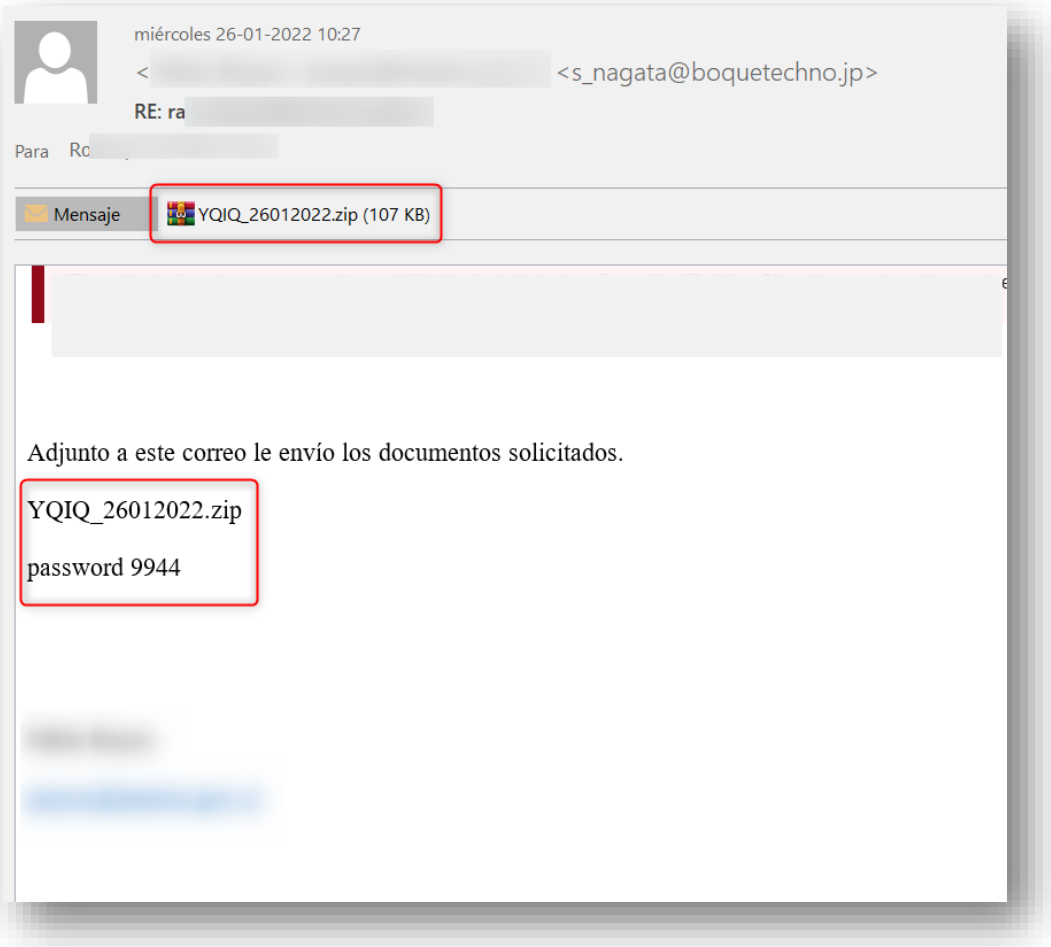
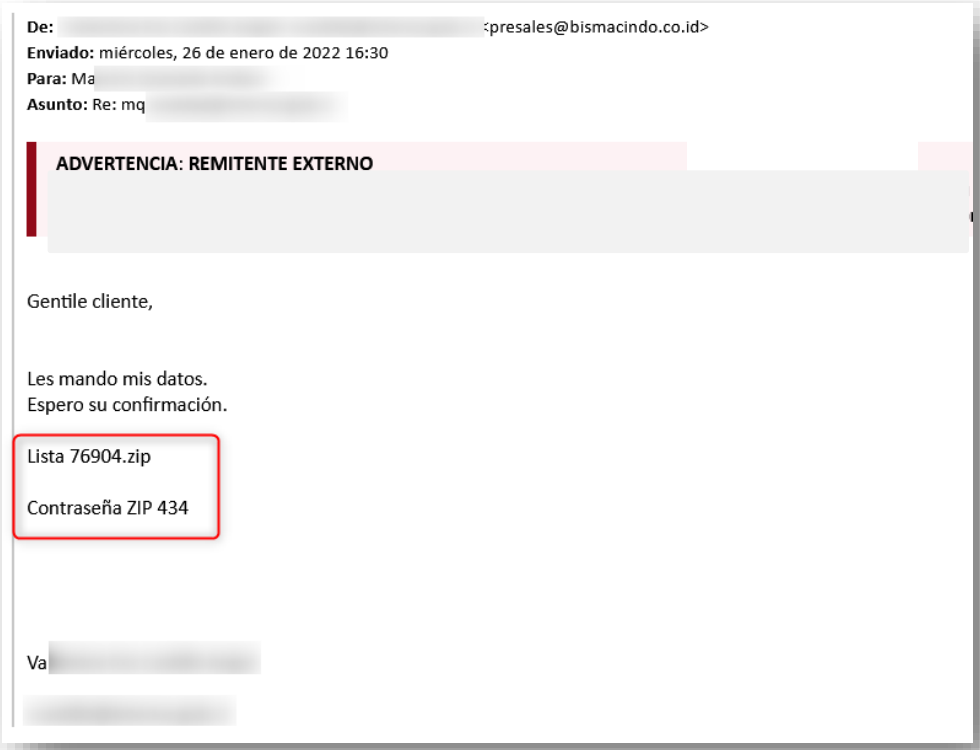
ALERTA DE SEGURIDAD CIBERNÉTICA

