Alerta de seguridad cibernética	2CMV20-00068-01
Clase de alerta	Emotet
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Muy Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2020
Última revisión	18 de julio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información recopilada de múltiples campañas de phishing con carga de Malware Emotet.

El fenómeno, que se inició el día de ayer con manifestaciones a nivel mundial, también ha sido detectado en campañas con énfasis especial en Chile.

CSIRT hace un llamado a las organizaciones públicas y privadas para que tomen las precauciones respectivas a partir de la información recopilada en este informe y alertar a los usuarios de sus sistemas para extremar precauciones sobre los correos en las bandejas de entrada y advertir sobre los peligros de descargar archivos sospechosos.

Los indicadores entregados son muestras obtenidas por CSIRT, así como de fuentes abiertas comprobadas.

Mensajes de correo electrónico - Chile

TODOS

Próxima reunión ordinaria el viernes

Por favor ver/revisión adjunta.
Por favor hazme saber si tienes preguntas. Gracias.

Atentamente,

Querido colega,

Encuentro extraordinario

Por favor ver/revisión adjunta.
Por favor hazme saber si tienes preguntas. Gracias.

TODOS

Puntos del planificador de reuniones

Por favor confirmar.

Sinceramente,

Información de los correos electrónicos

Asunto
Reunión previa a la ley
Hoy - Reunión de presentación 1:00pm
Hoy - Reunión de presentación 1:45pm
Hoy - Reunión de presentación 5:45pm
Todos deben asistir a la reunión de mañana
Solicitud de reunión de profesionales de empleo exprés
Encontrarse pasado mañana
Encuentro extraordinario
Muestra reunión del miércoles 28 de jul

Adjunto
Todos deben asistir a la reunión de mañana.doc
Reunión mañana.doc
Nuestra reunión el viernes.doc
Puntos del planificador de reuniones.doc
Reunión no programada.doc
Reunión 27 y 28 de jul.doc
La reunión se llevará a cabo el viernes.doc
Reunión regular el viernes.doc
Reunión de oración.doc

Sender
motsumi@mateyss.co.za
ketoan@dec.vn
facturacion@isgbc.com
sakai@teinet.co.jp
horii-k@officebusters.com
ntalledo@constructorarodema.com
malarcon@ferreteriamadrid.cl
ad5.rmf@redmeatfood.com
jestinah@established.co.zw
reception@raneenmep.ae
casaqorikancha@cuscogastronomico.pe
stock@classyhotelspa.com
operaciones@boltsandtools.com
natalie@ardena.uz
r.taha@alturki.med.sa
hse.bpo@quick.com.co
ketoan@misaco.vn
trodriguez@induser.com.ar
sunat@metalboard.com.pe
info@travelmice.com.tr

gerencia@clerysa.com.ar
omalque@tecnomarket-sa.com
dan.plg@phanthietgarment.com.vn
resa2@dlghoteldanang.com
natalie@ardena.uz
ebihara-k@tsuchiya-corp.com
karla.puente@key.com.mx
k.hariu@urban-palace.com
resa2@dlghoteldanang.com
logistica@metalboard.com.pe
vinayak@haassouthindia.com
nieuwemorgen@breede.co.za
trodriguez@induser.com.ar
seguridadsocial@quick.com.co
gg@handsgroup.com
gt2829@greattree.com.tw
manjushree@phs.ae
tech707@next-engineering.com
lauris@sfc.com.pe
silvana.paz@newmaq.com.bo
gt2829@greattree.com.tw
manjushree@phs.ae
lauris@sfc.com.pe
silvana.paz@newmaq.com.bo
ventas@metalboard.com.pe
economicos@gobmex-sp.org.br
renee.bonneau@registrarcorp.com
rajitha@eaglepower.lk
wendy@twcopto.com
balsas@speedy.com.ar
jesus.alvarado@key.com.mx
sugaya@md-kikaku.jp
hr_pingsilhouette@hotelartists.com
ecommerce@efhk.com.hk
silvio.cesar@saaejacarei.sp.gov.br
sky-blue@chengda1.com.tw
madeleyne.gutierrez@digetelperu.com
garbancera@superdelnorte.com.mx
ratchadapa@ratchatravel.com
carol@ontime59.com

