

## Alerta de Seguridad Informática (8FPH-00016-001)

**Nivel de Riesgo: Alto**

### MALWARE EMOTET - PHISHING

Fecha de lanzamiento Original: 01 de Mayo de 2019 | Última revisión 01 de Mayo de 2019

### RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña activa del Malware Emotet que está utilizando como vector de entrada el correo electrónico con documentos adjuntos del tipo Microsoft Word (con extensión visible .doc) y del tipo archivo comprimido (en formato Zip). Su carga principal se enfoca en el robo de las credenciales de correo electrónico para su propagación y luego descarga en el equipo infectado un nuevo artefacto con alguno de los siguientes nombres de programa: “The Trick Dridex”, “Panda Banker”, “IcedID”, “Qbot2”, “Gootkit”, “Pony”, “Nirsoft password recovery tools” o “Infrastructure”, con los cuales establece la comunicación con el servidor de Comando y Control (C2) y realiza tareas específicas según las instrucciones o definiciones del controlador del malware.

### IoC

#### Payload delivery

[https://eternal\[.\]co.il/wp-content/INC/yqd1sn9uxp\\_98byj-936921475830/](https://eternal[.]co.il/wp-content/INC/yqd1sn9uxp_98byj-936921475830/)  
[https://drleisch\[.\]at/euu24ly/KsIZFPXXAsdkztnVIRbyLUAUFGF/](https://drleisch[.]at/euu24ly/KsIZFPXXAsdkztnVIRbyLUAUFGF/)  
[http://webaphobia\[.\]com/images/72Ca/](http://webaphobia[.]com/images/72Ca/)  
[http://sanko1\[.\]co.jp/lp/cJ\\_du/](http://sanko1[.]co.jp/lp/cJ_du/)  
[http://ihs.com\[.\]py/cgi-bin/LLC/XYWKgM1yEZ/](http://ihs.com[.]py/cgi-bin/LLC/XYWKgM1yEZ/)  
[http://icv.edu\[.\]au/wp-includes/RH\\_Xw/](http://icv.edu[.]au/wp-includes/RH_Xw/)  
[http://havenfbc\[.\]com/wp-admin/x1d8e/](http://havenfbc[.]com/wp-admin/x1d8e/)  
[http://fasian\[.\]com.vn/wp-includes/l7qivj8vt61s\\_a54c4ub2do-507402877790120/](http://fasian[.]com.vn/wp-includes/l7qivj8vt61s_a54c4ub2do-507402877790120/)  
[http://epsarp\[.\]com/wp-content/sites/bHgZrPCbDbqAIDAYdnJSk/](http://epsarp[.]com/wp-content/sites/bHgZrPCbDbqAIDAYdnJSk/)  
[http://depobusa\[.\]com/foamorder/tObUfzBc/](http://depobusa[.]com/foamorder/tObUfzBc/)  
[http://best-baby-items\[.\]com/wp-content/Y1CH/](http://best-baby-items[.]com/wp-content/Y1CH/)

Servidor de comandos y control (C&C) de la botnet

189.196.140.187:80  
200.58.171.51:80  
50.99.132.7:465

Archivos adjuntos

SHA-256

01dd700041bb3873945fe44bd9f86585a758bddea8cbc09c4441ee0ae3a3fe98  
05c074ecb60a92bc5b436451c9a3e8bca4be0e5c3c0f797482c78756f2b17d82  
43516fad66f9cc99189e248029ebedbea0eb34957aaa4f88d2e4aa17850c395e  
567c4f99a489d6e26cdd76b719f290108f558cb49b7f5f7e2d84dc8929f7613b  
5f401aefe65751c9e09131d50f1a6ea3f86f542552ecab2973a334a360357699  
6c53c3f9f2d4a2371367019734bed40ff98401090a297b4856b9997df56168ff  
80f34fdc893cca0437d09488e4f69e0ce2f87f0e1f5861fdcf6e6b8e00ee9adf  
8444d472c64cef41e3a0b2f057c208b585b24d5a5db163ccd24cac2501e04ed1  
852e62a35876c8ed552591964b889621a672b89c641a585f84f5b9f043f51f1e  
854cdddb19feff91dc4b4fba1ec91452c996a460cd5bd9ea2ff6e88f8c20f66c  
a79e58fe34d8635a83e7c907f2f32006bcb7c1c0f41861cd313d893ba9132216  
a96a5266998010dd24309a7cd7c1c9ef37099fb2c17c87c5810b2e0a31c6aeb9  
b90d32be34042971e387225c257b0b3ea8ea2a59e73be419e5b4883cf2cf9df7  
b9f24da9d2aaf36536aa8feb72acb2524459815e264e5087c3efa6f59c12d82d  
c7b713458c6bcff31a43f5365d451efa392c0f61506e59af43a58667f06267a7  
c8f4ce1f4f059ec1eb5e216c4a1cec505c3d812bbe82e61a4bb214760e8f6b7e  
e22419b24abf50f5e0895a22b94034dcb8b4d29d89edbb20814947719bd0e20b  
fd0666be8043c1d58b39868e5236856bd32f80fdeb994081e9a1c59974fe101b

