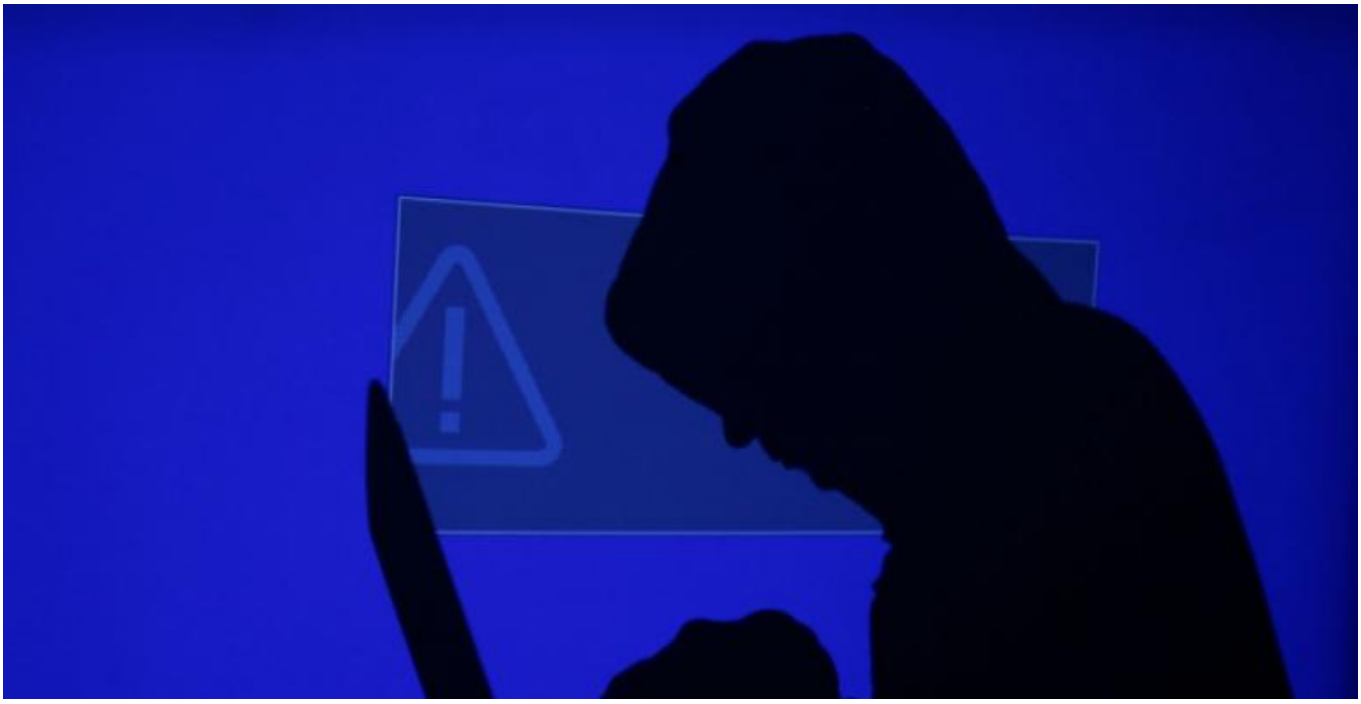
Snowden: El ataque con el virus extorsionador Petya se realizó utilizando un 'exploit' de la NSA

28/06/2017



Este martes, varios países de la Unión Europea —entre ellos, España—, además de EE.UU., Ucrania y Rusia, se convirtieron en blancos de un ataque cibernético con un potente 'ransomware' llamado Petya. Al analizar lo sucedido, varios expertos en seguridad informática afirman ahora que este virus utilizó una herramienta de la Agencia de Seguridad Nacional de EE.UU. (NSA, por sus siglas en inglés).

Se trata concretamente de EternalBlue, una herramienta para 'hackeos' usada por la agencia estadounidense. Este programa aprovecha una vulnerabilidad del protocolo Server Message Block de Windows para lograr acceder al sistema. El vínculo entre la herramienta y el nuevo 'ransomware' fue confirmado por el exempleado de la CIA y de la NSA Edward Snowden y por las empresas Kaspersky Lab y Symantec, proveedoras de servicios de seguridad informática.

El periódico 'The Washington Post' recoge las declaraciones de varios miembros de la NSA que defienden el uso del EternalBlue para obtener datos de Inteligencia. Un exempleado asegura que el volumen de información recibida a través de esta herramienta recuerda a una "pesca con dinamita".

Después de que la NSA aprovechara esa vulnerabilidad de Windows sin informar de ella a Microsoft, el ataque con Petya ha impedido el funcionamiento correcto de lugares como bancos, aeropuertos o centros médicos.

"¿Cuántas veces más tiene que causar daños a las infraestructuras civiles el desarrollo de armas digitales de la NSA antes de que se asuma alguna responsabilidad?", se preguntaba este martes Snowden en Twitter. "Cuando el foco de la NSA en el ataque en vez de en la defensa provoca apagones en hospitales estadounidenses, es hora de actuar", insistió en otro tuit.

Con diversas modificaciones, el virus Petya se conoce desde 2016. A diferencia de otros 'ransomware', Petya no encripta los archivos por separado, sino todo el disco duro, con lo cual impide el arranque del ordenador hasta que sea desactivado. Este virus 'extorsionador' encripta así las computadoras y pide dinero para desbloquearlas. El ataque de este martes solicita 300 dólares en bitcoines para recuperar el acceso al dispositivo y a los archivos.