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, **advierte que continúan las campañas** de correo electrónico que buscan propagar en las organizaciones que conforman la administración del Estado el **malware Emotet.**

Durante las últimas horas, algunas instituciones recibieron diversos correos que contenían este programa malicioso y que adjuntaban un **archivo adjunto con extensión .zip junto a una contraseña para descomprimirlo.**

Cabe destacar que los atacantes están suplantando la identidad de personas que trabajan en las organizaciones afectadas, al igual que sus direcciones de correo electrónico institucional. Adjuntamos algunos ejemplos de correos:





De: [redacted] <presales@bismacindo.co.id>
Enviado: miércoles, 26 de enero de 2022 16:30
Para: Ma[redacted]
Asunto: Re: mq[redacted]

ADVERTENCIA: REMITENTE EXTERNO

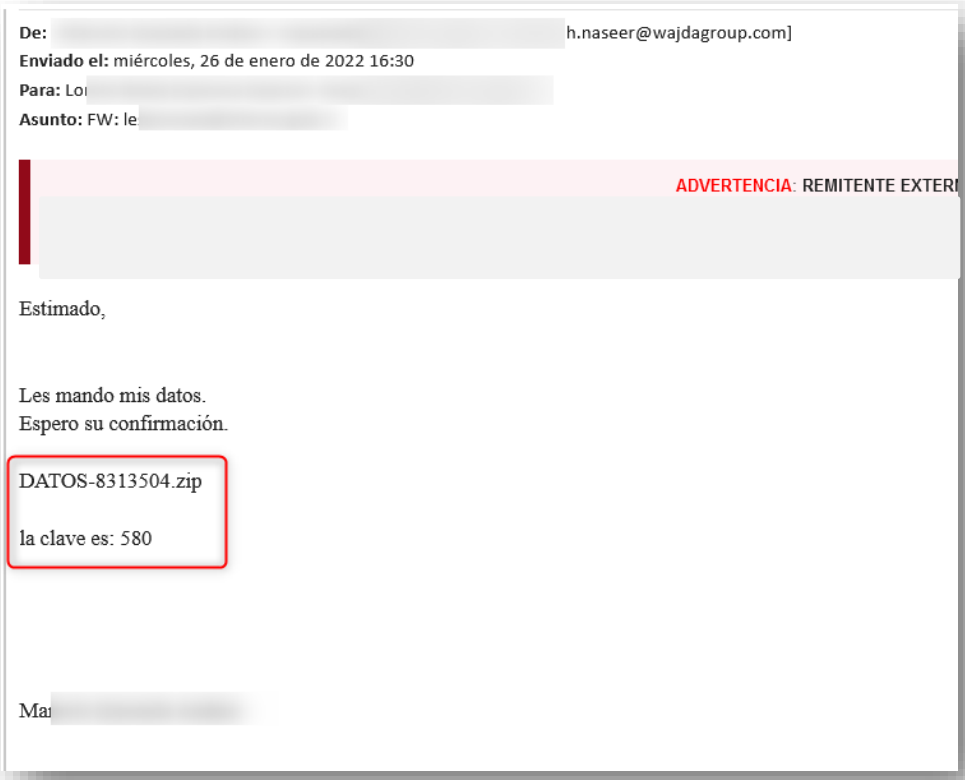
Gentile cliente,

Les mando mis datos.
Espero su confirmación.

