EternalRocks, un ver mieux outillé que WannaCry

Traumatisés par WannaCry et sa viralité, les chercheurs en sécurité sont toujours aux aguets concernant des répliques. Miroslav Stampar, membre du CERT Croate et créateur du service sqlmap pour détecter les attaques par injection SQL, a trouvé au sein d'un honeypot (serveur piège), un ver s'appuyant sur plusieurs outils de la NSA ciblant aussi SMB de Windows.

Sept exploitation de failles exactement contre 2 pour WannaCry. Ce ver baptisé par le chercheur EternalRocks intègre 6 services visant SMB. Il s'agit d'EternalBlue (utilisé par WannaCry), Eternalchampion, Eternalromance et Eternalsynergy qui sont des exploits SMB. Deux autres solutions SmbTouch et ArchiTouch servent à mener des opérations de reconnaissance des ports SMB vulnérables. Enfin comme WannaCry, EternalRocks se sert de l'outil DoublePulsar pour se propager sur d'autres machines vulnérables. Soit 7 outils de la NSA au total.

Moins dangereux pour l'instant

Pour le chercheur, EternalRocks est moins dangereux que WannaCry , car il ne contient pas de charges malveillantes. Nonobstant, Miroslav estime que ce ver n'est pas à prendre à la légère, car il s'avère très complexe. Une fois qu'il infecte sa victime, le ver s'installe en deux temps avec une seconde étape différée. Sur la première, EternalRocks s'installe sur son hôte, télécharge un client Tor et fixe son serveur C&C sur un domaine en .onion sur le Dark Web. La seconde phase attend pendant une période définie, 24 heures dans le cas présent, pour activer le serveur C&C. Ce long délai sert au ver de contourner les tests de sécurité via des sandbox et les analyses des spécialistes de sécurité, car très peu attendront une journée pour avoir une réponse du serveur C&C. Une fois ce laps de temps passé, le ver télécharge une archive zip au nom évocateur : shadowbrokers.zip. Elle contient les exploits de la NSA cités précédemment.

On peut ajouter dans les moyens de subterfuges l'utilisation par EternalRocks des noms de fichiers identiques à ceux de WannaCry. Mais contrairement à ce dernier, EternalRocks n'inclut pas de domaine kill switch, talon d'Achille du ransomware que des chercheurs ont trouvé pour endiguer sa propagation.

Pour Miroslav Stampar, EternalRocks est dangereux, car il peut-être armé en un instant. Actuellement, le ver s'apparente à un test ou un début de développement. Ransomware, RAT, trojan bancaire, la liste des charges utiles est longue pour tenter de faire mieux que WannaCry.

A lire aussi :

Windows 7 est l'OS Microsoft qui a le plus souffert de WannaCry

WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue

Photo credit: medithIT via VisualHunt / CC BY