Alerta de seguridad informática	2CMV20-00047-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware que cita a la víctima a una reunión de trabajo. El mensaje del correo indica que se debe asistir a una reunión con urgencia, incluyendo un archivo ".doc", el cual, al momento de abrirlo, ejecuta una un programa que instala el malware Emotet infectando a la víctima

Indicadores de compromisos

Servidor Smtp

[217.70.178.231]

[216.172.167.215]

[213.246.108.84]

[212.210.215.246]

[211.13.204.73]

[211.13.204.71]

[209.126.121.30]

[207.38.2.144]

[205.207.122.142]

[203.128.6.123]

[203.82.48.8]

[202.229.18.122]

[202.162.241.221]

[202.59.80.59]

[201.183.251.101]

[201.131.19.153]

[200.25.0.165]

[198.54.125.239]

[198.38.82.72]

[198.23.90.155]

[197.242.145.198]

[197.242.145.93]

[197.211.212.80]

[197.211.212.76]

[197.211.212.75]

[197.211.215.18]

[196.205.93.106]

[196.201.244.5]

[196.11.146.231]

[194.25.134.21]

[194.25.134.19]

[192.254.138.161]

[192.254.137.180]

[192.232.192.173]

[192.185.160.12]

[192.185.47.80]

[192.155.241.218]

[190.210.196.118]

[190.183.222.130]

[190.160.0.176]

[190.106.132.238]

[190.61.219.202]

[190.61.250.150]

[190.12.72.151]

[190.0.230.73]

[185.240.248.116]

[185.240.248.15]

[184.171.253.218]

[181.114.224.13]

[178.17.171.99]

[173.243.136.65]

[169.1.20.138]

[164.138.210.180]

[162.241.138.37]

[161.34.20.178]

[161.34.14.216]

[161.34.9.2]

[161.34.2.220]

[158.199.161.242]

[157.7.104.44]

[148.244.114.30]

[147.135.54.119]

[143.202.160.203]

[132.247.16.103]

[129.205.241.4]

[123.30.133.92]

[121.83.254.141]

[119.245.151.191]

[119.245.189.66]

[116.202.87.46]

[111.221.43.203]

[103.254.210.173]

[103.254.84.150]

[103.241.181.154]

[103.110.83.71]

[103.74.54.6]

[103.15.48.141]

[99.198.125.118]

[81.169.214.254]

[87.236.103.22]

[79.96.163.158]

[78.128.60.93]

[72.249.68.136]

[72.18.130.123]

[70.32.94.84]

[69.167.175.219]

[69.36.48.22]

[68.171.210.132]

[67.225.129.56]

[66.113.181.152]

[66.97.34.190]

[66.96.189.4]

[66.96.185.9]

[66.96.185.7]

[66.96.185.3]

[66.96.184.10]

[66.96.184.6]

[66.96.184.5]

[66.96.184.2]

[66.96.184.1]

[66.84.15.151]

[65.254.253.29]

[64.37.52.52]

[61.216.99.188]

[61.112.24.164]

[59.106.27.230]

[54.240.2.18]

[50.31.12.148]

[49.212.207.12]

[45.115.115.27]

[45.115.115.26]

[45.115.115.22]

[45.115.115.15]

[45.115.115.10]

[45.115.115.9]

[45.115.115.7]

[45.115.115.5]

[45.56.110.58]

[34.192.122.33]

[27.254.87.146]

[23.83.209.12]

IP

[42.115.22.145]

[118.98.75.85]

[107.181.187.155]

[41.185.66.173]

[89.252.141.160]

[145.14.144.154]

[43.255.154.93]

[45.55.179.121]