Url descarga archivos Emotet

http://tarisfotografi.com/aup/Overview/
http://movie.cxyw.net/fork/LLC/jj0av1ems/xrgxn858627574n193e6s4zoqd2/
http://teste.hoonicorns.pt/ddfcn41dj/payment/epwsnm/
http://demo.xoweb.cn/static/public/yn4g1lj32bix/
http://www.leonardoenergie.it/media/balance/
http://watkins.mitchellpwright.com/wp-includes/docs/lg2wm6zn/sxhgff291213969722cb2tpmjwffm/
http://linhkien36.net.co/wp-admin/browse/
http://www.mikesar.com/cgi-bin/FILE/9iy3rbp/yc697386432801482480z1o1srx37/
http://exchangecamp.ir/wp-admin/Documentation/
http://www.gdstechnologies.co.in/app/eTrac/
http://akzy.top/h8ioc8/Documentation/
http://www.ajanews.asia/wp/Document/5r65712504026116389jmyzp09zw2b3sfn63/
http://www.aumhealings.org/wp-admin/docs/1izhzmhbo/
http://ulfhorror.com/wp-admin/83279465106718/7fkhh84265327972167057acuknjrmhrfbxz9bdd/
http://steelworks-students.com/wp-admin/FILE/ype8vbeho2jn/
http://longphuong.tk/wp-admin/browse/buz7el/
http://pasca.fapet.ub.ac.id/l/sites/
http://drive.medisail.fr/lib/INC/
https://doraflob.com/fef2/Document/
http://ranks.hoonicorns.pt/comp3/Overview/00giwvmzhy/s04054954269w9vtvn5tqlan/
http://www.timelyrain.top/wp-includes/ID3/parts_service/enlbnfk4xl/
https://koncenful.com/wp-content/lm/hmhj52/ook7ri689941810111164mlk5ffuksnm6anf/
https://daniwilkinson.co.uk/dup-installer/sites/3u01718046821pkh6l38v42wa3e1eiw/
https://max-hoffmann-webdesign.de/eTrac/
http://aarunya.in/wp-admin/swift/3jc4jqgai3rf/98382623658csjsmcfrnnlx032w6e9/
http://elilaifs.cn/wp-admin/parts_service/jecxwnaz1j/
https://gayasianporn.men/wp-includes/docs/
http://www.calzadosyaccesorios.com/wp-content/plugins/wp-optimize/cache/balance/6uum399349075e49y7zg5lmhju/
http://misuperpodereslaprogramacion.com/wp-includes/459766/f9bk24443570nsfmvcorb3d0fs0/
http://hyundailamdong.com.vn/wp-content/LLC/z9uf09t/pf4c2866715286295d0poxdviz16wlsy8/
http://elnasr-co.com/b36ybn/parts_service/81mv7870218z8fosnwspopk3th53i4/
http://batdongsanthanhhoa.xyz/wp-admin/esp/syx8t7sa7pn/
http://benjamin-jauernig.de/bilder/parts_service/
http://mikesar.com/cgi-bin/rqag0gz/
https://kettaravision.com/wp-includes/Reporting/1g89974878316032719mibv1xp63/
https://computerfamilie.com/wp-admin/sites/5zbl583454520034794wvuqb80aka/
https://letu8888.com/wp-admin/report/ck165923294108833875trpu7qznfted/
https://jacksinspiration.com/wp-admin/sites/2fipqcb/
http://www.joycareu.com/9re/payment/luv7f9hd/
http://zeing-kor.com/b/common_array/open_12aprkbzsnv01y_4uawa/87933126050098_FOkxEXj/
https://kompenas.org/wp-admin/open_disk/corporate_portal/ffn_tytwu1u928t/
https://kettaravision.com/wp-includes/Reporting/1g89974878316032719mibv1xp63/
https://jacksinspiration.com/wp-admin/sites/2fipqcb/
https://www.ziyuan.tech/wp-admin/Documentation/
https://qrtalk.nl/wp-content/docs/f6k3vrc0/
http://www.mikesar.com/cgi-bin/rqag0gz/

https://hightea.tk/wp-admin/LLC/uxblj70750248131jyb5yjz51vq9r3zg0yo/
https://steer2vision.com/recurringo/Overview/t8oku994412361893ciornz3iuaysczvm/
http://akzy.top/h8ioc8/Documentation/
http://cleardristi.com/cleardristi.com_WP_INSTALL/g84oq8lq9ek_d0qdnl3l0gkrr_module/corporate_wkg55rof6x_cf5kxjphwqyz/who5_06y576/
https://ideanetsolutions.com/wp-admin/multifunctional-zone/guarded-mglbz8f9qqm-77foumy8y423bo/ZqnWyCb1ePV-yhG1xbpjL/
http://cellstore.net.br/wp-admin/protected-zone/interior-zgirj9bvpgy5ef1-0z7d5cqgj949/KL4SoBjA0s-nGbvgduN/
https://www.chinavok.com/wv7kv/multifunctional-gmgtAcb-XzR6tiFghuo/additional-gN3u1-JPwnriOV0YM/wg7hzo1jit-0sus2x/