Lista 76904.zip

Contraseña ZIP 434

Va[redacted]



De: [redacted] h.naseer@wajdagroup.com]
Enviado el: miércoles, 26 de enero de 2022 16:30
Para: Lo[redacted]
Asunto: FW: le[redacted]

ADVERTENCIA: REMITENTE EXTERI

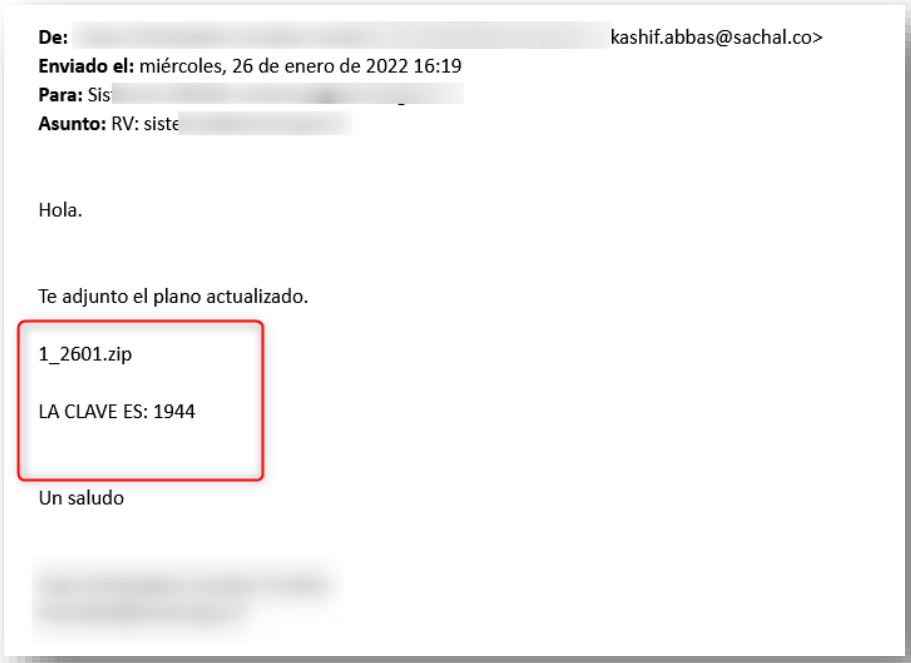
Estimado,

Les mando mis datos.
Espero su confirmación.

DATOS-8313504.zip

la clave es: 580

Ma[redacted]



De: [redacted] kashif.abbas@sachal.co>
Enviado el: miércoles, 26 de enero de 2022 16:19
Para: Sis[redacted]
Asunto: RV: siste[redacted]

Hola.

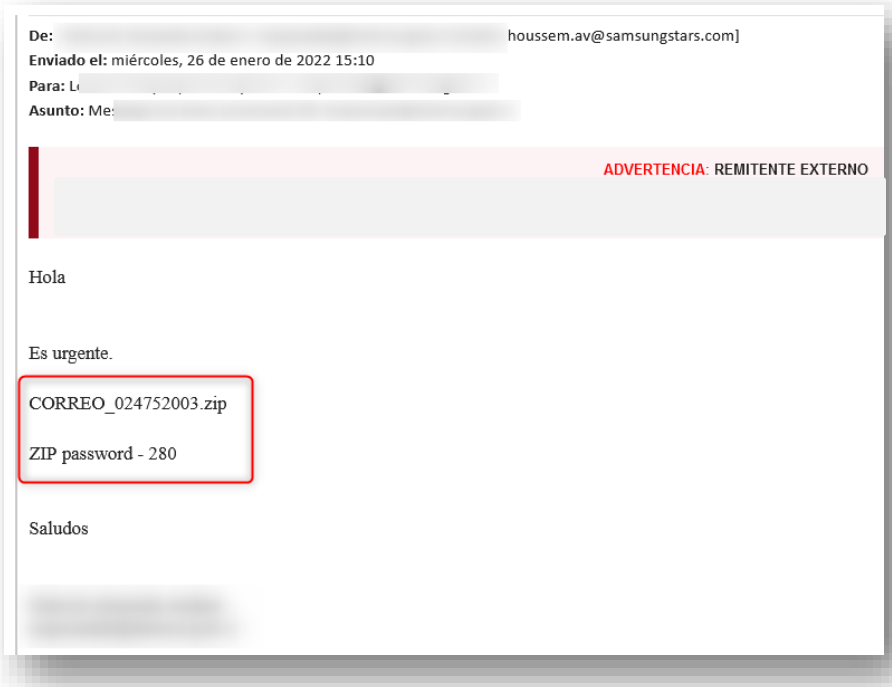
Te adjunto el plano actualizado.

