Un chercheur élargit à l'ensemble des plates-formes Windows les exploits de la NSA

Les outils de piratage de la NSA exfiltrés par le mystérieux groupe de hackers The Shadow Brokers en avril dernier n'ont pas fini de faire parler d'eux. Y compris du côté des experts en sécurité. A commencer par le chercheur Worawit Wang, qui semble se faire une spécialité d'enrichir les outils en question pour les rendre toujours plus efficaces, à des fins de démonstration évidemment.

L'expert d'origine thaïlandaise s'est penché sur EternalSynergy, un « exploit » qui, selon Microsoft, n'affecte que Windows 8 et les OS antérieurs. Pas les moutures plus récentes donc. Comme pour EternalBlue, notamment exploité par WannaCry pour se propager dans le réseau, EternalSynergy s'appuie sur les failles des services SMBv1 pour exécuter du code malveillant sur la base de la faille référencée CVE-2017-0143 et comblée en mars par Microsoft, via le correctif MS17-010.

Même vulnérabilité, autre méthode

Sauf que Worawit Wang entend exploiter cette même vulnérabilité, mais avec une autre méthode. Baptisée zzz_exploit.py, celle-ci *« utilise les mêmes bugs mais une méthode différente pour les exploiter*, explique le chercheur sur Twitter. *Mon exploit a moins de chance que EternelRomance/EternelSynergy de crasher sa cible. »* L'expert en sécurité fait notamment référence à EternelBlue qui faisait planter Windows XP. Ce qui a expliqué le manque d'efficacité du vieil OS de Microsoft dans la propagation de WannaCry, alors même que ses failles de sécurité ne sont plus corrigées depuis avril 2014.

Pire : l'exploit du chercheur serait efficace avec toutes les plates-formes Windows, de XP SP2 à Server 2016, en 64 bits comme en 32 (x86), à l'exception de Windows 10, selon les détails du code publié sur GitHub. Les capacités de zzz_exploit.py ont notamment été confirmées par Sheila A. Berta, experte en sécurité pour Telefónica, qui a publié une méthode d'exploitation d'EternalRomance/Synergy sur Windows Server 2016.

Windows 10 pas à l'abri

CVE-2017-0143 est exploitable avec EternalRomance, EternalSynergy et, désormais, l'outil de Worawit Wang. Les cybercriminels pourraient donc s'emparer de ce dernier pour lancer des attaques sur la quasi-totalité des plates-formes Windows, Windows 10 excepté. Mais ce dernier n'est pas totalement à l'abri. En juin dernier, les chercheurs de RiskSense ont mis au point un système, qui n'a pas été rendu public, pour contourner les protections de l'OS face à EternalBlue. L'apparition d'outils malveillants combinant l'ensemble de ces méthodes pour s'attaquer aussi à Windows 10 n'est peut-être plus qu'une question de mois ou de semaines. Les responsables de la sécurité ont tout intérêt à ne pas négliger les futures mises à jour système proposées par Microsoft.

Lire également

EternalRocks, un ver mieux outillé que WannaCry
Shadow Brokers : d'autres exploits de la NSA contre 22 000 $ mensuels
Esteemaudit : une zero day sur RDP de Windows XP et 2003 inquiète

crédit photo © Gajus- shutterstock