Masterhacks – Siete exploits supuestamente sustraídos de la Agencia Nacional de Seguridad (NSA), fueron detectados en el nuevo malware denominado EternalRocks. Se estima que puede ser más peligroso que WannaCry, que afectó a cerca de 150 países el pasado 12 de mayo.

Según RT, el nuevo virus aprovecha las vulnerabilidades de los sistemas Windows relacionadas con el protocolo de red SMB. Seis de estos exploits han sido utilizados por la NSA para llevar a cabo tareas de ciberespionaje, asimismo, estas herramientas habrían sido filtradas por el grupo de hackers ShadowBrokers.

Miroslav Stampar, experto croata en seguridad informática, fue quien identificó el malware, y explica que la ejecución del ataque de EternalRocks se produce en dos etapas. «Después de unas ocho horas de análisis descubrí cómo provocar la segunda fase», dijo Stampar a RT.

«Me sentí un poco conmosionado y asustado porque alguien ha logrado de forma exitosa y profesional empaquetar todos los exploits del SMB. Creo que algo más grande que WannaCry está por llegar», agregó el experto.

También afirmó que en la etapa inicial, EternalRocks se encuentra oculto en el dispositivo infectado, y se puede activar más tarde para propósitos maliciosos. «Su único propósito en ese momento es la propagación, está en espera de más actualizaciones de mando y control. Creo que esto sólo es el comienzo».

La segunda etapa se activa luego de 24 horas, cuando los exploits comienzan a ser descargados y el virus envía una señal a los demás servidores infectados. A diferencia de WannaCry, que alerta a las víctimas sobre la infección, EternalRocks permanece oculto y en silencio.

Se ha criticado a la NSA por mantener en secreto la existencia de estos exploits. El congreso de Estados Unidos presentó un proyecto de ley, que en caso de ser aprobado, obligaría al gobierno estadounidense a entregar su arsenal cibernético a comisiones independientes de revisión.