CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

07-01-2021 | Año 3 | N°79

Boletín de Seguridad Cibernética

Semana del 31 de Diciembre de 2020 al 06 de Enero de 2021

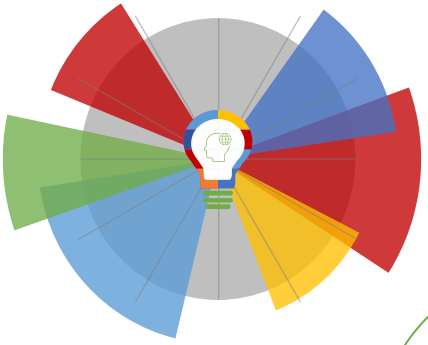
División de Redes y Seguridad Informática. Gobierno de Chile

Ministerio del Interior y Seguridad Pública. Gobierno de Chile

Resumen de la semana en cifras

Hash
90
Sha 256
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
11
URLs
Asociadas a sitios fraudulentos y campañas de phishing



Parches
14
para vulnerabilidades
Las mitigaciones son útiles para productos Huawei, Node.js e IBM.

IPs
111
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

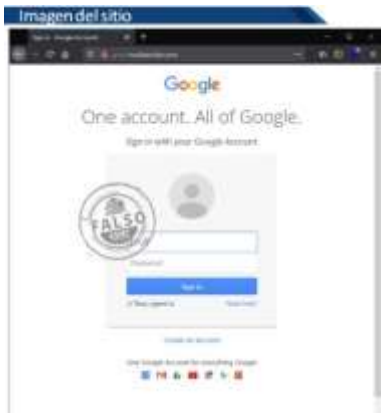
Sitios fraudulentos

Imagen del sitio

CSIRT advierte sitio de streaming falso	
Alerta de seguridad cibernética	8FFR21-00864-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
URL	
http://netflix-premium[.]gozviral[.]com/	
IP	
35[.]208.201.212	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00864-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00864-01.pdf	

Imagen del sitio

CSIRT advierte suplantación de página de software	
Alerta de seguridad cibernética	8FFR21-00865-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2021
Última revisión	05 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//uniqueacademysje[.]in/images/sa/hotmailattach/	
IP	
160[.]153.128.36	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00865-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00865-01.pdf	



CSIRT informa sitio fraudulento de servicio de correo electrónico	
Alerta de seguridad cibernética	8FFR21-00866-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2021
Última revisión	05 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//gmail.molliesmilez[.]com/	
IP	
192[.]185.52.10	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00866-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00866-01.pdf	

CSIRT advierte sitio falso de programas informáticos	
Alerta de seguridad cibernética	8FFR21-00867-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2021
Última revisión	05 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.login.microsoftonline.com.authche[.]cf/	
IP	
18[.]221.255.34	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00867-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00867-01.pdf	

CSIRT informa página fraudulenta de sitio bancario	
Alerta de seguridad cibernética	8FFR21-00868-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2021
Última revisión	06 de Enero de 2021
Indicadores de compromiso	
URL	
https://sms-personascl.live/1609935057/personas/index.asp	
IP	
[198.54.116.205]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00868-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00868-01-1.pdf	

CSIRT informa suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR21-00869-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2021
Última revisión	06 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//mobilewifi[.]rs/com_k2/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
http[:]//mobilewifi[.]rs/com_finder/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
[91[.]223.162.35]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00869-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00869-01.pdf	

Phishing

CSIRT informa phishing sobre un falso crédito pre aprobado	
Alerta de seguridad cibernética	8FPH21-00347-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//web-banestado-cl[.]gq/credito?token#mpiib6cbqg131	
IP	
[185.104.152.200]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00347-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00347-01.pdf	

CSIRT informa phishing de SúperClave inactiva	
Alerta de seguridad cibernética	8FPH21-00348-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//login.vumk[.]xyz/personas	
https[:]//login-santander.personascl[.]online/1609772783/index.asp	
IP	
[103.102.239.119]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00348-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00348-01.pdf	

CSIRT advierte phishing de actualización de correo electrónico	
Alerta de seguridad cibernética	8FPH21-00349-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2021
Última revisión	06 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//bcsalaharamikutia[.]com/file/.zm/correo/index.html	
IP	
[103.153.182.185]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00349-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00349-01.pdf	

