05-01-2020 | Año 2 | N°70

Boletín de Seguridad Cibernética

Semana del 29 de Octubre al 04 de Noviembre de 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.

Gobierno de Chile

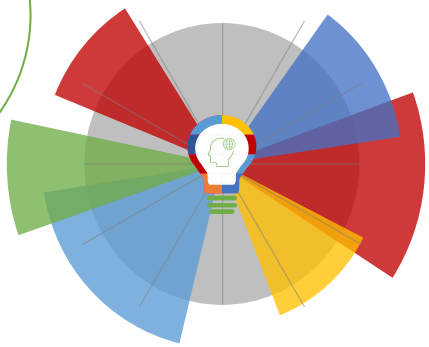
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras

Hash
28
Sha 256
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron
12
URLs
Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches
16
para vulnerabilidades
Las mitigaciones son útiles para productos Windows, Chrome, WhatsApp y Samba.

IPs
107
Informadas
Listado de IPs 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 advierte de sitio de suplantación de login de cuenta de correo	
Alerta de seguridad cibernética	8FFR20-00815-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Octubre de 2020
Última revisión	30 de Octubre de 2020
Indicadores de compromiso	
URL	
https[:]//google-services.com.devland[.]cl/index.php_archivos/index.php_archivos/index.php_archivos/index.php_archivos/CheckConnection.html#identifier	
IP	
104[.]168[.]194[.]208	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00815-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00815-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio que suplanta a web de energía extranjero	
Alerta de seguridad cibernética	8FFR20-00816-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Noviembre de 2020
Última revisión	01 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//energy.gov.procurement.bidnet.atacamalex[.]cl/auth/index.html	
IP	
99[.]198[.]101[.]234	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00816-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00816-01.pdf	

CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00817-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Noviembre de 2020
Última revisión	01 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//bancoestado.cl.iusm-cm[.]com/imagenes/comun2008/banca-en-linea-personas.html	
IP	
162[.]144[.]255[.]96	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00817-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00817-01.pdf	

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00818-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2020
Última revisión	02 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//mail.zax-associates[.]com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
91.220.196.45	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00818-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00818-01.pdf	

CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00819-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2020
Última revisión	03 de Noviembre de 2020
Indicadores de compromiso	
URL	
http://webbancofalabella.cl/	
IP	
162.241.62.3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00819-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00819-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de phishing bancario por oferta en seguro de salud	
Alerta de seguridad cibernética	8FPH20-00321-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Octubre de 2020
Última revisión	30 de Octubre de 2020
Indicadores de compromiso	
URL	
https[:]//fleetspread53[.]com/?xv6=b0d1c7cd523037cacb62f2c86786f244	
http[:]//scotiapersonasenlinea[.]experthvacandrefrigeration.com/1604071049/login/personas	
IP	
[92.223.65.225]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00321-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00321-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing bancario por cuenta suspendida	
Alerta de seguridad cibernética	8FPH20-00322-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2020
Última revisión	02 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//santander.personascl[.]site/1604318743/index.asp	
IP	
[148.251.94.252]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00322-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00321-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por falsa transferencia de crédito	
Alerta de seguridad cibernética	8FPH20-00323-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2020
Última revisión	02 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//cmmila6[.]pl/cli/enviar03.php	
https[:]//www.phone-experts[.]at/zy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[69.16.209.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00323-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00323-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por bloqueo de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00324-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2020
Última revisión	02 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//login.vumk[.]xyz/personas/	
https[:]//login-santander.pgcl[.]site/1604336197/index.asp#	
IP	
[188.165.0.1]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00324-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00324-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones obtenidas de WhatsApp para su aplicación de mensajería instantánea	
Alerta de seguridad cibernética	9VSA20-00314-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2020
Última revisión	02 de Noviembre de 2020
CVE	
CVE-2020-1907 - CVE-2020-1906 - CVE-2020-1905 CVE-2020-1904 - CVE-2020-1903 - CVE-2020-1902 CVE-2020-1901	
Fabricante	
WhatsApp	
Productos afectados	
WhatsApp para Android versiones anteriores a la 2.20.196.16. WhatsApp Business para Android versiones anteriores a la 2.20.196.12. WhatsApp para iOS versiones anteriores a la 2.20.90. WhatsApp Business para iOS versiones anteriores a la 2.20.90. WhatsApp Portal versiones anteriores 173.0.0.29.505.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00314-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00314-01.pdf	

