Combien de millions de BIOS voudriez-vous infecter ?

La conférence sur la sécurité informatique de Vancouver, CanSecWest, révèle toujours des surprises et propose des interventions de haut niveau. Patrick Wardle, ancien de la NSA et de la NASA va démontrer comment déjouer la sécurité de Mac OS X. Deux chercheurs de LegbaCore, **Xeno Kovah et Corey Kallenberg**, ont décidé de s'attaquer au BIOS.

Cet élément essentiel d'un ordinateur comprend un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère, lui permettant d'effectuer des opérations élémentaires lors de sa mise sous tension, par exemple la lecture d'un secteur sur un disque. Le Basic Input Output System est le fruit de toutes les attentions en matière de sécurité y compris par les Etats. Dans le catalogue de service ANT de la NSA, l'intégration d'un malware dans le BIOS était une cible. De plus, les récentes révélations sur le groupe Equation à l'origine du module NLS_993W.DLL qui reprogrammait certains firmwares, laissent peu de doute sur l'existence de rootkits touchant le BIOS sur le marché.

Un mouchard invisible dans le BIOS

Xeno Kovah et Corey Kallenberg ont élaboré ce type d'outil qu'ils vont dévoiler dans une communication au titre évocateur : « *Combien de millions de BIOS voulez-vous infecter ?* ». « *Le plupart des BIOS ont des protections pour les modifications. Nous avons trouvé un moyen pour automatiser la découverte de vulnérabilités et casser ces protections* », avouent les deux spécialistes interrogés par nos confrères de *Threatpost*. Ils ont réussi à placer leur agent « **LightEater** » dans le **System Management Mode (SMM)** qui est utilisé par le firmware et fonctionne séparément de l'OS. Ce dernier reste dans la ligne de mire de l'implant, car SMM a accès à la mémoire.

Pour la démonstration, l'agent a été masqué dans Tails, un OS sécurisé, qui a permis de voler des mots de passe et les communications chiffrées. « *Nous avons infecté un PC HP et nous avons observé comment LightEater s'appuyait sur la technologie Serial Over Lan d'Intel pour exfiltrer les données depuis SMM sans avoir besoin du pilote de la carte réseau.* » A noter que cet implant est parfaitement invisible et qu'il n'est pas sensible à la réinstallation de l'OS.

Les deux spécialistes soulignent que **leur expérimentation ne prend que 2 minutes avec un accès physique** à l'ordinateur pour en prendre le contrôle. Les tests ont été réalisés sur des équipements Gigabyte, Acer, MSI, HP et Asus. « *La plupart des gens ne corrigent par leur BIOS et donc la majorité d'entre eux est affecté par au moins une vulnérabilité* », explique Xeno Kovah à *The Register*. Il ajoute que le système UEFI qui est le successeur du BIOS notamment avec l'arrivée de Windows 8 est faillible « *en raison d'une importante réutilisation du code dans l'UEFI, les vulnérabilités du BIOS peuvent être automatiques et solides* ». Lors de leur présentation, ils vont dévoiler un petit programme à disposition des constructeurs pour évaluer leur exposition à ce type de menaces.

A lire aussi :

Rakshasa : le malware qui s’attaque au BIOS

Le BIOS peut cacher des ‘rootkits’

Crédit Photo : TKSdesign-Shutterstock