COMUNICADO SOBRE MALWARE WANNACRY/WANNACRYPT

Desde el pasado viernes 12 de mayo, han aparecido en los medios noticias sobre un ciberataque a numerosas instituciones y empresas, tanto españolas como extranjeras.

Este texto explica de forma sencilla todo lo necesario que cualquier ciudadano necesita saber al respecto.

¿Qué ha sucedido? ¿Por qué tanto revuelo?

Durante la mañana del viernes empezaron a circular noticias sobre que algunas grandes empresas españolas estaban sufriendo un ataque informático, que se estaban infectando sus equipos y que estaban enviando a sus empleados a casa.

La noticia resultó ser cierta y generó una importante alarma tanto en Internet como en periódicos y televisión, haciendo que muchas otras organizaciones, de forma preventiva, cortasen sus conexiones a Internet, o incluso enviasen a sus empleados a casa.

El causante era un virus informático que una vez dentro del ordenador cifra (o bloquea) toda la información que este contiene, mostrando un mensaje en el cual se pedía un rescate de 300€ para desbloquear la información. Este tipo de virus es conocido como *ransomware* (del inglés, ransom quiere decir 'rescate').

¿Cómo se infectan los ordenadores?

Aunque en un primer momento se creía que el virus llegaba como un enlace en un correo falso, parece ser que **existen múltiples formas de infección**. Una vez descargado aprovechaba un fallo de seguridad para atacar al sistema y secuestrar toda la información. Además, el ordenador infectado atacaba al resto de ordenadores de la misma red, llegando a cifrar la información de los discos USB que tuviera el equipo o las carpetas compartidas en red (algo muy utilizado en empresas y oficinas).

Así pues, con que una sola persona de la red se infectase, **toda la red podía verse secuestrada** de forma automática en pocos minutos, independientemente de que el resto hubiera sido infectado o no.

Conviene no centrarse únicamente en el correo electrónico, ya que podrían existir múltiples formas de infección, como ficheros en Dropbox o similares, en aplicaciones de descarga P2P, o incluso simplemente por navegar por sitios web de mala reputación.

¿Afectaba a todos los ordenadores? ¿Y tablets o móviles?

El virus **afecta a prácticamente todas las versiones de Microsoft Windows**, incluidas las que utilizan muchos tablets o pequeños portátiles.

Sin embargo, **NO afecta a dispositivos móviles con Android o iOS** (iPhone ni iPad), ni a ordenadores Mac (Apple) o Linux.

Tengo antivirus, ¿estoy a salvo?

Los antivirus funcionan como una vacuna contra "*enfermedades*" conocidas, pero este virus era completamente nuevo por lo que los antivirus aun no estaban preparados.

Ahora mismo es probable que la mayoría de antivirus ya conozcan este virus, pero si surgiese algún nuevo virus que se aprovechara del mismo fallo de seguridad, no se estaría protegido desde el primer momento.

¿Qué puedo hacer para protegerme?

Lo principal es corregir el agujero de seguridad que utiliza el virus. Para ello basta con instalar las actualizaciones de seguridad que Microsoft ha preparado:

- **En equipos con Windows 7 o posterior**, basta con instalar las actualizaciones automáticas y reiniciar. También es posible descargarlas manualmente desde este enlace: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- **En equipos con versiones anteriores**, como Windows XP, se deberá descargar la actualización manualmente desde el siguiente enlace:

  http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

Además, recordamos las principales buenas prácticas que nos protegerán de este y muchos otros virus informáticos:

- **Hacer frecuentemente copias de seguridad** en un disco USB externo o similar. Nunca en el mismo equipo.
- **Ser muy cautos a la hora de abrir ficheros adjuntos o hacer clic en enlaces de correos** sospechosos. Ante la duda, desconfiad y remitírnoslo a csirtcv@gva.es
- Tener el **equipo actualizado y utilizar antivirus**.

Ya me he infectado, ¿qué hago?

Si es posible, lo más eficaz es formatear el equipo, instalarlo de nuevo y recuperar la última copia de seguridad, comprobando previamente que no esté infectada.

Puede parecer una medida drástica, pero una vez un ordenador se infecta, es la única de garantizar su limpieza al 100%.

De no ser posible formatear, recomendamos apagar el equipo, desconectarlo de la red, y esperar a la información que publicaremos en los próximos días al respecto. Cabe destacar que **recomendamos encarecidamente NO pagar el rescate**, ya que no tenemos ninguna garantía de que vayamos a recuperar nuestros datos.

Más información

Si se desea completar esta información con **más datos técnicos** puede descargarse el siguiente informe de CCN-CERT.