Malware

CSIRT advierte campaña de malware con supuesto presupuesto solicitado	
Alerta de seguridad cibernética	2CMV21-00126-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
Hash	
EDF88C4B92F71C83DE456D1D0191C9385C0F86213DD34B578D1D0F99FC93004E	
8F10623DB4FC1E8289A02E94DB58942A94A25C59A06E559FA910094DA3DB7E9D	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00127-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00126-01.pdf	

CSIRT advierte malware con supuesto correo informativo	
Alerta de seguridad cibernética	2CMV21-00127-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
Hash	
CFDE1FB313A0CE73984E005F1AD21BF37D6E0052B474500A8550C552D00EB16B	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00127-01-2/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00127-01.pdf	

CSIRT advierte campaña de malware con supuesta factura de pago	
Alerta de seguridad cibernética	2CMV21-00129-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2021
Última revisión	06 de Enero de 2021
Indicadores de compromiso	
Hash	
BEFC59F442467A63D160C1A04B424C73087D398E8BD1870D8950E8E7C97C0B30	
CFEA06D5F9BC813FCB6446F194BA79D8A5D1ED001AFA55CE312CB85F36D7A28C	
EC810BF129F8ACC2DDD94E9761C34BDF7A071DD8041A4F74E410524EB9BE8A6F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00129-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00129-01.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones para Huawei	
Alerta de seguridad cibernética	9VSA20-00350-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2021
Última revisión	05 de Enero de 2021
CVE	
CVE-2020-1866 - CVE-2020-9203 - CVE-2020-9209	
Fabricante	
Huawei	
Productos afectados	
Huawei NIP6800: versiones V500R001C30, V500R001C60SPC500 y V500R005C00. Huawei S12700, S5700, S2700, S7700 y S9700: versión V200R008C00. Huawei Secospace USG6600: versiones V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500 y V500R005C00. USG9500: V500R001C30SPC300, V500R001C30SPC600, V500R001C60SPC500 y V500R005C00	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00350-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00350-01.pdf	

CSIRT comparte vulnerabilidades obtenidas de Node.js	
Alerta de seguridad cibernética	9VSA20-00351-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2021
Última revisión	05 de Enero de 2021
CVE	
CVE-2020-8287 - CVE-2020-8265	
Fabricante	
Node.js	
Productos afectados	
Node.js, versions de la 10.0.0 a la 15.5.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00351-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00351-01-1.pdf	

CSIRT comparte mitigaciones obtenidas de IBM Cloud Pak System	
Alerta de seguridad cibernética	9VSA20-00352-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2021
Última revisión	06 de Enero de 2021
CVE	
CVE-2020-4917 - CVE-2020-4928 - CVE-2020-4919 CVE-2020-4918 - CVE-2020-4916 - CVE-2020-4913 CVE-2020-4912 - CVE-2020-4910 - CVE-2020-4909	
Fabricante	
IBM Cloud Pak System	
Productos afectados	
IBM Cloud Pak System, versiones 2.3.0.1 a 2.3.3.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00352-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00352-01.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
ab6351d009865510df2ab196ad544a306ca97528739ce1f23b1e66d11ef5c9f0
328547d8fbddaf5087390a97bb4bd2032672e5ebda3e6c867bb5093cde59cb5d
707b4a55407d98ee3fdfa52aa7f7afc101c9840d61c3d57dd449a2855112f03b
f0cf111e03d080fc06a4e72970255b3d16b8aa7b2177d9b4bf6d9a396c9b65f2
33c69e52458fad394a63c6b518ada88882b2f76f105aa3372125ee57ae82ede6
915ebb0d27b6bce53b727f89cdec18014f4d40edb99e75cb7d77cea94c2d2f11
60c055641f936f338ca340c4ae2919b4f545217ba8f991ae83b2d6706c19f6cf
5ad9ad89dbd1685f3a5aa45c7d74492a9ca134b6308aa1e94f157d1fd897cc8d
226677eee73124065c8011188279cff2018066cba9f06e88da86a130b174bec6
40678b0dd69ff9a00d4bf0a194bf42e7868b9374159ace3a9bc94a7f463d89b1
c64f02177df8516f4af183607151236e1a6761d533b900777a18384fe38b1ce1
0745ec389f93d672009867300d2cbab8ed00bad2db9496fab3f62a649e156943
54413a3364d7383be6a49ec65e0c3f16f662b84ba5c59968b60fcee797714cf2
fc54284371340d5ee0e9de0094b70280b063294cc1408866edeb19387215462a
7a0c3c2563056d616fc421c5d432bcb659b934093b470899af981fd321a162a4
7e02cee4970608058fda2b43e61217bcf29977b2f2339fc77ba5be871de1b130
eea58b2b0043981ad90b971ebe83901ebcefceda806a25b6eaf21408b3d3a689
c89d8cf447d03687818fda76021467eb01ca57915644cc3516ed2b47d99b3eb9
68f339174767db80cb1578578631e93ff0ca10f79e575271ced080937a3f3159
555882aa0c70bf9f62ae71584a9e5e18353d6126de19390f8c2859c15693764c
fa91514bcf7bf7d49942a9540a1d515095c09cd936dae7f0073647dff6249c37
ed554fe56ab46d0e27c0febbe54663474540030391fb638542a4beead28f8ae8
ce77e9e1fe235b5bcda9dd1e3db5ed575bd397a7e5f96da2775491ee0c23639c
bc60a50738caeabfcd59cfc7f355ad5fcb5ac7d0b57afd7d96aef09e6eca8b0e
403df2e81bbb1cbe0b761a68962a96d99082642fb0f7764a1f7ea057c7854988
57573ae812bd40b5f1f02c9098899b026dbe071fddd98c0f39e979e542925274
54496830b594a269cf3ec9c90a9358b797f967912c3e7ee8c6a8da7f31135f12
c17d21ceb8f0d7793ea5c6f7cb0278569d96642bec9dad54cab3c249bb3d9fd4
1b815075fbe2801ca89c6f4227c9ae2fdb2275698791758ef57f7073fd4d0d6f
906f8cd4e47a854b5529ec1ba4e7af7a9429b6cdb09772e8cc661a0071cd46f8