CSIRT comparte actualizaciones obtenidas de Google para Chrome Resumen	
Alerta de seguridad cibernética	9VSA20-00315-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2020
Última revisión	03 de Noviembre de 2020
CVE	
CVE-2020-16010 - CVE-2020-16004 - CVE-2020-16005 CVE-2020-16006 - CVE-2020-16007 - CVE-2020-16008 CVE-2020-16009 - CVE-2020-16011	
Fabricante	
Google	
Productos afectados	
Google Chrome para Android versiones anteriores a la 86.0.4240.185. Google Chrome para Windows, Linux y Mac, versiones anteriores a la 86.0.4240.183.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00315-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00315-01.pdf	

CSIRT advierte de vulnerabilidad día 0 en controlador criptográfico del Kernel de Windows	
Alerta de seguridad cibernética	9VSA20-00316-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2020
Última revisión	03 de Noviembre de 2020
CVE	
CVE-2020-17087	
Fabricante	
Windows	
Productos afectados	
Windows 10 versión 2004 Windows 10 versión 1909 Windows 10 versión 1903 Windows 10 versión 1809 Windows 10 versión 1803 Windows 10 versión 1709 Windows 10 versión 1703 Windows 10 versión 1511 Windows 10 versión Gold Windows 8 Windows 8.1 Windows 7 y Windows 7 SP1 Windows Server 2019 versión 2004 Windows Server 2019 versión 1909 Windows Server 2019 versión 1903 Windows Server 2019 versión 1803 Windows Server 2019 versión 1709 Windows Server 2016 Windows Server 2012 versión Gold Windows Server 2012 versión R2 Windows Server 2008 versión R2 SP1 Windows Server 2008 versión SP2 Windows Server 2008 versión R2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00316-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00316-01.pdf	

IoC - Malware

Se comparte a continuación el listado de IPs que fueron detectadas durante la semana pasada por el Equipo del CSIRT intentando ejecutar escaneos de puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad.

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
015aaecbeea372d2cde18c72ef93ce742b3e8c3ddf7247918403295dfa7357b5
0213f39e2bd4830d8d51e23e421396ba63f2dd763ee30b14e93be50e6260e9bc
07b12baabc51749df13d78cc093496d641f03a1aed14ee0ecb867e2a4a2d70d5
1b4a65a4c674b33eb2c9d88cd1e9e44a67b2344f27caad6868d5423a4d6f73c8
1d0a436d11e82575e2d3159ad264e3a58bb3caa9f6638ee4b8a94a5373219628
2176a02ebbadceedea35c2a83fcce17fd40120ff2cc4390a9f210fc26b40a310
2371e0e135a47c424d7d495b502671d79498f2d6b046c20b9b780bc05ca36205
2d94f5620906f353b2bda6b6eb984695737cdecd6ddc88ca747fad5bc457d090
2efeab91d822ab76173df70e491b2cd6881d1435186ad6659da73c4e5c5214bf
2f9bd3cdb00bfc460e34a3397631cec4c68a88396709dcd19f4ffd4ede764fa8
336b84aa55993361e79fde52e5427d3c545ece50df3b2faafe811b3e03557e62
34d2852606570037 91b2816bffed0a723c26806adb1483d592fb38d3f04d1943
3cc938a9acddafc3e794e45e9e82d1c24efc3d811739899713c21d96ca510711
46e694bc430fde3727a791bbc879a7d3b9d84b4572c4a26ee59127d1bb0b227d
4937e26d4bf2f3ddd43cfebe507c1ad452c29cab1451e7685e24045e74cf514b
54ca61ec982bde21aeaadab8529cd81e950e26421934c016f6997720420e4e61
651b29b58ee39b2e950b47f9c71d76e9db2051ca7ada24a41d784cb33d8427cc
72394ca2be1e27dd4702d4e02caad4d284420bd177124477909eafeab530f41a
8ceb329d808d01facd5a35eaab98066ccd470f311da7fa0fc11f61e8340e51a0
9143453f9dd04d35a094a0332fdc37a1d517cc582db210673a79310a26505e65
a4587f4066fee8762f410d564c2f5acc9fd245292213beb4ebafe6d1f92f9c71
a692ebd8ffaf553afe6a7e4b21ec46977dfc073877399130d26bcb1aac0ec33e
b89f3ae4badac97fc44a153bfb215de77641bff4cbcbe7ddc321af38e097f2be
c864f510cfcaca5ca5acb2a8ef66706e173195d47f0bc0956f1757e9f74325d1
d51925f43c610d0116c831c9282a4b3fcbca83fce4a02bde7f425d81eb7a2243
e30eceea75b291ff394ffb670b46a3b07e8725dc0a146c1df069952d9ed885a9
e4c4aa874feb371209199ddd6b159ed4a677b94568dfe6b09351807263dbef9b
fdd08f8a983b5fc70a146d936dc6ef6d53ae736a3eed003bf193343704e5ad47