Sender

underwriting[@]sanctuary[.]co[.]zw

envios[@]boletas[.]acor[.]gob[.]ar

brandon[@]triggertimeoutfitters[.]com

socialmedia[@]sgi[.]co[.]zw

ktakasugi[@]mizokawa[.]jp

_administratie_hv[@]hotelvermeer[.]nl

hska-beck[@]t-online[.]de

lhdao[@]ppj-tic[.]com

sumanth.reddy[@]topsgrup[.]com

cuitlahuac_v[@]fypa[.]com

miriam.gomez[@]groupcm[.]com[.]mx

nazca2[@]magher[.]com[.]ar

sekkei[@]rissho[.]co[.]jp

credit.officer[@]grandpalmhotel[.]com[.]pk

shaikh.salman[@]alkaram[.]com

accounts[@]emwt[.]co[.]za

candice[@]wrapacademy[.]co[.]za

a.kazi[@]aletiasolutions[.]com

ganesh.yadav[@]pratap[.]co[.]in

k-murakami[@]sok[.]ohtorikogyo[.]co[.]jp

info.mail[@]eigbox[.]net

sattai[@]eigbox[.]net

iszymanska[@]emerald[.]pl

kelvin.li[@]haiyi-hotel[.]com

nishida[@]as-estelle[.]com

merino.romero[@]graduadosocialcadiz[.]com

cr[@]child-pro[.]com

sale[@]hmgrandcentralhotel[.]com

khalil.najjar[@]ccagrouplb[.]com

claudia.vasquez[@]e[.]vtr[.]cl

abigail.perez[@]groupcm[.]com[.]mx

pbensch[@]vodamail[.]co[.]za

adrianmc[@]imp[.]edu[.]mx

badru.sekamanya[@]dakscouriers[.]com

kelvin[@]progiant[.]com[.]tw

shirasu[@]fcnet[.]co[.]jp

cporzio[@]estudiopalenzona[.]com[.]ar

expdoc.pk[@]globalconsol[.]com

inquiry[@]aletiasolutions[.]com

mansoor.ali[@]yourhostingaccount[.]com

lee[@]eigbox[.]net

yoshitani[@]shinwa-steel[.]co[.]jp

cpn[@]gentiletucuman[.]arnetbiz[.]com[.]ar

comercial[@]evolutrans[.]com[.]br

edwin.medina[@]attken[.]com

raisca[@]mitra-ku[.]com

info[@]yourmedsdelivered[.]co[.]uk

tamara.lapasini[@]vialparking[.]com[.]ar

info[@]zncc[.]co[.]zw

admin[@]gv-pk[.]com

y.tateishi[@]ts-foods[.]jp

info[@]skamorimpex[.]com

sabuj[@]aji-group[.]com

ventas[@]hotelcityplaza[.]com[.]ec

tanja.cerquettini[@]rbiemmetech[.]it

gustavo[@]larocca[.]com[.]ar

kevin[@]swfs[.]co[.]za

tinashe[@]beta[.]co[.]zw

NollT[@]teampannon[.]hu

emilio.lopez[@]juanroces[.]com

HKmikahotel[@]mikahotels[.]com

shogo-kamiyama[@]ways-wp[.]co[.]jp

hyp[@]vw-lagos[.]com[.]mx

thi.dd[@]viethung[.]com[.]vn

gerencia[@]acomputerservice[.]com[.]pe

bilashkp[@]opexgroup[.]com

remuneraciones[@]win[.]pe

exp.nsa[@]transvisionshipping[.]com

erarmendariz[@]chihuahua[.]gob[.]mx

clotero[@]veragi[.]com[.]ar

kumar[@]rconsutlinginc[.]com

rh[@]hotelparadorsantacatarina[.]pt

clotero[@]selservicios[.]com[.]ar

info[@]hotelparadorsantacatarina[.]pt

sophie.ncube[@]simbisa[.]co[.]zw

sales[@]mrzautobody[.]co[.]za

fjddiazf[@]wanadoo[.]es

t-konishi[@]fujikuuchou[.]co[.]jp

tkongolo[@]efcug[.]com

ventasalajuela[@]rolinsacr[.]com

kutishenko[@]newlogic[.]ua

hr[@]kashatours[.]com

shehzadsabir[@]fast-cables[.]com

catalinadeportillo[@]eigbox[.]net

info[@]cmch[.]net[.]pk

shohin[@]suehiloya[.]jp

Asuntos

Reunión de emergencia

Solicitud de reunión de profesionales de empleo exprés

Información de la reunión

Todos deben venir a la reunión mañana.

reunión regular el viernes

Url's:

http[:]//42.115.22[.]145/UvYUhxYJEhYFjZ

http[:]//42.115.22i[.]145/QsfegKf

http[:]//42.115.22i[.]145/NCKAmkp04xSDd

http[:]//42.115.22i[.]145/ivhJT2mo

http[:]//aws.firstdistribution[.]com/engl/mlfiRzCJT/

http[:]//helpvan[.]su/

http[:]//reklamlar.mamadunyasi[.]com/wp-admin/beFSJnQ/

http[:]//bolehprediksi[.]com/wp-includes/ifrEFSqSw/

http[:]//45.55.179[.]121[:]8080/otq0FCjgM

Archivos adjuntos.