Hash SHA-256 documentos Emotet

999f7f6c8abe867a0f8a80c3fa71b8603564d29f8257f3734c8fd3817d6a11a7
5f6d8525a28494c7eda3df2fbb04bcacc9ec20abd2884a8e690d91a2de033807
56ca979add889f731b0f90db151af8bb24a5688a0a071e7a78d3811be6081dc5
1121d769f4ee470a79e5a236b6e7d8ee08a59516ddf0551fdc26b76a82ca819d
285c7162332f6110b4d4425cbdf3f969e78051bffa4baf5fb0b536200f6de4e9
17349a4713477389332878314d893e7719798a93f8f9a69e7784901234dab8af
209e82fa6ae3e04595cfe5be6748f7edf64322f7a941cc0dea71cdfa58d67b16
aa1a0ff9b42a8d686ce043eebdd511b76c27e8222269bdc8df22216bc188a533
9affebf9743a24814684c2e6b915db97652fbebf374ce6847c90b555b2df48d0
0c1bcdbdacd25aad1e0618a72d12c8ed3b0f0037dc5054db556a2a5ebe22eea9
2174d0d833b48c8e309505713db7531193b28067d0b033a98fa9c41953b652ea
b4c406d1484f59bda24f2f02c9029284f1113222c321f3f4306550c728df8c5c
b69be57ed72b61452b73f2690fd2240aefad9f90f34c2af1663ad26f0a5b2f30
0321dcc5d416f60aa5a24e206e06a2f787dc3021fa9a4589508637668f25c892
235905e0f1e943ece9739738d7eafbe365d0b86d3e8c80453056e6cf5f94df17
25941d1dac273e9438afe0bf0b3a913474ff21b6c559c8f9c5a1820eac5e6281
e9cdb9eed210e1ef9fef04891b1739922b435e2ca30c9dd18cde8d79c4c25c4f
45833b34f285a5105d355c15d2afa190b86d1875763e42f531185263227e1d93
f441acc4d711bcbbdf09e71a85e3c8e18b635bd1b20fcbf6a86432ea328a7614
6e6bf8344fb9473bb6804815ea6162440c958a04e41ce815f048034b6f4d4f3e
c1897c410a839fa5e18b492ba4b120752f8e9aa18c63b45ff2b62df7a02fd5ec
ba43537a550f2717f37cfaeab08736c06e5dc3c8aa1b780876842c5aebc57559
039d3c16562212063e5d5fabb2cbc3c783f134c0e073a13c900d3d0aa2904bb7
f909c6fc593985a3df36c86b32588edbbf3e2c43a7020a8a32b081ec3153139d
443db428583d6cdc78e5b36275f584a95900cea3318fe31c41025d6800f72392
603250a8b6b9eb43a05e0b98498b77a7cb8b5a1fac668262ee07a24986a08670
40ff69629d016b471e8d629757c3cd4ab76c1958b851d9484fe5b9f12bd05b20
7e40afbfe1b4cb286d03bc2af804c66f01eef9b144d77d2d593b78e2eef9efd0
140826ff8504695349da93d44b8cc8bc99720a9c4155b14653f7924beaba8e52
98ff83d44d2a1d8e59aa9c90d56ac4c6fb1bc08ccf6320d7e0956075e7f8d059
3f4547463b7ed3f83a9fe1f4aa956bf8e5302f0181fab9c1357d98f80ca8017c
1b571fc563b1cb2aad093ccdb4f872510cb7f649942195fa2fb627eaf1bfe8e2
c4fef70e62aafcefd6600e91edd401ccd941dae7472d89fd2cb164219eeb34f3
6264e94597601ac38cf03e59970036714ef4047d46a6c16f2de4716a4aee449c
328a1ddb0998b010e99d5314354fa47de97745a0e09b6682e043ffba500f19cf
2f2bf71ff720e834455f232dad3c4c5a0b4e7a0160fe14230fd7d73e3b394883
4cb454edded5fb4393844fee5acd13a0e5b1ff881c2c184d01fd42f38fe99ec9
273b63046e85b9089957375db46fa53bdf6544588f42c68ac859af27aa61688c
48f75ed1957f7f219b5e20a94be45fff1825fb354e2272871fc678731e71a1d4
770fd6643c934cc3aa0fddf589d643b7b59e18a005ff89fc9113bd8181c21a2f
493accf3563320001bb8c5d727fb01bd790bdd20df7f179b12e771330274ddfc