Direcciones Ip de servidor SMTP donde es enviado el correo malicioso
185.222.57.240
50.116.1.181
173.247.245.167
192.51.144.19
200.73.116.8
210.245.92.234
210.131.4.98
31.210.88.198
192.190.84.36
199.201.89.23
103.252.255.62
210.131.0.52
150.95.29.49
117.54.5.10
89.251.48.76
103.217.93.32
203.191.33.81
195.29.150.125
185.222.57.71
37.49.225.155
54.240.8.18
37.46.150.190
156.54.7.82
217.61.130.193
185.222.57.73
60.36.166.21
154.66.197.58
203.138.177.2
103.12.211.45
45.126.132.221
92.54.18.66
66.96.185.7
66.96.188.1
167.89.82.128
65.254.253.43
66.96.185.6
66.96.188.2
185.222.57.249
77.68.31.54
200.6.114.185
104.148.61.186

Correos electrónicos de donde son enviados los archivos adjunto con malware

alamgir@multitex-bd.com
alertasyavisos@bcp.com
amalina@mustika-ratu.co.id
arun.natarajan@pff-group.com
c.fernandes@idee4.fr
compliances@khfl.co.in
ConsulTransExt@bcp.com.pe
eldosespaul@fleetship.com
esquivelplumbing@bellsouth.net
hr.sp@happyfamily.co.za
huong.vu@adrem.com.vn
info@ivorist.com.tw
jeffreylai@kpmg.com.tw
kouyos@educet.plala.or.jp
martinez.sabio@economistes.com
master.V7A2203@globeemail.com
miyagawa-sui@nst-sumisys.co.jp
muhasebe@zumrutparfumeri.com.tr
n.mataka@ud-eng.com
nst-honsya@nst-sumisys.co.jp
nwe-support@clealink.jp
office@shenzhentoptrade.net
phanuwat_p@globaltel.co.th
raandaya@comglasco.com
recepcion@dt-sa.com
ricardo.martinezb@bbcconsultores.cl
rusmi@tigermp.co.id
saravanancbe@msashipping.com
sk.tan@advhse.com
thuy.nqc@namyangdelta.com
trading@expoalimentos.com.ec
twokings992@gmail.com
ured@os-marijeiline-umag.skole.hr
vanessa@frimaster.com.br
wandaver2@gmail.com

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) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP
5.188.206.201
45.150.206.113
45.150.206.114
45.150.206.115
45.150.206.116
45.150.206.117
45.150.206.118
45.150.206.119
78.128.113.118
78.128.113.119
78.128.113.120
78.128.113.121
109.238.186.169
144.217.178.248
185.234.219.227
185.234.219.228
185.234.219.229
185.234.219.230
193.169.254.105
193.169.254.107
193.169.254.109
103.133.109.40
103.253.42.54
103.75.197.69
113.64.92.98
141.98.10.136
141.98.10.143
141.98.10.192
141.98.80.74
141.98.80.76
158.69.115.206
176.111.173.15
185.234.216.66
185.234.218.82
185.234.218.83
185.234.218.84
185.234.218.85

185.234.219.11
185.234.219.12
185.234.219.13
185.234.219.14
188.255.178.58
193.56.28.183
212.70.149.5
217.217.179.17
37.49.225.198
45.125.65.105
45.125.65.39
46.29.160.113
58.214.10.242
58.221.47.236
72.11.135.222
77.40.2.120
77.40.3.144
77.40.3.238
77.40.61.10
77.40.61.110

Actualidad

Ciberconsejos de seguridad para compras online

El Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT) y el Servicio Nacional del Consumidor (SERNAC) elaboraron el siguiente documento, con la finalidad de explicar los tipos de fraudes que utilizan los delincuentes para robar datos personales u obtener ganancias económicas y cómo identificarlos rápidamente.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberguia-de-mediacion-parental/

Investigaciones

Implementación y configuración de MISP para compartir información de malware

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la edición n° 21 de su publicación sobre Análisis de Amenazas Cibernéticas. El presente artículo elaborado por Miguel Kurte, analista de nivel 2 de CSIRT, analiza brevemente la plataforma MISP, ofreciendo una guía para su instalación y conexión. El presente trabajo pretende fomentar entre sus lectores el uso de esa herramienta. Las primeras dos secciones del documento buscan definir en términos generales que es un MISP y cuáles son sus características generales, para luego enfocarse en los pasos que deben considerar los administradores para instalar, configurar, sincronizar y conectar herramientas MISP.

Ver más: https://www.csirt.gob.cl/reportes/an2-2020-21/

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 del mismo.

- Gabriel Irausquin
- Hugo Salgado
- Valericio Carrasco