Archivo : Misión Cena de liderazgo comunitario Invitación a reunión.doc

SHA256 : 22915d9af211cb95d30455f9603e9f0055d4c5465aaf44820faac4633494bd90

Archivo : 733.exe

SHA256 : 55b579f47776c2d8efb32e4ced2c92f636f20e7db3d83426fa9a7d2a35f6e063

Archivo : nuestra reuniÃ³n del miÃ©rcoles 28 de feb.doc

SHA256 : 22915d9af211cb95d30455f9603e9f0055d4c5465aaf44820faac4633494bd90

Archivo : ReuniÃ³n de emergencia.doc

SHA256 : e00a192806f2d37cce984841748debb6a213bfdffc0dd9449b9457d4413945fd

Archivo : 733.exe

SHA256 : b7d35747e45128fb3f7a7bfda7b51eea6d70a92c2116bfd5d96a133f57feabae

Archivo : 733.exe

SHA256 : 73333c7796f0f96abb3ab3ca6edbb98bdb6eba44f29f6c3ca5dbb8c6b79bc893

Archivo : ReuniÃ³n no programada.doc

SHA256 : 746bec4e33cdc9c52cc294d75ca562b2bc98aa18124bcd3ac2394259138d3176

Archivo : 633.exe

SHA256 : 088a3e955b69829ad58591e96e40aea7819c417b1eb9a5e0b766de1ede804f94

Archivo : Siguiente junta.doc

SHA256 : 95985e4ccc56a2c70d17d69bc35db107d767c4ac49e512f65909f987322cd73b

Archivo : 733.exe

SHA256 : 088a3e955b69829ad58591e96e40aea7819c417b1eb9a5e0b766de1ede804f94

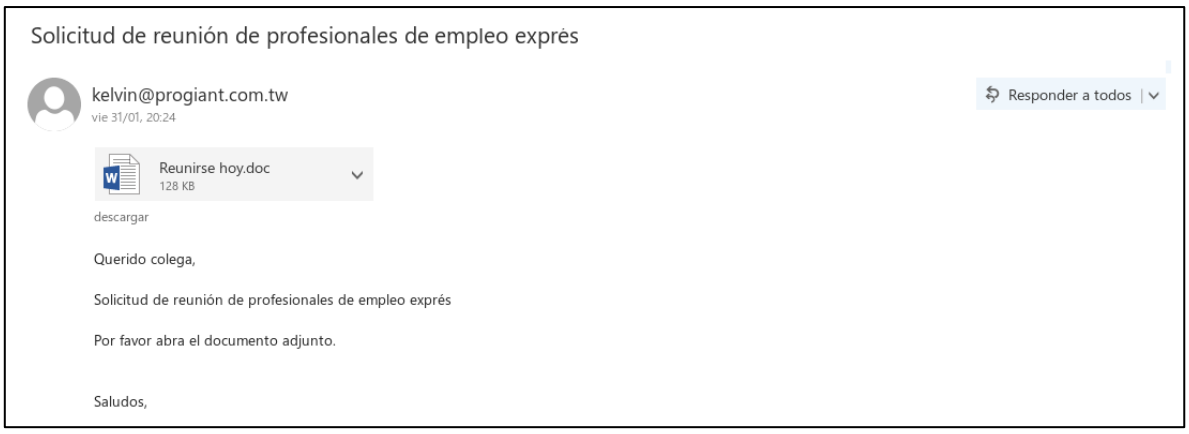
Archivo : Encuentro extraordinario.doc

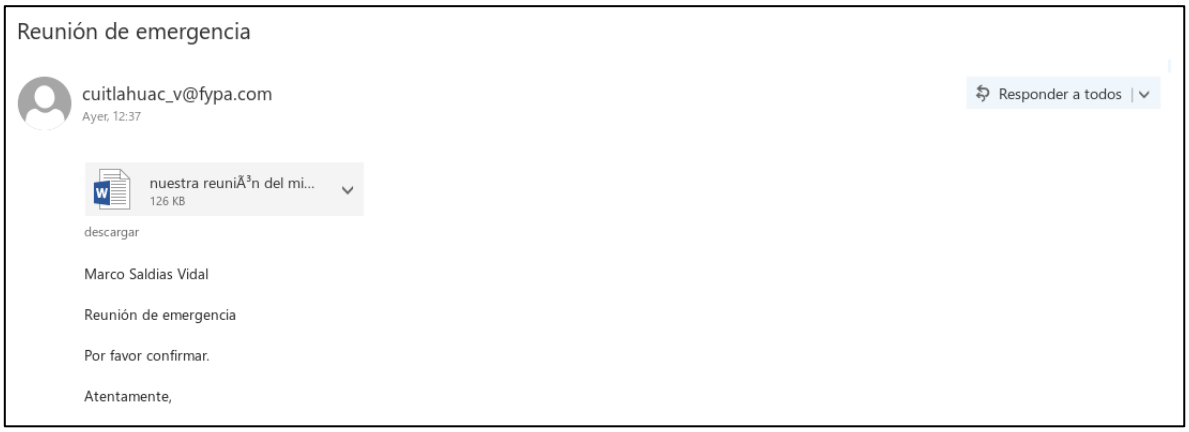
SHA256 : 8cd81b098c348286a711147f3e79bae46855aacc94d53dc9e650db227d61533a

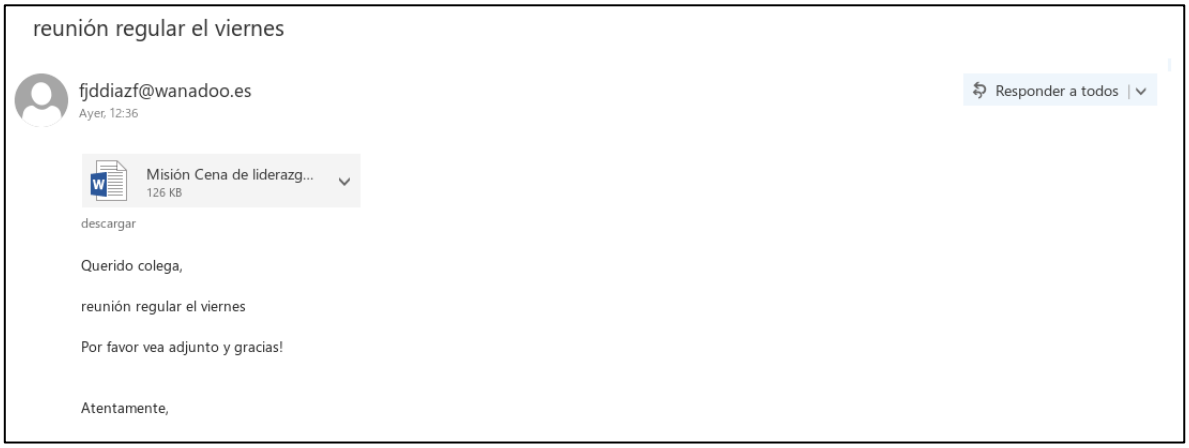
Archivo : 209.exe

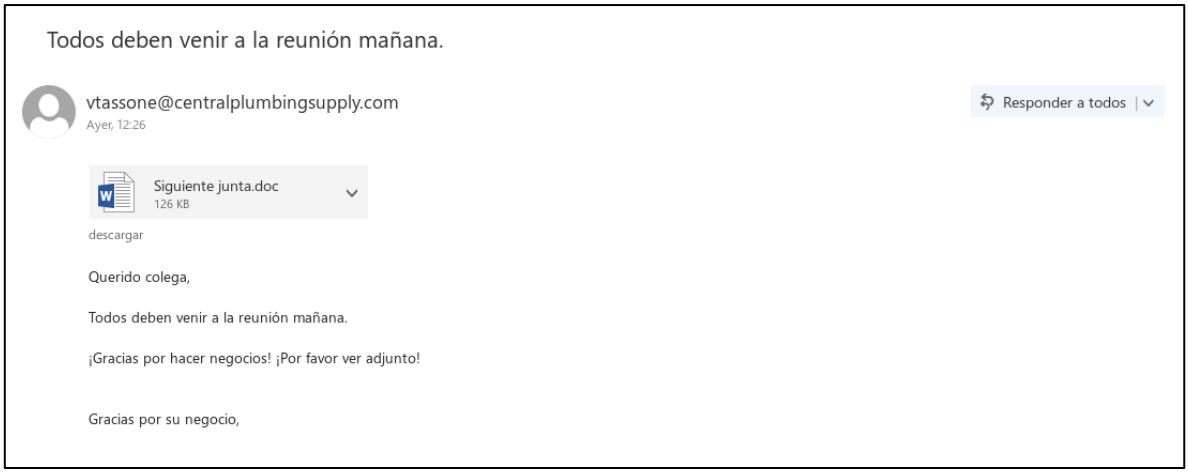
SHA256 : 0ddde52ca3e01fdf8dbaff394135e34de7f446d8d47942329f9b9832b3b2246

