EternalRocks, le successeur de WannaCry encore plus inquiétant ?

EternalRocks, le successeur de WannaCry encore plus inquiétant ?

Après l'attaque du ransomware WannaCry, les chercheurs ont identifié le ver de réseau EternalRocks. Celui-ci utilise jusqu'à 7 outils de hacking ayant été volés à la NSA puis exposés par le groupe Shadow Brokers.

Selon Malwarebytes, WannaCry a recherché les ports SMB vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et le backdoor DoublePulsar pour installer le ransomware. EternalRocks utilise aussi ces deux outils. (crédit : D.R.)

Une semaine après l'attaque perpétrée par le ransomware WannaCry au niveau mondial, un autre logiciel d'exploitation de failles fait parler de lui. Selon des chercheurs en sécurité, il y a au moins une personne qui utilise 7 des outils d'attaque volés à la NSA dans un ver de réseau dénommé EternalRocks par ceux qui l'ont identifié. Les chercheurs ont constaté que ce ver ciblait la même vulnérabilité du protocole SMB de Windows, en s'avérant plus menaçant et plus difficile à contrer. Comme WannaCry, EternalRocks utilise EternalBlue, l'un des outils de la NSA.

Malwarebytes pense que WannaCry n'a pas été diffusé par une campagne de spams malveillant mais par une opération de scanning qui a d'abord recherché les ports SMB accessibles publiquement et vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et d'utiliser la porte dérobée DoublePulsar pour installer le ransomware…[lire la suite]

Réagissez à cet article