Archivos Adjuntos

acuerdo.doc  
nuevo-acuerdo.doc  
contrato.doc  
nuevo-contrato.doc  
Contrato.zip

Sender Original :

academica@frq.utn.edu.ar  
administracion@nauticoolivos.org.ar  
arche-kh@t-online.de  
btv1==024f73a0005==mlaiko@ccs.com.pg  
cartera@hotelcostadelsolcartagena.com  
ciampichetti@marelli.com.ar  
clarionreservations@aumhotels.com  
compras@elytel.arnetbiz.com.ar  
contabilidad@hotelcostadelsolcartagena.com  
contact@panamacrown.com  
contador@redcopmaco.com.ar  
crivellosrl@redcopmaco.com.ar  
dromero@bavosi.com.ar  
fernandozambrano@enoxsa.com  
fivestar3@triplejsaipan.com  
gladis.nunez@gquimicas.com  
gpsafimex@afimex.mx  
guillermo.perez@essa.com.sv  
imprentaparat@impparat.com.ar  
informacion@gruposerefri.com  
javier.ergo@ullamaquinarias.com.ar  
jl-gauna@gaunacomexterior.com.ar  
jose.cortes@lrscapital.com.mx  
loreto.silva@e.vtr.cl  
marcoquioga@quirogacortinez.com.ar  
oscarh@cpinform.com.mx  
planificacion@solorzanoindustrial.com  
plegado centro@arnetbiz.com.ar  
raramburu@tecnapo.com  
reservas@panamacrown.com  
secretaria@pacaloca.com  
secsanpedro@arnetbiz.com.ar

Sender Original :

serviciotecnico@bramaq.com.ar  
shirley@yueshing.hk  
srs0=fzh9lv=tb=consorciolaboro.mx=ana.martinez.b@yourhostingaccount.com  
srs0=x5uyty=tb=wymdesignco.com=aadams@yourhostingaccount.com  
tbgs@transportbgs.ca  
ventas@invefa.com  
ventas-mi@mi.arnetbiz.com.ar  
wakerman@regiongas.com.ar

Smtip Host Name :

mctserver.vservers.es  
smtpout06d.arnetbiz.com.ar  
p3plsmtps2ded02.prod.phx3.secureserver.net  
mail.bavosi.com.ar  
walmailout05.yourhostingaccount.com  
imta-38.everyone.net  
smtpout05a.arnetbiz.com.ar  
mail.grupof.com.gt  
sil.afimex.mx  
imsantv72.netvigator.com  
imta-36.everyone.net  
amazonas.ecuahosting.net  
walmailout07.yourhostingaccount.com  
iron15.vtr.com  
walmailout08.yourhostingaccount.com  
imta-37.everyone.net  
servidor2.minegocioenweb.mx  
walmailout06.yourhostingaccount.com  
mx2.qbasica.com  
e3-1270v3.bl-phx0.1.141.7.4.g1.securedservers.com  
gateway30.websiteswelcome.com

Smtip Host Name :

gateway33.websitewelcome.com  
mail.online.net.pg  
gateway36.websitewelcome.com  
walmart02.yourhostingaccount.com  
imsantv23.netvigator.com  
smtpout03c.arnetbiz.com.ar  
tbjbbihbhedi.turbo-smtp.net  
smtpout04a.arnetbiz.com.ar  
smtpout01c.arnetbiz.com.ar  
gateway20.websitewelcome.com  
116.sipanserver.com  
correo.frrq.utn.edu.ar  
mailout06.t-online.de  
imta-35.everyone.net  
server.pacaloca.com  
smtpout03e.arnetbiz.com.ar  
mailout08.t-online.de  
ns1.coninfo.net

Subject :

El monto de su tarifa para confirmacion  
Modificacion de su tarifa  
Modificacion de su tarifa de 01 mayo 2019  
Aumento de su tarifa por acuerdo  
Aumento del pago de su trabajo  
Cambiar los terminos de pago de sus servicios  
Cambion de pago de sus servicios  
Cambion de su tarifa  
Cargo por sus servicios  
Devengamiento de su tarifa  
El monto de la tarifa por sus servicios  
El monto de su tarifa de 01 mayo 2019  
El monto de su tarifa para inspeccion  
El monto de su tarifa para confirmacion  
El monto de su tarifa para referencia  
Pago de su tarifa  
Pago de su tarifa de 01 mayo 2019  
Pago de sus servicios de acuerdo  
Pago por sus servicios  
Pago por sus servicios por acuerdo  
Procedimiento de pago para su trabajo  
Procedimiento de pago para sus servicios  
Solicitudion de una extension de los terminoss de pago de sus servicios  
Su tarifa  
Su tarifa de 01 mayo 2019  
Su tarifa en virtud del contrato  
Su tarifa para confirmacion

