Une backdoor cachée dans les derniers processeurs Intel ?

Y a-t-il une backdoor dans les dernières puces d'Intel. Damien Zammit, chercheur en sécurité, a découvert un sous-système dans ces processeurs qui est plein de mystères. Ce sous-système se nomme Management Engine (ME) et il est présent physiquement sur un micro-processeur ARC 32 bits à l'intérieur du chipset x86. Il exécute son propre code source. Le fondeur explique que ME a été conçu pour aider les entreprises à gérer leurs ordinateurs à distance. Une option payante que l'on peut enclencher via Active Management Technology (AMT). Damien Zammit souligne qu'AMT fonctionne en dehors de tout OS installé et peut accéder à n'importe quel ordinateur déployé.

Pour qu'AMT puisse exécuter ses fonctions de gestion à distance, la plateforme ME accède sans autorisation à une partie de la mémoire de la puce et installe un serveur TCP/IP via l'interface réseau. Ce serveur est capable, selon le spécialiste, d'envoyer et recevoir des données, sans se soucier de l'exécution ou non d'un OS et d'un pare-feu.

Une succession d'obstacles opaques

A première vue, cet outil de gestion des ordinateurs à distance n'a rien d'inhabituel, mais Damien Zammit soulève quelques interrogations. La première est que personne n'a eu accès au code source de la plateforme ME. En second lieu, le firmware de ME est chiffré avec une clé RSA 2048, résistante donc à une attaque par force brute. Troisième élément, l'expert constate que dans les gammes de CPU, au-delà des Intel Core 2, ME ne peut pas être désactivé sinon le processeur refusera de démarrer. Enfin quatrième et dernier point soulevé, il n'existe aucun moyen d'auditer le bon fonctionnement du firmware ME.

Le Management Engine s'appuie sur un modèle de sécurité fondé sur l'opacité pouvant se traduire par le « vivons heureux, vison caché », constate le chercheur dans un exposé pour la conférence BoingBoing. Une méthode considérée comme mauvaise par les spécialistes. « *En effet, si les secrets de ME sont compromis (et ils finiront par l'être soit par des chercheurs, soit par des pirates), le modèle de sécurité de ME tombera, exposant tous les systèmes Intel récents aux pires rootkits imaginables* », prédit Damien Zammit.

Le chercheur s'attelle donc maintenant à trouver une alternative libre pour le firmware de ME. *« L'objectif n'est pas de remplacer ME, mais de fournir au minimum un firmware libre, auditable et de laisser le choix aux utilisateurs »*, conclut-il.

A lire aussi :

Chiffrement : la CNIL casse les backdoors

Mozilla : la sécurité ne doit pas passer par des backdoors

Crédit Photo : PANIGALE-Shutterstock