7fdedf2abac344613c34295f9709038790437c77b65f72491def7dc2ea11aa08
f0473363310244862950 3a0b0df30e77c694298c6e2bac53b89099f796a4a04c
eedc56307590cb415b9388656d7287000bf530c10ab8c8c1f8bf4875321c2398
6e9366c10b06f94a3e436527ed163f7b68c4a81f911d593d64e6312d7b0e39b8
2f410493048157fd2bccd80a02a83ad071a7b37038ab5fb6160ff9d6d1312522
d315e07599f48461af20a81347aae5972ba5aea6210a0e28244b902a18cefc78
68f2889fb26be5dfaef1c55d3d1509e9a6b88f12ad89c8f869bf829d463ef59f
3a68f92f681e5348c3753dc5ff6cbe0f652f0fdcc581cf727a8bfd99c52f77f0
38d17dfd9fc5d7eb04a6ed019750022081fd13b253d0eb08d92fd9109815ec52
f1ff8d81d84d73a186c72546b5efdc3abd4f4a91243d0f2bb537cc1418d8bdae
401e09065cc4fe70319e8924de8ab2ace957de8a65a2a1ac15330fdfe2f9c092
773a15b11264f83c09890cedbb7aedc943a30430f5b355d38e5625f2ebd3fb8f
9b5ceeadb9d26cc60561054e3ea318e82923f3b04a9e505aeb8750ef4b3d902c
269b7e9055041b22adcfd3f3d1d0a4711292eb08c8674a535071c2ccf27a31fd
dc9236f8bdf3716d6ad5bd3fc91beab4505cfe0585682cc68064718e9680c53f
63162fe833789ed99b85cf9524ce3254d7f676c2a187f7e2c2ecd23ad59ac5c0
d4e6f646fefbec70addba05ff09663419b87f9639b77c91ed711cadebd38f1da
4ce9c1ba330aeca51cd7b8f6b7e1796c1ead42dde6868d7a5fd636b9a3a9f4f9
3a7192ae0a86e22de203cd0bd9c3b2ddae45e918207d4ad84f4cfe6b1d975c95
1f3408d6afcfe5d362d5ff3499a030b245b4f62883dca94f64bea90ac430fc24
f5e030f99b3221f7b2d8b52bce2b0b913b2d183c3f7bd5016bd17ddbfe0be793
c468614a769e571b1c2ca14280030b4c2ba662c84c293f1c8eba3013acedb1dc
0daffdebae76adc451e7450a0655b6cdb1755cf372b24c67e462531a3a535469
145466e49f1ebf4ed38896709a64733353a2389bd676b7ef055c79637f53c082
7bb94464b3d84793306c5871494ec5b557815c2dee93f5ff5ba01e1fe7c85d88
bd71cb5216319d67b7163d101b227e46c1b8172480c96aee9172be8670c32fbf
335244fcbcc6009ad28d75a6dfe0349e05900474914247fa1170d8aa92d7e988
17c93d81b95f2b725804776e87495cb9c024cd0c25c389dbb1931bfe5b335824
3f3f62535aec0a614e68f5b3cd747165c445e75ea4ebe33f94906643cdc59ef2
8781ae428abd96615cd293485c613d369872793f18196da555f90664fe739aca
dd6c7639d37dd74a6c38509064836fb8ad9d39f8f7dade457d5bc5557bcf64da
02593420fb4231788dd0e0512424a6f7314f4879bd6251a8f373713fcf21d123
2c0780a1e89c3eaee48f329332ed55c2b272af466f82d20e0d91c97bd1ca36f3
82d7ccf8a708facd6356a918e9930803db68740bffed556687da9891ebb7910c
918b035fa23083286866d7ab947c9fc167e3e9c398b7e6e83cb7169056ae43d5
046eca51b5320c60641116cde38fc1f11ba67cfeb38ee1abc034e8ff05733324
e11d4e5bcc76c2fd3a7cdd203d329daeaa1819a854c9e43096625f0efaa7cf0f
f8f286a03f9077ad8f3a28d55f3a36839714d8939a2d5ec9b6d1fa0b6f15a2d6