e90c88a5cbec9eb57a69658a28abc2a72c188a4d8b491e8df5b855fbb1ba950a
169f03cee2b674a04eb777235895e2e6d94f82785fac8764ebb330df2bf2448d
1ca54edf6c4dd0c896bea1dcf8000035c111adb890a2d2d395489c1c3b24d6e6
211a160cb4b1f9b0166c5701cffe1b3f47ebd10d59d0899a1ad0dac6dac1e855
4bcb1fe8e41fb17f8088e6227be73e271a53a7f22123e115ce320f50f2b6baf9
61a437bbed8e3ac3a4641ce788de7880516f124ad0a3223f107e92fb0cf969ea
7a13fe46e41ca646a1cc4e3cfeeb88c4d2079abb75c5fe6c5ad0c2d1aacbed8c
8b8ccd4f24be195ddf2b59efcacfe6486785230cc152b5a31a5f5e217050a8ae
a0d3eeaae4f459d8f244b90d97b4b8a40bca8daae995e676e4a4307e98a8e2bb
d0fd2d71c1267d3ad20bbc348b043e49ea7eda9acbfbc30e64dafb296a1a9011
e7aa68a37366fdb984c4f06b66b571cc67ff6ffd25f6af3064f8e684f1f7c26c
ea488cfef075f8314cbc01390816578b77f0f03778254e6a802d18e5e764daac
f1ba4f3b21895f22266d2e46aebbe34552096de287c3b64a9975a5f81c18fffc
169f03cee2b674a04eb777235895e2e6d94f82785fac8764ebb330df2bf2448d
1ca54edf6c4dd0c896bea1dcf8000035c111adb890a2d2d395489c1c3b24d6e6
211a160cb4b1f9b0166c5701cffe1b3f47ebd10d59d0899a1ad0dac6dac1e855
4bcb1fe8e41fb17f8088e6227be73e271a53a7f22123e115ce320f50f2b6baf9
61a437bbed8e3ac3a4641ce788de7880516f124ad0a3223f107e92fb0cf969ea
7a13fe46e41ca646a1cc4e3cfeeb88c4d2079abb75c5fe6c5ad0c2d1aacbed8c
8b8ccd4f24be195ddf2b59efcacfe6486785230cc152b5a31a5f5e217050a8ae
a0d3eeaae4f459d8f244b90d97b4b8a40bca8daae995e676e4a4307e98a8e2bb
d0fd2d71c1267d3ad20bbc348b043e49ea7eda9acbfbc30e64dafb296a1a9011
e7aa68a37366fdb984c4f06b66b571cc67ff6ffd25f6af3064f8e684f1f7c26c
ea488cfef075f8314cbc01390816578b77f0f03778254e6a802d18e5e764daac
f1ba4f3b21895f22266d2e46aebbe34552096de287c3b64a9975a5f81c18fffc
0a64798861089c14e40315e3b16a49b9fbe503f4cce3daacd2642728ff93ada9
135e53da5e208b721976fb0d4ceedc1cfff80ce5c30b70dfe903e781c8abcdea
1b974503fc4101d5c1035b95fc3efc29222a4bcffc09aece30c2e23ed86300a6
387d77c8e6f2bec88f678ba342d4e032d11a1b5ff4f8dbe7bf7fddc024445ef0
54f8740ffab35d14e05c039a433737452d7f3de5ea39227e493f83efe74aa59a
5ca300850e158b2968b590e3773a084fce54b7237723d2d1657415a642da3f31
5d120f70cd581faa4efdf88f603b50b4b50131d95874ab20bdcaee60772a9a99
7a733d17086e931aef853d510622e89dc2edee5b4f214f92b8b523ac8d73e19a
98a334015ccef973f6cf29c6374beba0d1a636ff5ef5f5b18f16a475bc136b94
a721a61fa7fea85fc4bd19f57585f03699ee0fc58d003432e9669f985f90817f
b3907f1b5e2e21fc65f193d50bd16992dc9dc41a8565d5073a37cbff1d725fb9
bf169dd24062fe8bc98c6e08aac99476670e4e621854f4d00bdc4ab88b50832b
bf72069bdf671e14c551ae12b4b287ab44dc12df4096be4506cb9602154c5421
c0379496fb724eaafc718b7ec2ac362e420ae85098ab5b18fab991af52802193
c3ebbbc69aef85f31e12a81096f8e1d9b83b9ed179efd7e1b0c69cb9eca9dc20
d5606359c71b5217e35ccdb928404788494c2ccbdc3cd2d4026bed510628caec
ec99c82fb7b072159cf6f439d0d7f53c2355bbeb31a963383e35ccdd6cd384d3
f899c40439696439b161e1c4a0b6a1b48d552afde6ce5e136df4bb5cbd3360ea

