GRUPO PARLAMENTARIO

PREGUNTA CON RESPUESTA POR ESCRITO

A LA MESA DEL CONGRESO DE LOS DIPUTADOS

D. RODRIGO JIMÉNEZ REVUELTA, y D. PABLO SÁEZ ALONSO MUÑUMER, en su condición de Diputados del **Grupo Parlamentario VOX (GPVOX)**, al amparo de lo establecido en los artículos 185 y siguientes del vigente Reglamento del Congreso de los Diputados, presentan las siguientes **preguntas para las que solicitan respuesta por escrito.**

EXPOSICIÓN DE MOTIVOS

El día 23 de marzo la Policía Nacional ha detectado un nuevo virus, y nada tiene que ver con el Covid-19, este es informático, y ha irrumpido en escena tratando de colarse como información adjunta en correos electrónicos de sanitarios. Disfrazado de "información sobre la Covid-19", pretendía "romper" el sistema informático de los centros médicos en plena crisis sanitaria. Se llama Netwalker y es un ransomware [secuestrador de datos]. Los expertos recomiendan al personal médico no abrir ningún correo sospechoso.

El mecanismo de este tipo de virus "que suelen provenir en un 99% de países del Este de Europa", según explican investigadores especializados en delitos telemáticos, consiste en "corromper" la información –"en este caso la de los

Grupo Parlamentario VOX, Carrera de San Jerónimo s/n 28071 Madrid
Telf. 91 390 57 63 /91 390 76 42
gpvox@congreso.es

hospitales en lugar de empresas o bancos"-, y solicitar un rescate para recuperarla. "Si no pagan, no la devuelven", aseguran.

La Policía Nacional detectó este domingo un intento de bloquear los ordenadores de los hospitales españoles mediante el envío al personal sanitario de correos electrónicos con un virus "muy peligroso" con el señuelo de contener información sobre la Covid-19, según informó este lunes el director adjunto operativo del cuerpo, el comisario principal José Ángel González. Por eso instó a los trabajadores de la sanidad a no abrir los correos electrónicos sospechosos para evitar posibles daños. "La mejor protección es la prevención", dijo.

La principal característica de Netwalker, detallan fuentes policiales, es que introduce un código malicioso en el explorador del sistema informático para que los antivirus sean incapaces de detectarlo y eliminarlo. Y "aunque en España aún no se ha producido una distribución masiva, las consecuencias de un ataque exitoso con ransomware, que inutilizara los sistemas informáticos de un centro hospitalario, tendría consecuencias devastadoras", señalan fuentes policiales.

El nombre del documento adjunto en los correos que esconden el malware [programa maligno] es CORONAVIRUS_COVID-19.vbs. Cuando algún receptor clica en el documento se ejecuta y el malware encripta los archivos: "Hey! Tus documentos han sido encriptados por Netwalker", se anuncia. Y prosigue con las instrucciones para realizar el pago en la dark web, o la Internet profunda y desregulada.

Además de ser tremendamente desafortunado por la situación crítica mundial, el ciberataque es inesperado. Algunas bandas criminales dedicadas al secuestro de datos anunciaron hace días que iban a dejar a los centros sanitarios fuera de sus objetivos. El grupo Netwalker no es uno de ellos. La atención a otros problemas hace que sea un buen momento para atacar para estos grupos.

El 12 de marzo hubo un ataque contra una organización sanitaria en Illinois (Estados Unidos), Champaign Urbana Public Health District, que les bloqueó la página web y debieron crear una alternativa. Este ransomware fue encontrado también en febrero en un ciberataque contra Toll Group, una empresa australiana de logística.

Los sanitarios no son las únicas víctimas de la actuación de los ciberdelincuentes que se están aprovechando de la situación creada por la pandemia de la Covid-19. Se han advertido correos enviados a la población que tienen como finalidad "infectar nuestro ordenador y tener acceso a todas nuestras claves e información personal". De hecho, los últimos informes del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC, dependiente del Ministro del Interior) alertan sobre una quincena de ciberestafas perpetradas con el señuelo del coronavirus. En ellas se ha utilizado software malicioso difundido a través de aplicaciones y web que atraen a las víctimas con información para identificar síntomas o mapas de la pandemia. Su objetivo es robar, pero algunos añaden la peligrosidad de ofrecer falsos diagnósticos de la enfermedad.

Este lunes, la Policía también ha pedido a la ciudadanía que tenga cuidado con los más de 200 bulos y falsas noticias detectados con la única intención de

provocar miedo y pánico. Entre ellos, ha destacado dos: un audio que alertaba de una inminente declaración del estado de sitio y aconsejaba a hacer compras masivas en supermercados, y otro de un motín en una cárcel española con un vídeo de una prisión italiana de la semana pasada. "La gente ahora tiene mucho tiempo. Hay gente que se dedica a distraerse, pero hay mucha gente que se dedica a crear estos bulos", ha manifestado la Policía.

Además de la Policía, la Guardia Civil también está sumando esfuerzos para garantizar la ciberseguridad durante la crisis. El director adjunto operativo del cuerpo ha recordado en la misma rueda de prensa que el instituto armado hace seguimiento de las redes sociales para velar por su "seguridad" y ha destacado que es "muy importante" que cualquier institución que crea estar sufriendo un ataque informático lo comunique "lo antes posible" para tomar medidas.

PREGUNTAS

1. ¿Qué otras medidas se están tomando por parte del Gobierno para informar a la población de este tipo de ciberataques?

2. ¿Qué capacidad de respuesta tiene el Ministerio del Interior para la detección de este tipo de ataques?

3. ¿Qué medidas preventivas se están tomando al respecto para detectar con antelación este tipo de ataques?

Palacio del Congreso de los Diputados, a 24 de marzo de 2020.

D. Rodrigo Jiménez Revuelta
Diputado GPVOX

Dña. Macarena Olona Choclán.
Portavoz Adjunta GPVOX.

D. Pablo Sáez Alonso Muñumer
Diputado GPVOX