NSA : backdoors à gogo pour affaiblir les disques durs et les serveurs

Si les révélations d'Edward Snowden, relayées par Der Spiegel, jettent un trouble sur la sécurité des équipements réseaux des principaux équipementiers, les DSI ont ce soir un autre motif d'inquiétude : les **backdoors créées par la NSA au sein des BIOS de cartes-mères et des firmwares de disques durs**. Deux cibles que semble privilégier la division ANT (acronyme signifiant probablement Advanced ou Access Network Technology), véritable SSII du hack mettant à disposition des autres services de la NSA un **catalogue de services** pour mettre en place leurs opérations d'espionnage. Catalogue qu'Edward Snowden s'est chargé de faire fuiter auprès de Der Spiegel, même si la version publiée remonte à 2008.

Ainsi, la vulnérabilité IronChef permet d'écouter à distance des communications sur un réseau privé via l'installation d'un logiciel et d'un module de communication matériel. « *Cette technique est supportée par le **serveur HP Proliant 380DL G5**, sur lequel a été installé un implant matériel communicant par l'interface I2C (un bus de communication conçu par Philips et maintenu par NXP, NDLR)* », écrit la NSA dans un document publié sur Der Spiegel. Dans son article détaillant les services de ANT, nos confrères précisent que les machines de Dell sont également concernées par les techniques d'écoute sur mesure citées dans le catalogue de la division, via une vulnérabilité appelée DeityBounce. Celle-ci permet d'assurer la **persistance d'un logiciel espion sur les serveurs Dell PowerEdge 1850, 2850, 1950 et 2950**.

Swap protège le logiciel espion

Au-delà même des concepteurs de machines, ce sont les composants que cible la division ANT. Notamment avec Iratemonk, qui s'implante dans les MBR (Master Boot Record, soit le premier secteur adressable d'un disque dur) des disques **Western Digital, Seagate, Maxtor et Samsung**, soit les principaux fournisseurs du marché. La technique supporte les systèmes de fichiers suivants : FAT, NTFS, EXT3 et UFS.

Une autre technique, baptisée Swap, permet d'exploiter le **BIOS des cartes-mères** et les secteurs protégés des disques durs pour assurer l'exécution d'un applicatif avant le lancement de l'OS. Swap fonctionne sous **Windows, Linux, FreeBSD ou Solaris** avec la plupart des systèmes de fichiers (FAT32, NTFS, EXT2, EXT3 et UFS 1.0). Autant dire qu'à ce petit jeu, c'est l'ensemble des plates-formes serveurs qui semblent aujourd'hui accessibles aux opérations spéciales de l'agence de renseignement américaine. Car il semble probable que ANT ait depuis modernisé (voire étendu) son catalogue de services pour cibler les nouvelles générations de matériels et d'OS.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes