12/5/2017

El “Centro Criptológico Nacional” confirma un ciberataque masivo de Ransomware a multitud de empresas

- El CCN-CERT ha calificado el nivel de alerta como "muy alto"
- Telefónica ha sido una de las compañías afectadas por el ataque

El centro criptológico nacional (CCN-CERT) ha confirmado un "ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas" cuyo nivel de alerta está catalogado como "muy alto". Este ataque ha afectado especialmente a Telefónica, así como se han tomado una serie de medidas de protección en otras compañías como Iberdrola, Gas Natural o BBVA.

El CCN-CERT apunta que "el ataque masivo de Ransomware a varias organizaciones afecta a sistemas Windows cifrando todos sus archivos y los de las unidades de red a las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red".

La vulnerabilidad parece estar originada en un agujero del sistema operativo de Microsft, ya que la compañía publicó la vulnerabilidad el día 14 de marzo en su boletín y hace unos días se hizo pública una prueba de concepto que parece que ha sido el desencadenante de la campaña.

El tipo de ransomware es una versión de WannaCry que "infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red".

Los sistemas afectados son: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2012 and R2, Windows 10 y Windows Server 2016. Para estar seguro, se recomienda actualizar los sistemas a su última versión o parchear según informa el fabricante en su web. Para los sistemas sin soporte o parche, como Windows 7, se recomienda aislar de la red o apagar según sea el caso.

¿Qué significa "Muy alto"?

El CCN-CERT ha catalogado el nivel de alerta por esta ciberamenaza como "muy alto" pero, ¿qué significa esta calificación?

El nivel "Muy alto" es el penúltimo nivel en cuanto alerta de riesgo, y significa que se trata de "una amenaza importante afecta a las instituciones por lo que se requiere una acción inmediata. La probabilidad de afectar y dañar a los sistemas de información es alta. Además de todas las medidas señaladas en los niveles anteriores, los responsables de seguridad deberán coordinar los esfuerzos necesarios con los Equipos de Respuesta, tomar precauciones adicionales en sus políticas de seguridad y prepararse para ejecutar planes de contingencia".

https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html