced Investment Limited	4IIA21-00041-01
5.188.206.235	Technology Advanced Investment Limited	4IIA21-00041-01
109.95.180.76	BDINET TYLSKI spolka jawna	4IIA21-00041-01
45.144.225.205	Serverion BV	4IIA21-00041-01
203.159.80.190	Transferred to the RIPE region on 2017-11-22T23:30:38Z.	4IIA21-00041-01
31.210.21.220	Serverion BV	4IIA21-00041-01
45.133.1.102	Serverion BV	4IIA21-00041-01
170.239.54.81	Latin American and Caribbean IP address Regional Registry	4IIA21-00041-01
45.133.1.58	Serverion BV	4IIA21-00041-01
5.188.206.199	Technology Advanced Investment Limited	4IIA21-00041-01
103.25.86.61	ApnaTeleLink pvt. Ltd.	4IIA21-00041-01
136.144.41.70	RIPE Network Coordination Centre	4IIA21-00041-01
87.107.159.144	Pardazeshgar-raay-azma	4IIA21-00041-01
195.133.40.83	Des Capital B.V.	4IIA21-00041-01
43.224.182.88	Panchsheel Broadband Services Private Limited	4IIA21-00041-01
31.210.20.48	Serverion BV	4IIA21-00041-01
5.188.206.197	Technology Advanced Investment Limited	4IIA21-00041-01
45.144.225.204	Serverion BV	4IIA21-00041-01
5.188.206.196	Technology Advanced Investment Limited	4IIA21-00041-01
37.0.11.124	Serverion BV	4IIA21-00041-01
103.241.243.9	Apna telelink pvt ltd	4IIA21-00041-01
185.24.233.168	ServeByte VPS	4IIA21-00041-01
136.144.41.87	RIPE Network Coordination Centre	4IIA21-00041-01
91.192.207.68	Niles sp. z o.o.	4IIA21-00041-01
196.0.86.62	Uganda Telecom Ltd	4IIA21-00041-01
45.144.225.206	Serverion BV	4IIA21-00041-01

103.156.91.43	Representative office No. 2 of VietServer Services technology Ltd.	4IIA21-00041-01
45.133.1.109	Serverion BV	4IIA21-00041-01
138.122.37.41	Latin American and Caribbean IP address Regional Registry	4IIA21-00041-01
45.133.1.100	Serverion BV	4IIA21-00041-01
5.188.206.195	Technology Advanced Investment Limited	4IIA21-00041-01
2.56.59.87	Serverion BV	4IIA21-00041-01

Sitios fraudulentos

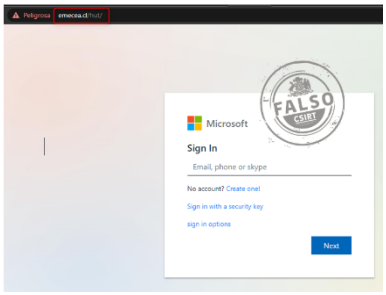


CSIRT advierte ante página fraudulenta que suplanta portal de correo de Microsoft	
Alerta de seguridad cibernética	8FFR21-00994-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de julio de 2021
Última revisión	23 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
http://kincob[.]cl/administrator/authorize_client_id:7p1c2z9r-ihc6-6cip-l7uz-qzna7xfeyko5_p0yx4fo8h1idtgu256czaswvqnr9bmjk7el3zwbr9logy856iqfm204cdpavek31xn7stujh2xafs07pog1ru53lkmn49dctw8ivbzjyehq6?status=putuser	
IP	
[186.64.114.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00994-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00994-01.pdf	



CSIRT alerta de página fraudulenta que suplanta a OneDrive	
Alerta de seguridad cibernética	8FFR21-00995-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de julio de 2021
Última revisión	23 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
http://toptransferchile[.]cl/000/0003589/	
IP	
[162.241.114.223]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00995-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00995-01.pdf	

Imagen del sitio



CSIRT alerta ante página fraudulenta que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR21-00996-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
http://emecea[.]cl/hut/	
IP	
[192.185.173.74]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00996-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00996-01.pdf	

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta a Outlook Web App	
Alerta de seguridad cibernética	8FFR21-00997-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
https://sweetb34rokacik[.]ru/zxcv/d78ebf41ac9c1ce9eb100f5ed023ed74/	
IP	
[103.153.182.55]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00997-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00997-01.pdf	

Phishing

CSIRT alerta de campaña de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00420-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de julio de 2021
Última revisión	26 de julio de 2021
Indicadores de compromiso	
URL de SMS	
bit[.]ly/Alertas-bchile	
URL sitio falso	
https://xn--prtpsas-bhl-l-rdbg9ihi8e9egf69bb77kcgf52b[.]com/1627311110/bcochile-web/persona/login/index.html/login	
IP	
[66.29.137.55]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00420-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00420-01.pdf	