Imagen Mensaje


Solicitud de reunión de profesionales de empleo exprés
kelvin@progiant.com.tw
vie 31/01, 20:24
Responder a todos
Reunirse hoy.doc
128 KB
descargar
Querido colega,
Solicitud de reunión de profesionales de empleo exprés
Por favor abra el documento adjunto.
Saludos,

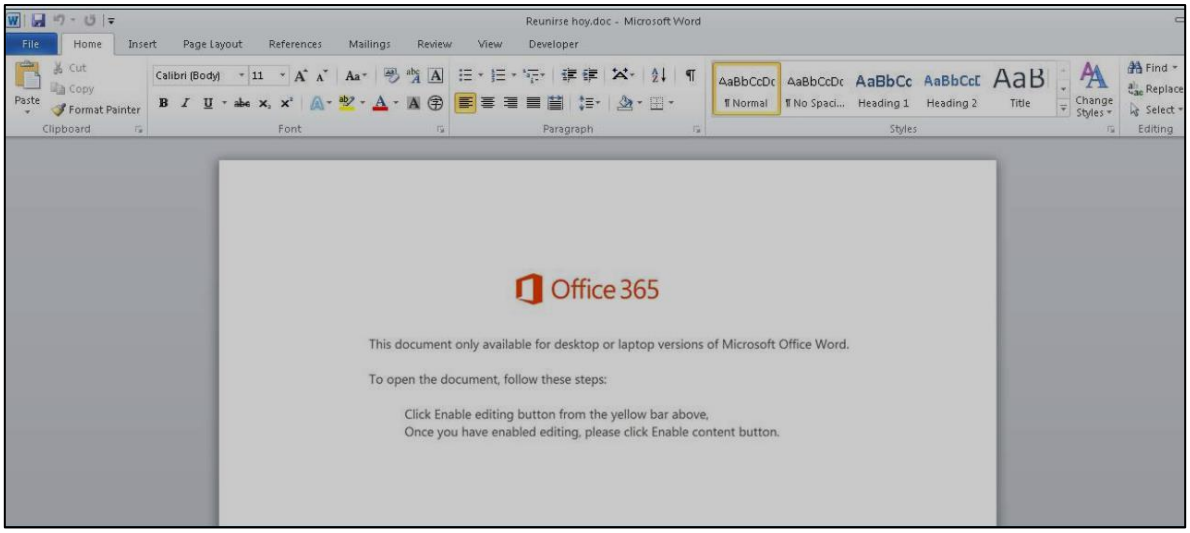

Reunión de emergencia
cuitlahuac_v@fypa.com
Ayer, 12:37
Responder a todos
nuestra reuniÃ³n del mi...
126 KB
descargar
Marco Saldias Vidal
Reunión de emergencia
Por favor confirmar.
Atentamente,


reunión regular el viernes
fjddiazf@wanadoo.es
Ayer, 12:36
Responder a todos
Misión Cena de liderazg...
126 KB
descargar
Querido colega,
reunión regular el viernes
Por favor vea adjunto y gracias!
Atentamente,


Todos deben venir a la reunión mañana.
vtassone@centralplumbingsupply.com
Ayer, 12:26
Responder a todos
Siguiente junta.doc
126 KB
descargar
Querido colega,
Todos deben venir a la reunión mañana.
¡Gracias por hacer negocios! ¡Por favor ver adjunto!
Gracias por su negocio,


Información de la reunión
sabuj@aji-group.com
Ayer, 12:21
Responder a todos
ReuniÃ³n de emergencia...
126 KB
descargar
Querido colega,
Información de la reunión
Por favor abra el documento adjunto.
Atentamente,

Documento con malware



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.04 12:59:23 -03'00'