## **MITIGACIONES.**

Bloquear Urls involucradas

Bloquear Sender Original

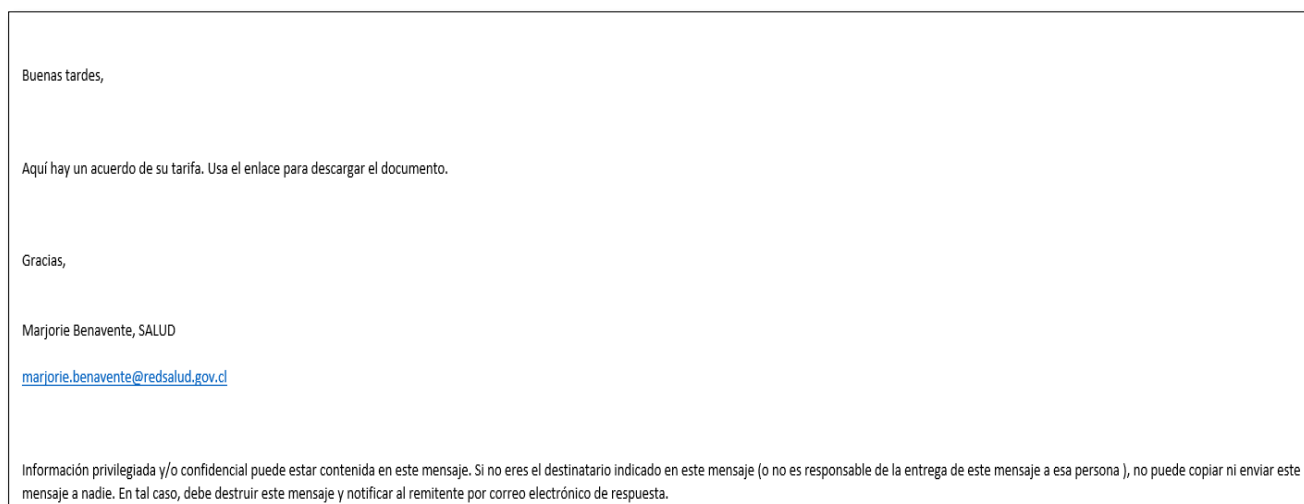
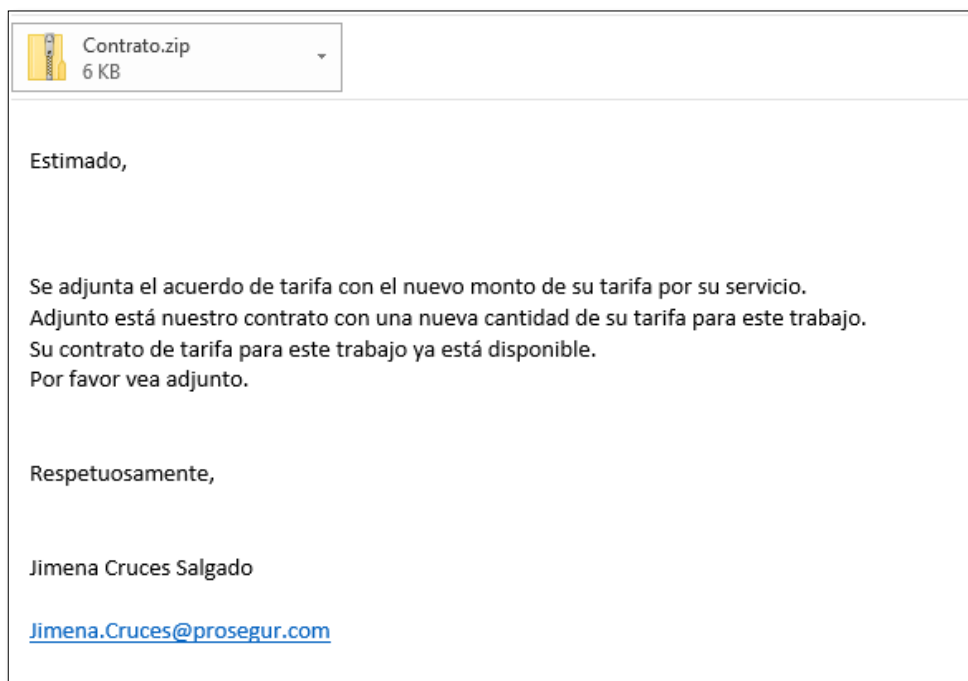
Bloquear Subject

Actualizar las tecnologías de detección de amenazas

Revisar los controles de los AntiSpam y SandBoxing

Realizar concientización permanente para los usuarios sobre este tipo de amenazas

## IMAGENES DE CORREO





## IMAGENES DE CORREO

