Athena de la CIA, une autre épée de Damoclès au-dessus de Windows

Branle-bas de combat sur Windows ! L'OS de Microsoft est attaqué de toute part. Après WannaCry, utilisant une faille dans SMB, et EternalRocks, s'appuyant sur d'autres outils de la NSA, c'est au tour de *Wikileaks* de dévoiler Athena issu du portefeuille de la CIA.

Ce projet de l'agence a pour objectif de compromettre n'importe quelle version de Windows sur le marché, soit de XP à la version 10. Cet exploit est capable de déployer d'autres malwares ou d'accéder aux fichiers locaux. « *Une fois installé, le malware fournit une capacité de balisage (y compris de la configuration et de la gestion de tâches), le chargement/ exécution des charges malveillantes sur des tâches spécifiques, la délivrance et le retrait de fichiers vers ou depuis un répertoire désigné sur le système ciblé. Cela donne un moyen à l'opérateur de configurer les paramètres pendant l'exécution et le personnaliser pendant une opération* », précise *Wikileaks*. Ces quelques phrases montrent que la CIA peut maîtriser complètement un système Windows, récupérer les données de l'ordinateur cible et les télécharger sur ses propres serveurs.

Un malware créé avec une société tierce

Athena a été créé en août 2015 soit un mois après le lancement de Windows 10 (juillet 2015). Les documents analysés par *Wikileaks* montrent que le malware n'a pas été développé par la CIA elle-même. Il s'agit d'une collaboration avec une société américaine nommée Siege Technologies. Cette dernière se définit comme un spécialiste de la sécurité informatique se concentrant sur des « *technologies offensives de cyberguerre* ». Le projet Athena a été développé à l'origine pour contourner les antivirus.

Dans la documentation de la CIA, on peut lire que « *l'installation contourne le service dnscache* ». Et d'ajouter : « *sur Windows 7 et 8, ce service s'exécute dans une instance netsvcs par défaut, mais sur Windows 8.1 et 10, ce service tourne en tant NetworkService* ». La question en suspens après les révélations de *Wikileaks* : est-ce que Microsoft a déjà corrigé les failles liées au projet Athena dans Windows, le site dirigé par Julian Assange s'étant engagé à prévenir les éditeurs concernés par les exploits de la CIA qu'il dévoile peu à peu ? Même si l'existence d'un correctif ne constitue en rien une assurance tout risque. Le cas de WannaCry, basé sur des failles patchées depuis mars 2017, suffit à le prouver.

A lire aussi :

Cisco panse les switches vulnérables aux zero days de la CIA

Intel corrige une faille sur les puces serveurs commercialisées depuis 2008