CSIRT alerta ante campaña de phishing que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FPH21-00421-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3zbcUjL?l=www.tarjetacencosud.cl	
URL sitio falso	
http://www.tarjetacencosud.cl.intra[.]az/	
IP	
[185.22.155.185]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00421-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00421-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidad en productos de Apple	
Alerta de seguridad cibernética	9VSA21-00474-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de julio de 2021
Última revisión	26 de julio de 2021
CVE	
CVE-2021-30807	
Fabricante	
Apple	
Productos afectados	
macOS: 11.0 20A2411 a 11.5 20G71. iPadOS: 14.0 18A373 a 14.7 18G70. Apple iOS: 14.0 18A373 al 14.7 18G69.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00474-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00474-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en Zimbra	
Alerta de seguridad cibernética	9VSA21-00475-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
CVE	
CVE-2021-35208 CVE-2021-35209	
Fabricante	
Zimbra	
Productos afectados	
Zimbra 8.8.15, versiones anteriores al parche 18. Zimbra 9.0, versiones anteriores al parche 16.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00475-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00475-01.pdf	

CSIRT alerta ante vulnerabilidades en productos de Trend Micro	
Alerta de seguridad cibernética	9VSA21-00476-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
CVE	
CVE-2021-36741 CVE-2021-36742	
Fabricante	
Trend Micro	
Productos afectados	
Trend Micro Worry-Free Business Security 10.0 SP1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00476-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00476-01.pdf	

IoC Malware

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

Recomendamos 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	Tipo de malware	Documento web
02c10e4943caad34e424ca72a545a2d416b73eee0d3099d80e2ee3cb86c1932f	MSIL/Kryptik.ACCR!tr	2CMV21-00205-01
18321caf87215750bb9821aca4c50c13de7d30e69fa056e1894f644332043909	MSIL/Agent.GIQ!tr	2CMV21-00205-01
1a94be42daac6ce93b9cb5564934898f2b1bdcfbd24c9db7d37b9e04639a49d9	MSIL/Kryptik.ABZB!tr	2CMV21-00205-01
239ab5d4355bfbeb28962fa372ff4004d94f5aa7d5c423be9c84548c521908fa	MSIL/Kryptik.ABZB!tr	2CMV21-00205-01
3fc21fc6c204930b144bffcd4eb0ad572908533a199e2008e1508613f9be785e	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00205-01
44064d93545f38520fcadc58302473ea99087deb716b245fcec3d3bd78b9ba34	RTF/CVE_2017_8570.VQR!exploit	2CMV21-00205-01
5c602bf190d06a7b541c9629bd48bb63745ef463c24e572c7a285f9891e507ec	MSIL/GenKryptik.FHZB!tr	2CMV21-00205-01
6a61427fa26132640faa4616ef57d8d13785f8f73e2697720e036da63c7acdf3	MSIL/Agent.GIQ!tr	2CMV21-00205-01
6dd997c225f5e598cb1cfe95b5689a51599cc0f4b8f1dfa610f92a63469c281f	RTF/CVE_2017_8570.VQR!exploit	2CMV21-00205-01
6f7d6ab9dd45bebc793602779f132e11a28884dfc688f7710cdad670931e9864	MSIL/Kryptik.ABZB!tr	2CMV21-00205-01
7409ceb633397a1854309a81169d6391bb87abd66705baf71abcdbad755c500a	MSIL/GenKryptik.FHZB!tr	2CMV21-00205-01
8d3dcceb1f017ceb60e22af0abff3f67095eb9327068e38eb872ccb7570d7779	HTML/Phishing.5532!tr	2CMV21-00205-01
8f5b6b2c0c2204797c4b29217eab69c341fe06d8cbc6f54f9ac04481f17861f9	MSIL/Agent.GIQ!tr	2CMV21-00205-01
9c203a23b7ca95d7b840c9e3fa451d691a2e8a53df5e22bd1c872a55acbdb386	MSIL/Kryptik.65DA!tr	2CMV21-00205-01
b7f4d8718eed4813c9326fa3e977e7dfdd6de80e6b597db61a9c5583c755dfed	RTF/Abnormal.F!tr	2CMV21-00205-01
ba7731b6dc348e539c3e92a30f7811579de525f4346b223430b0b668e68e30c0	VBA/Agent.1873!tr.dldr	2CMV21-00205-01
c435ee050c32e9de7560a2f0b9f08b7a9b3919c7761bdb2140fc7f80d16fe35f	Malware_Generic.P0	2CMV21-00205-01

cfac96c006899be8f8793a5da85b1264c5b7a696e e7bc775262d2082c534e4be	HTML/Phish.BMD!tr	2CMV21-00205-01
d1b4347d7887ca25444518b4250fcde245d9136a 79237ef28b5f93f355c6c2b8	W32/Injector.EPVF!tr	2CMV21-00205-01
e273e3fe4d92b5b08db5cbd12db9542fba9aa559 c3cfde3fe5e4c52d3dbdb7e7	MSIL/Agent.GIQ!tr	2CMV21-00205-01
ee7979d6fd168eac5e0cdfc2438e99454ff3b6144 c9e08133bc255073b028d4a	MSIL/Agent.GIQ!tr	2CMV21-00205-01
fa963d4d83f84c063302d32d411f535cbd496553 9869e2752efda5d0d267c2bc	MSIL/Agent.GIQ!tr	2CMV21-00205-01
fe04378dd45882a26898da0e74a054847878eb1d 9b4515edb317d5c30805acd4	MSIL/Agent.GIQ!tr	2CMV21-00205-01
ffaddd9987582634ac6b9e8955b3a85caaf1a4a96 f410cd931455d630a76de3c	MSIL/Agent.GIQ!tr	2CMV21-00205-01

