Rakshasa : le malware qui s'attaque au BIOS

Expert en sécurité IT pour la société **Toucan**, le Français **Jonathan Brossard** a mis à profit la conférence **Defcon** pour lever le voile sur **Rakshasa**, un backdoor capable de se substituer au BIOS d'une machine pour l'infecter à l'amorçage sans laisser aucune trace sur le disque dur.

Ce malware est un croisement des BIOS open source **Coreboot** et **SeaBIOS**. Après quatre semaines de développement, il est capable d'infecter quelque 230 modèles de cartes mères à l'appui d'un simple fichier texte anodin. Sa particularité : il se propage jusque dans le firmware de périphériques PCI telles les cartes réseau, dont il peut notamment reprogrammer le micrologiciel iPXE pour contourner les éventuels obstacles que pourraient constituer des interrupteurs matériels (switchs).

Méfaits en coulisse

Avant même le démarrage du système, une connexion s'initie, de préférence par Wifi ou Wimax pour laisser des traces moins tangibles sur le réseau local. À défaut, l'interface Ethernet entre en jeu pour rapatrier du code malveillant, par HTTP(S) ou FTP (prise en charge des protocoles IP, UDP, TCP, etc.) via un bootkit. Le processus est effectif à chaque mise en route, car rien n'est stocké sur le disque dur. Rakshasa transfère tout en RAM dans un souci de discrétion. Il peut également se mettre à jour à distance.

Agnostique des systèmes d'exploitation, ce malware dont la dénomination reprend celle des démons de la mythologie hindoue contourne les pare-feu et les proxys, désactive le chiffrement des données et affiche si nécessaire un simili-BIOS. S'attaquer directement aux microcontrôleurs de la carte mère pour émuler un clavier lui permet de passer outre les protections par mots de passe. Quant aux puces TPM (Trusted Platform Module), elles s'avèrent inutiles, Rakshasa ne sollicitant pas la mémoire de masse.

Irréductible malware

Pis encore, cette trouvaille dévastatrice de Jonathan Brossard, en plus de rester incognito au radar des antivirus, est à même de se loger dans le firmware d'autres périphériques, typiquement les lecteurs de disques optiques. En cas de détection et de remise à zéro du BIOS de la carte mère, Rakshasa, confortablement dissimulé aux yeux des victimes peu soupçonneuses, n'a plus qu'à se remettre à son office. La seule manière de s'en débarrasser sans retour implique un démontage et une réinitialisation de tous les composants sujets à infection. Ce qui requiert du matériel onéreux.

À l'occasion de la conférence Black Hat de Las Vegas et de la Defcon qui a suivi, Jonathan Brossard a mis en avant les pratiques douteuses de certains États en la matière, alors qu'une enquête sénatoriale de Jean-Marie Bockel a récemment démontré que certains routeurs chinois soulevaient des risques pour la sécurité nationale. D'autant plus que la plupart des machines concernées par

Rakshasa sont assemblées… dans l'Empire du Milieu !

Crédit image : Bloomua – Shutterstock.com

Voir aussi

Quiz Silicon.fr – Connaissez-vous le monde des stations de travail ?