436ca025416de5f2e4b98d6112bdcf6677f2c9398b8c7a2e1e644a5717916014
fea083de9b31b49497005d6f38cc508f73e1853f6563eb2775257b8a48b9ff42
04fa2ec3d0efb179ea69fc29e6c0e6daa8b409de0bf51e4a9c67d150a1bd3b23
8eb70d010ca662e71b14616b3939c6b40722ef1e40c1b7822b972177150fb345
6dbcc0255f24c2876b32acaea6ac383eb2995ef52d51806db60df781d4b15e54
7a51e8dcde57b5c660458c92066f4c69487cc9744367150724316852815 5c9e5
9c2c5917f69605a3c17204d2d1aa7c95b2e6cbd92840c85e52c6dce965b9ba98
0614f4be806c4157708ed39928754468081f972f73b31c990e9b66f3bba05c4d
c965992bba351d9e718017dbf01acba42b1f8a42602f26000c9c1a07460b7e5f
706a19b0ff78fefb6808c5832c447d9a8283c62cc1ecbe98c8080d1cbba8b881
3b4484e3fbdb11633142fe67123007cda529580b734a81044d8827a6480e9233
dc5ca596e8b79ce0402bc63258f8494a2e836700dedb32153708f7bc711e3fb4
5e0b310151e5c233f7c7876f5bf0576ebbd42a25c344ded180114607428afb78
a784af36e65ec0e7a189cb17abcde4fbecbb95e87bc34dd1bcdae5d639e6be1c
c32677479dab9138f3439c5a09f0d9b0a707b3aa71ccda84c297c2c0f5fad452
56f1f482c0c6991b2732a1332161e67eb97338eaf3db3edcc5495015c5fd56e7
f3efc2e5997e186211e391501b22d5fb0127c1415d96e27455669d22e498ccea
afa53bc493798be5f623e757b93db30cd9ba85e82202c2d697b56e67ebb431e1
944b7940e6d91589c998cb7f62b847b2cc65292e82e66eb0727d48c9ed15a4b5
38ea911347b44aac8f665e2e717f82d8568e814339f64865ccac87c0e54584ff
edf88c4b92f71c83de456d1d0191c9385c0f86213dd34b578d1d0f99fc93004e
009126d3c2a00d870169209de28569da3db9aaf2d48e4c2efc44ea274cf12baf