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
209.85.167.69	Google LLC	2CMV21-00205-01
77.105.0.60	Orion Telekom Tim d.o.o	2CMV21-00205-01
45.137.22.67	RootLayer Web Services Ltd.	2CMV21-00205-01
77.247.110.225	PEENQ.NL	2CMV21-00205-01
185.222.57.156	bd-rootlayer-1-mnt	2CMV21-00205-01
208.70.251.202	Colocation America Corporation	2CMV21-00205-01
185.222.57.68	bd-rootlayer-1-mnt	2CMV21-00205-01
103.139.45.212	Trung Hieu Services Trading Investment Company Limited	2CMV21-00205-01
185.222.57.94	bd-rootlayer-1-mnt	2CMV21-00205-01
185.29.10.119	Virtual Servers	2CMV21-00205-01
5.181.166.234	Heymman Servers Corporation	2CMV21-00205-01
185.29.8.39	DataClub S.A.	2CMV21-00205-01
159.65.97.226	DigitalOcean LLC	2CMV21-00205-01
200.10.184.122	Corporacion Administrativa del Poder Judicial de C	2CMV21-00205-01
167.89.60.5	SendGrid Inc.	2CMV21-00205-01
40.107.236.50	Microsoft Corporation	2CMV21-00205-01
200.55.203.148	AFP Habitat S.A.	2CMV21-00205-01
170.233.152.50	Latin American and Caribbean IP address Regional Registry	2CMV21-00205-01

167.89.62.71	SendGrid Inc.	2CMV21-00205-01
167.89.58.195	SendGrid Inc.	2CMV21-00205-01
170.233.152.67	Latin American and Caribbean IP address Regional Registry	2CMV21-00205-01
209.85.167.181	Google LLC	2CMV21-00205-01
170.233.152.49	Latin American and Caribbean IP address Regional Registry	2CMV21-00205-01
170.233.152.61	Latin American and Caribbean IP address Regional Registry	2CMV21-00205-01
209.85.208.71	Google LLC	2CMV21-00205-01
209.85.208.72	Google LLC	2CMV21-00205-01
209.85.210.71	Google LLC	2CMV21-00205-01
209.85.216.69	Google LLC	2CMV21-00205-01
40.107.95.83	Microsoft Corporation	2CMV21-00205-01
209.85.219.169	Google LLC	2CMV21-00205-01
209.85.210.69	Google LLC	2CMV21-00205-01

Actualidad

Director del CSIRT de Gobierno lidera Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de la Cooperación y Confianza en el Ciberespacio de la OEA

Esta mañana, el Director del CSIRT del Gobierno de Chile, Carlos Landeros, dio inicio y dirigió la Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de la Cooperación y Confianza en el Ciberespacio de la Organización de las Estados Americanos (OEA). Estuvieron presentes en la reunión, realizada de forma completamente virtual, los líderes de las instituciones nacionales y gubernamentales encargadas de la ciberseguridad de los países miembros del Grupo de Trabajo, junto a los representantes de la OEA, encabezados por la Secretaria General del Comité Interamericano Contra el Terrorismo, Alison Treppel.

Uno de los principales motivos de esta reunión fue la elección de un nuevo país líder del Grupo de Trabajo, posición que fue ejercida por Chile desde 2019, con México en la vicepresidencia. Las naciones partícipes eligieron a Isaac Morales, Coordinador de Seguridad Multidimensional en la Secretaría de Relaciones Exteriores de México como nuevo país líder, mientras Estados Unidos fue elegido para la vicepresidencia.

Más información sobre la jornada, aquí: https://csirt.gob.cl/noticias/director-del-csirt-de-gobierno-lidera-tercera-reunion-del-grupo-de-trabajo-sobre-medidas-de-fomento-de-la-cooperacion-y-confianza-en-el-ciberespacio-de-la-oea/.

El Comando de la Semana | No. 10 Comandos para hacer u test de stress

En la sección El Comando de la Semana de hoy les traemos a TSHARK, un *sniffer*, programas dedicados a rastrar y monitorear de forma constante el tráfico de nuestras redes locales o externas, analizando los flujos de paquetes de datos enviados y recibidos.

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.

Se puede encontrar aquí: https://csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-10-tshark/.

El Control de la Semana | No. 5 Política de Control de Acceso

La Ficha de Control Normativo que compartimos esta semana trata sobre las mejores formas de establecer controles de acceso, 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://csirt.gob.cl/estadisticas/el-control-de-la-semana-no-5/.

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.

- Osvaldo Fuentes Escobar.
- Jorge Portilla.
- Maurizio Mattoli.
- Andrés Aldana F.
- Jair Palma.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.30 12:19:07 -04'00'