Alerta de seguridad informática	2CMV22-00269-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2022
Última revisión	26 de enero de 2022

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 de Gobierno) ha identificado una nueva campaña de malware Emotet, a través de la cual un atacante busca persuadir a las personas de descargar un archivo adjunto y ejecutarlo, para infectar el equipo.

Para convencer a la víctima, el mensaje del correo indica que se adjuntan los documentos solicitados, los cuales vienen en un archivo .zip e incluye una contraseña para abrirlo

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
alshamil.net.ae [217.165.163.221]

IoC IP

IP : [91.240.118.168]
IP : [3.133.153.111]

IoC URL

URL : hXXp://91.240.118.168/qw/as/se.html
URL : hXXp://unifiedpharma[.]com/wp-content/5arxM/

IoC Archivo DLL

Nombre : ssd.dll
SHA256 : 3f7be42ab1f47d8ab6ad4403af234abeba288ce7ed859bf91ca18d95fca3c3d8

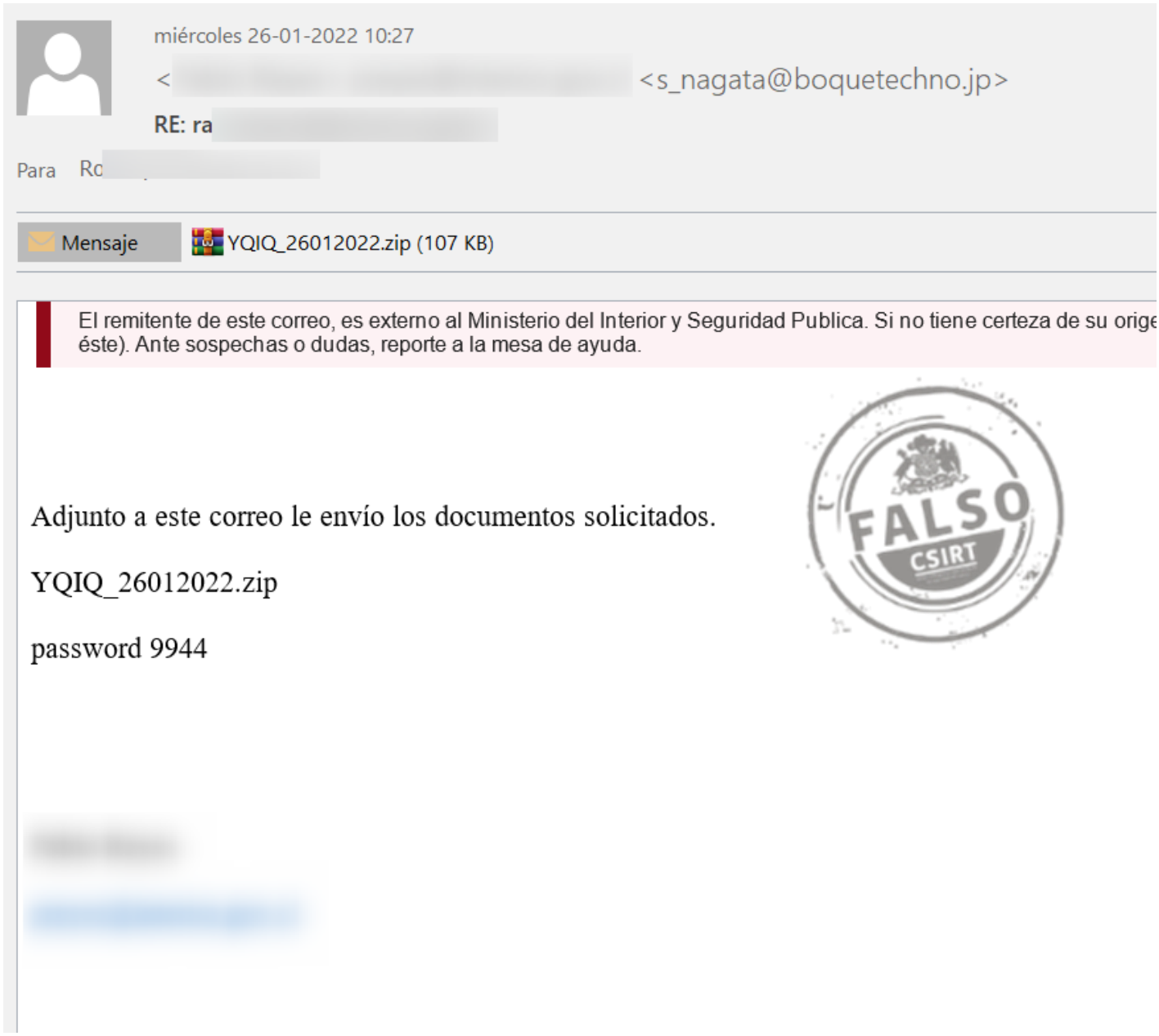
IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : YQIQ_26012022.zip
SHA256 : 5fbef501e52081fdbe5425b94948cd18c0dea6ec2cbd25090456b8455c5bbf7f

Nombre : YQIQ_26012022.xls
SHA256 : c1c31b94de7d8fdb409fb59724dc9143ab00ff2870e10a82e3ef3987401fb8d8

IMAGEN DEL MENSAJE



RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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.
- Visualizar los sitios web que se ingresen sean los oficiales.