Correos electrónicos de donde son enviados los archivos adjunto con malware

account@charutarhealth.org
accounts@dmppuae.com
accounts2@seawheel.com.sg
adrianw@k-d-wolf.de
Ali.Mirza@hidro-insaat.com
amar.zunaira@asiainsurance.com.pk
arc.west@nifty.com
armond@internode.on.net
as.chirurgie@spitalcopiitm.ro
atefosman@daralemandubai.com
chandara.gb@medai-group.com
chinhpq@apectrans.com

contabile@gruppovalleimpero.it
contabilita@speedlog.org
cuentas1@blipack.com.ar
d.moustapha@self-assurance.fr
doxon.gm@doxon.jp
edp.pv@magicmaruti.com
f.soleimanzadeh@mammutteleca.com
faiz@justap.ae
franz.eversheim@eppa.com
h.azarkamand@mammutteleca.com
info@aquabros.jp
info@garagezuid.com
info@gia-caucasus.gr
info@mtcclc.com
inovacii@fitr.mk
ivan.adric@os.ht.hr
jackkurz@highspeedsolutions.com
jeffrey.alburqueque@jprtelecomunicaciones.com
jetro_vicente@dt-factory.com
khalid.pervaiz@aasenterprises.com.pk
khanhmq@pigeonlog.vn
khurram.ahmed@itenablersglobal.com
laboratoriocancun@conquimex.com.mx
liyq1@sinoair.com
luisa.tapia@plasticaboris.com.mx
mgrac.nexa@magicmaruti.com
muhasebe@zumrutparfumeri.com.tr
mustafa-khan-jam@icmjapan-to-carib.net
nam.dao@htmlogistics.com
naser-de@scs-net.org
naveed.waheed@dadabhoy.edu.pk
olivera.zafirovska@dukovskiconsulting.mk
paolo@batiksrl.com
paqueteria.salta@correoflash.com
pm01@ddoverseas.com
reception@amazonfoods.ae
rehman.ali@afzalelectronics.com.pk
roberto@erreviricambi.it

rodrigo.veto@veto.cl
saeed@amazonfoods.ae
sales@bdpave.com
srinivasan.sv@johnsonliftsltd.com
sujin@mcl.com.my
sympathique@wh2.fiberbit.net
telesales.kb@magicmaruti.com
tengku_qusyairi@tmmsb.com.my
trucking.hpg@apectrans.com
ured@ss-obrtnicko-industrijska-zu.skole.hr
vimal@ethix.in
werkplaats@garagezuid.com
w-hi@scs-net.org

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

62.149.156.105	192.185.143.47
65.254.253.175	192.185.45.133
65.254.253.196	193.198.233.96
86.106.170.120	193.238.102.69
87.253.234.100	195.8.209.16
87.253.234.152	202.129.241.99
87.253.234.162	203.124.41.30
96.125.173.240	210.131.2.91
173.201.192.102	210.2.153.132
192.185.149.105	211.129.7.126
205.147.111.116	212.8.231.116
210.211.117.200	219.143.232.5
212.227.126.131	98.142.105.18
213.178.226.251	23.83.209.13
103.141.97.52	23.83.212.26
103.31.82.190	31.210.88.198
103.82.198.114	54.156.49.34
103.82.198.115	182.75.98.252
103.82.198.116	62.149.156.75
103.82.198.130	62.162.71.33
103.82.198.133	66.228.55.251
103.82.198.134	66.96.185.3
103.82.198.135	66.96.185.9

103.82.198.136	66.96.186.1
103.82.198.137	66.96.187.1
103.82.198.138	66.96.187.10
103.82.198.91	66.96.187.2
104.145.234.96	66.96.187.4
104.247.72.249	66.96.189.6
113.23.215.81	66.96.190.5
116.58.56.122	185.255.84.197
121.83.220.206	188.118.50.140
124.41.211.69	188.121.43.193
139.198.17.248	72.52.142.75
150.101.137.10	77.105.37.234
150.101.137.13	80.241.246.3
156.54.13.62	81.91.176.150
159.8.83.126	88.208.216.50
173.63.149.23	94.156.46.244
181.30.0.186	98.142.105.18

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
141.98.80.99
5.188.206.204
37.59.160.147
167.114.57.100
199.192.16.253
212.70.149.85
212.70.149.54
103.156.92.189
91.134.169.23
171.112.195.200
193.56.28.190
78.128.113.69
37.49.225.207
141.98.80.99
96.47.230.238
103.133.109.40
77.88.224.66
144.217.199.2

Actualidad

Ciberconsejos para unas vacaciones seguras

En ocasiones, los padres tienden a publicar en sus redes sociales fotografías de sus hijos, una práctica que si bien parece inofensiva trae asociados algunos riesgos y consecuencias que pueden ser perjudiciales para los menores.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-unas-vacaciones-seguras/

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 del mismo.

- Felipe Hernández
- Claudio Valderrama

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.08 15:13:40 -03'00'