Masterhacks – Algunos ataques informáticos que se han registrado últimamente, incluidos WannaCry en mayo y NotPetya ayer, funcionaron con vulnerabilidades que ya eran conocidas por la NSA desde hace cinco años.

La vulnerabilidad explotada por el ransomware NotPetya ya era vieja en la Agencia Nacional de Seguridad de Estados Unidos, y que además comenzó a utilizar una herramienta llamada EternalBlue, algo que maximizó su capacidad de vulnerar redes y explotar vulnerabilidades serias de sistemas operativos como Windows.

Sin embargo, la NSA no informó a Microsoft sobre dicha vulnerabilidad hasta principios de este año, por lo que la compañía lanzó un parche, pero algunos equipos antiguos se quedaron con el problema.

En marzo, Microsoft publicó el parche para corregir el problema, pero equipos que utilizan Windows 7 SP1 o XP y no actualizaron sus sistemas tuvieron problemas.

NotPetya, similar a Petya, utiliza EternalBlue, al igual que Petya, pero este de una forma más sofisticada y peligrosa. Esto ya que en lugar de cifrar uno por uno los archivos, encripta toda la tabla maestra de Windows, lo que imposibilita el arranque y hace que los usuarios paguen en Bitcoin.

Aún sabiendo todo esto, se espera que en los siguientes días sigan habiendo equipos infectados por la vulnerabilidad EternalBlue.