Urls descargadores de Malware

http://cpads.net/7iuhq/mri/
https://tyres2c.com/wp-admin/zu2h/
https://thesuperservice.com/wp-admin/rL00/
https://ssuse.com/wp-content/uploads/IMv2xyEc3/
http://shubhinfoways.com/p/XEcc5x1qx73/
http://test2.cxyw.net/hyeht3/aWybkzi/
http://sustainableandorganicgarments.com/komentarz/KHF6ry92657/
http://staging.icuskin.com/wp-content/o5hhrj8wvfv372729/
http://defensacovid.com/wp-admin/dGzIMVvo/
http://doorbhai.com/wp-admin/Wq6Kdoisk1r4060453/
http://agilentgame.reviewshell.com/cgi-bin/csoa45gw51315935/
http://karir-up.com/wp-admin/CCzj96yk23/
http://www.szhealthshield.com/websiteguide/k82i/
https://digitalcon7.net/wp-snapshots/0Wn/
https://exam.ylsbmeirong.com/data/tjEyH973/
http://abatiy.com/yaa/po0395/
https://www.20190607.com/wp-admin/ixyjozs/
https://lovely-lollies.com/wp-admin/fgvid/
https://www.angage.com/wp-content/mtincvc /
https://connect-plus.co.uk/aspnet_client/3yey3rr/
http://mapas.hoonicorns.pt/comp3/ly8cmti/

Hash SHA-256 archivos de Malware

2c938f830769a51cb32579935a76223f4aa433ac7e893b2714fc1952bf19dc8a
4069206c26d317894fb19dc5e76abdfbbaba86ac799a86cc432b085931b54c02
44f2c9c71044ba58a54215d12c23b52bf18122070a5e7f1b9df4f48f02c5e44f
52b360aac5fa916627edae6e085f9207d317d39bca9c0407e5baefd33f27df35
6d80126f27ffaafa8de1f9410d5e702cbfc6ff1882d728d2c331eb8bde829a6a
72cb240782df1f5da252a098494ecc3806e638b25e31f9fb9280de2e24c6bb57
750f2c1bb627958e69bb93107570cdc3010101b120a421bbe07f871e46119b80
98ec3c92b6fbbf9411187ec4de8a4e3ae49f6e5fc7b7f03531a4ae6154b58db4
a833d889425e25dd5a581b647abf622af8075190d60238277e4b810ca2e64c67
bf3d8d713b36a34b67d1f952f810ca5287acb1129e8484c575593e5de0ff821e
c9a6bd824b82ead04a1c040c9cfd26a34161877bbe874b84fd40ac0838346804
ca64440bed6daaa0c700aadc73f82f60a7aeedf1bbb682efe1876b2efb084e11
d00b8bdb422e421a9f6dac9ed8860daae48603b2da6b984d7d1abbf78622805c
da2123dcf722cf9fc8c14ff7d6aa8c3eb1f167c40f63caab137ad9c230b37e32
de2e251cef96697f068549e4c51e17f8b1ed1cdae36c5af962b1dc589557c8a8
e67925d34d6d9b769dbe63651c9f47fa1c81a535ad57b20845f88bb21d6fcd1f
ecb86239942ddff646bb234cd21f9564d17596e7cee193b0ed402a2728c11245
ed8f3ec81f977a6d1b386dbfc3dc24b69faedc2a1f8b8a5240c1d45692a39e24