1_2601.zip

LA CLAVE ES: 1944

Un saludo

[redacted]



De: [redacted] houssem.av@samsungstars.com]
Enviado el: miércoles, 26 de enero de 2022 15:10
Para: L[redacted]
Asunto: Me[redacted]

ADVERTENCIA: REMITENTE EXTERNO

Hola

Es urgente.

CORREO_024752003.zip

ZIP password - 280

Saludos

[redacted]

El CSIRT de Gobierno solicita a los encargados de ciberseguridad informar oportunamente a todos los usuarios que utilizan correo electrónico sobre esta amenaza, para evitar que una institución se vea afectada. Junto con esto, recomendamos:

- Mantener actualizados los sistemas operativos, navegadores y complementos.
- Mantener antivirus e instalar sus actualizaciones periódicas.
- Aumentar las medidas de seguridad de los programas antispam o poner en cuarentena los archivos .zip que incluyan una contraseña, con tal de realizar una revisión preventiva.
- Solicitar a los funcionarios que informen y estén alerta ante correos electrónicos con las siguientes características:
    - Remitente desconocido o que provenga de un funcionario de la institución, pero que esté acompañado de otra dirección de correo desconocida.
    - Contenga un mensaje breve con archivos .zip, .doc, .xls o .PDF
    - El mensaje incluye una contraseña para abrir el documento, generalmente, de cuatro números.
    - Firma con el nombre y correo del supuesto funcionario sin logo o imagen institucional.

De igual manera, solicitamos informar al CSIRT de Gobierno si detectan este tipo de correos electrónicos o si sufren una afectación de los sistemas para apoyar cualquier incidente.

Indicadores de compromiso

El CSIRT de Gobierno pone a disposición algunos Indicadores de Compromiso analizados por el equipo, además de otros IoC proporcionados por otras instituciones del Estado.

IoC URLS

hxxp://91.240.118.168/qw/as/se.html

hxxp://unifiedpharma.com/wp-content/5arxM/

IP

[91.240.118.168]

[3.133.153.111]

IoC archivos DLL

Nombre: ssd.dll

SHA256: 3f7be42ab1f47d8ab6ad4403af234abeba288ce7ed859bf91ca18d95fca3c3d8

IoC archivos adjuntos

Archivo: YQIQ_26012022.zip

SHA256: 5fbef501e52081fdbe5425b94948cd18c0dea6ec2cbd25090456b8455c5bbf7f

Archivo: YQIQ_26012022.xls

SHA256: c1c31b94de7d8fdb409fb59724dc9143ab00ff2870e10a82e3ef3987401fb8d8

Archivo: DATOS-8313504.zipx

SHA256: 2b1b009db37779a03c652827698cf19d6b392b8ea5917b6b814b2801684f812c

Archivo: DATOS-8313504.xls

SHA256: 90bc550e8d3e6ea7b0785998cacdd1a7bb464bcdd1d7ef8b55b1c727770fe355

Archivo: Lista 76904.zip

SHA256: 60ca395e02b351b6e6eb0ef8a54cb728c372f81dcbb3ff9a49e1774ead8c08ce

Archivo: Lista 76904.xls

SHA256: 14d448a7a70c7a5a004d6568a752d70372f46ffc7b749996cb2e2956cde56965

Otros IoC relacionados

IoC Archivos:

Archivo: 26012022.xls

SHA256: 01b78b11993b456bd267dfc90432404bfdf7ad76dc8c67d27b9e4d40b0e42143

Archivo: hH_2601.xls

SHA256: 0345c5e3b981a865dfbe868995d17b03c3b11f3f27814429de05f308025818ad

Archivo: doc_2601.xls

SHA256: 072e43caecdb7f5562f007f43d386fa9b475848d805b0afeef91619eb72a9cf6

Archivo: 8205_5440.xls

SHA256: 0852a71bdaffc71d8e68687c247ad72e22ee37994055f74ddf53b767ff7fb595

Archivo: carga útil_1.bin

SHA256: 085a8a0329cb558dfc1694cc175d260ac90cf0bd2f1dd30bab7eda06b182d8d1

Archivo: Correo_116400366.xls

SHA256: 0a6d0aaf398176b36623035d2a8567ef280a2d7ad42f34a428092ae0ec823be7

Archivo: _26012022.xls

SHA256: 0e5974428401fa42f1245323d16cefc734e2a450f48057c761c3e318553cb0ae

Archivo: Correo_82587.xls

SHA256: 1478b1b53ff7b1941488489a5a5c07f51e3389119dc6635a0199efd7f337c123

Archivo: Lista 76904.xls

SHA256: 14d448a7a70c7a5a004d6568a752d70372f46ffc7b749996cb2e2956cde56965

Archivo: DOCUMENTO_2601.xls

SHA256: 16d825b2304bdc5ab408e5440703caa0d3a1172406d7d1b40e3db13202b34bb5

Archivo: comentarios-844735.zls

SHA256: 17e10455cfccf042305c2eacca48516ab35134ab0b1140bb761e7d8813427c56

Archivo: itur_597.xls

SHA256: 18b650117d03c5e75c0f2b53a9a0c057d5c417acf12d3ec622ec97565a681a6f

Archivo: Grupo Editorial Opast.xls

SHA256: 19ef9646a32b6fd446bb79b5b8901b39367cc2e73dfe0071ab1f537b4ce45dd3

Archivo: n-90727172.xls

SHA256: 19fbf474eed7540f1a79c2efc0b3e21c48abdb7e6ea7892e755d72cd5aef925f

Archivo: iframemsg?id=download-3927260452

SHA256: 1b792eac386e26dcdfd800f9a5941fe04a5a86917bf6f1085f53be5b0deff161

Archivo: mensaje-2601.xls

SHA256: 1b846e1ffb7b04dd60200cc3741fa3a341f9a8cf982a974b596eab20804917a5

Archivo: carga útil_1.bin

SHA256: 1fbc034b30e25ab7747780e6df958cd8bbd6ffbae6e78170f52a981d5da40c29

Archivo: Doc_2601.xls

SHA256: 21ff6d208b8707a2e84236e0388570226f22250d30cd1a4689817c56432649fd

Archivo: carga útil_1.bin

SHA256: 2267ef163777caa897d03592c1f48930ad4e38b8b3f4368d2b6a42bb2c8002d3

Archivo: ybq-85.xls

SHA256: 27b4999d426087dec496d2a41b4e8721e91f4ad1eebe5837da0da5b178e8664b

Archivo: r_2601.xls

SHA256: 27bad3c2810baf3799764e193fc5a81bea0c3c527d6e2678883fa8f74607d89c

Archivo: Lista_2601.xls

SHA256: 27e400ec75a6391da1a8e47de2c24530a6d303361f3cbf525a106c35a9a58ea5

Archivo: carga útil_1.bin

SHA256: 291e5b7c5f38b1ea5064b126ce5bb85d696f267efe1281feb65691384763bae9

IoC IP

185.244.166.137

185.168.130.138

IoC Correos

planningdept5@gactme.com

store16@gactme.com

miyake@kinkigas.co.jp

IoC Dominios

unifiedpharma.com

hotelamerpalace.com

connecticutsfinestmovers.com

icfacn.com

krezol-group.com

ledcaopingdeng.com

autodiscover.karlamejia.com

crmweb.info

accessunited-bank.com

pigij.com

artanddesign.one

strawberry.kids-singer.net

eleccom.shop

izocab.com

IoC SHA256

fe5f2fe9d91c5552c56aae19f9b2c0dd86b40d5cfaf7038c1cee0bcea1722b01

1f68b3cc988aa115495dd93324bbc8fc4c1dac99134cc484cb851c3f64994f2a

a5214f9d7fa067492d19fa7654222fdaad16d4855f0676e5e99c682e4dd62a47

3f0ddcee07d774b9ff05f013a2f74003406d17ba62f7209e37a8be50089b946c

9a4ff335758aa5ea1dc44c57fa5d66c6f5ee2c19c6a8b7d60227fc449a377b2a

5bd4987db7e6946bf2ca3f73e17d6f75e2d8217df63b2f7763ea9a6ebcaf9fed