Alerta de Seguridad Informática (8FPH-00015-002)

Nivel de Riesgo: Alto

MALWARE EMOTET - PHISHING

Fecha de lanzamiento Original: 01 de Mayode 2019 | Última revisión 02 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 Actualizados.

Payload delivery

http[:]//5elements-development[.]com/wp-content/uoesp16/
http[:]//programmephenix[.]com/wp-content/languages/kjdx0ls2/
http[:]//axletime[.]com/wp-admin/r0gmx40208/
http[:]//bestphotographytnj[.]com/rrm9/lm83yx518/
http[:]//citilinesholdings[.]com/wp/cysk9wh832/

Archivos adjuntos

SHA-256

ee12d6a7678d385cad6d92d505223faf379e765e2e4aa55694b49d462445ae64
5949291f649526ff88f4742c813f89abdcf6e06335b1d42ca740b5e775a58169
7caa4ded7e7be4167ac5991e8a563e231ae9b80813dd36f5618494e30886a700
52977ea9ddbf4be1c05c0ea100009b32ad85f4be401e647c9fe13a3057413c39
da90642a84ccf0e03150cbce192af56cff8e5ec145fde46e2d41a86989219d28
3c76fe0b00eee4d76979eb6f27a9395ff952967b39a6c02e62f5e988ca351cb1
7e5a6e6ecf5554cebd655af3e1db09d80552510bd42af3af1cd364fa84fc788f
c8f4ce1f4f059ec1eb5e216c4a1cec505c3d812bbe82e61a4bb214760e8f6b7e
01dd700041bb3873945fe44bd9f86585a758bddea8cbc09c4441ee0ae3a3fe98
9afded52c30b230da28ab2add95ce4e0e2edc0165737a3a2a49ba51885835e9b
b815dcfbc641aa5025593c3ba7d5fc5b1528e8933eeb2915c8a753cc046c07b7
e2f8c6de5954d3d27891ce947c27df0d04e29beaadc6f75234d281a182b6f240
69e5a7464a6a695ff4a5e2d0204dfa15bc81d7b7620aaee7ae9026f5ce2e2b29

IoC

Payload delivery

https[:]//eternal[.]co.il/wp-content/INC/yqd1sn9uxp_98byj-936921475830/
https[:]//drleisch[.]at/euu24ly/KsIZFPXXAsdkztnVlRbyLUAUFGF/
http[:]//webaphobia[.]com/images/72Ca/
http[:]//sanko1[.]co.jp/lp/cJ_du/
http[:]//ihs.com[.]py/cgi-bin/LLC/XYWKgM1yEZ/
http[:]//icv.edu.au/wp-includes/RH_Xw/
http[:]//havenfbc.com/wp-admin/x1d8e/
http[:]//fasian[.]com.vn/wp-includes/l7qivj8vt61s_a54c4ub2do-507402877790120/
http[:]//epsarp[.]com/wp-content/sites/bHgZrPCbDbqAlDAYdnJSk/
http[:]//depobusa[.]com/foamorder/tObUfzBc/
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@frrq.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
imprentaparatz@impparatz.com.ar
informacion@gruposerefri.com
javiera.ergo@ullamaquinarias.com.ar
jl-gauna@gaunacomexterior.com.ar
jose.cortes@lrscapital.com.mx
loreto.silva@e.vtr.cl
marcoquiroga@quirogacortinez.com.ar
oscarh@cpinform.com.mx
planificacion@solorzanoindustrial.com
plegadocentro@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

Smtp 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.websitewelcome.com

Smtp Host Name :

gateway33.websitewelcome.com
mail.online.net.pg
gateway36.websitewelcome.com
walmailout02.yourhostingaccount.com
imsantv23.netvigator.com
smtpout03c.arnetbiz.com.ar
tbjjbihbhedi.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

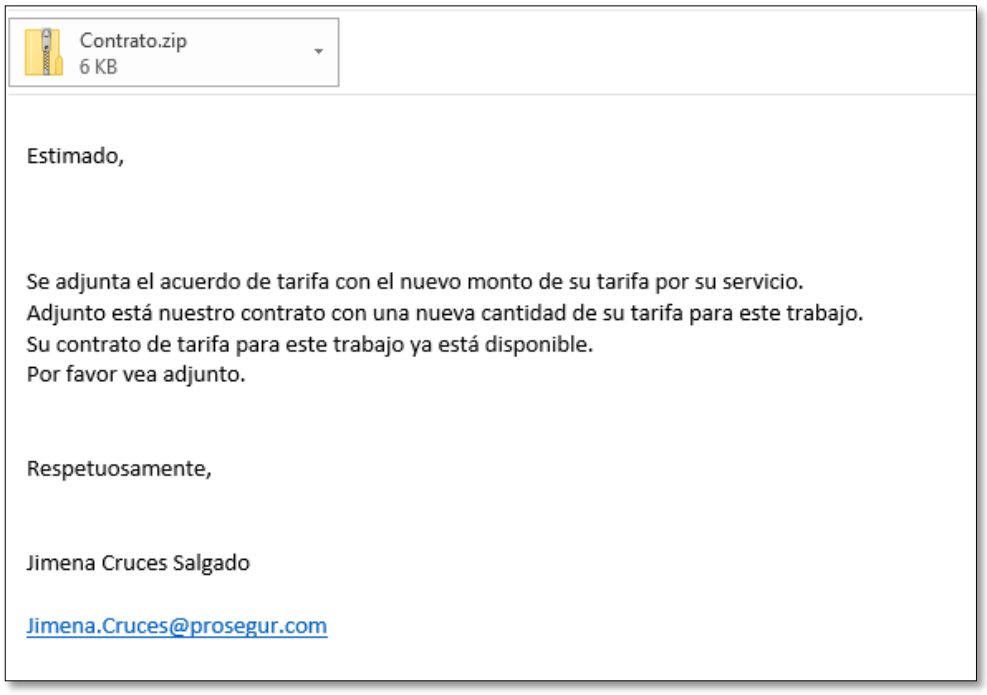
Subject :

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


Contrato.zip
6 KB

Estimado,

Se adjunta el acuerdo de tarifa con el nuevo monto de su tarifa por su servicio.
Adjunto está nuestro contrato con una nueva cantidad de su tarifa para este trabajo.
Su contrato de tarifa para este trabajo ya está disponible.
Por favor vea adjunto.

Respetuosamente,

Jimena Cruces Salgado

Jimena.Cruces@prosegur.com


Buenas tardes,

Aquí hay un acuerdo de su tarifa. Usa el enlace para descargar el documento.

Gracias,

Marjorie Benavente, SALUD

marjorie.benavente@redsalud.gov.cl

Información privilegiada y/o confidencial puede estar contenida en este mensaje. Si no eres el destinatario indicado en este mensaje (o no es responsable de la entrega de este mensaje a esa persona), no puede copiar ni enviar este mensaje a nadie. En tal caso, debe destruir este mensaje y notificar al remitente por correo electrónico de respuesta.

IMAGENES DE CORREO