Windows 10 toujours sensible aux attaques visant l'accès mémoire

Malgré les mesures prises par Microsoft pour prévenir les attaques DMA (Direct Memory Access), il semble que celles-ci soient toujours possibles sous Windows 10 et 8.1. Les attaques DMA visent à récupérer des informations stockées en mémoire du système comme un mot de passe, la clé de chiffrement de BitLocker, l'utilitaire qui permet de protéger les données d'un disque dur en chiffrant une partition, ou toute autre donnée sensible.

Ces attaques exploitent simplement les ports dits DMA et taillés pour permettre à un périphérique externe au PC, agrémenté d'un logiciel adéquat, d'accéder directement à la mémoire vive de son système. Les attaques DMA nécessitent donc l'accès physique à une machine allumée. Ce qui en limite certes les risques mais n'a rien d'impossible.

De la désinformation

Avec Windows 8.1, Microsoft avait pris des précautions pour éviter les attaques DMA qui n'ont rien de très récent (elles existent depuis les années 90). Simplement en implémentant des règles de sécurité. A savoir que les ports DMA sont désactivés lors du démarrage de l'OS et sont gelés lorsque l'utilisateur met son PC en veille. Néanmoins, les ports utilisés avant cette mise en veille restent ouverts au transfert de données.

Selon le chercheur en sécurité Sami Laiho, il existe des situations où les protections anti-attaques DMA de Windows ne fonctionnent pas. Et d'en faire la démonstration (à partir de la 45e minute dans une longue vidéo, repérée par *Bleeping Computer*, et réalisée dans le cadre de la conférence Microsoft Ignite 2016 à Atlanta). *« Pour Windows 10, Microsoft a déclaré que cette fonction [de protection DMA] était en place et activée par défaut. C'est de la désinformation alors qu'elle est bien présente mais pas activée par défaut »*, y déclare le chercheur. Qui plus est, la fonction ne serait configurable qu'avec InTune MDM, le gestionnaire de terminaux et d'applications de Microsoft. Soit par *« très peu »* de personnes, suggère Sami Laiho.

Une correction dans une prochaine mise à jour de Windows

Le chercheur a fini par être entendu des équipes de sécurité de Redmond. *« La protection [actuelle] ne protège que les bus PCI, par exemple ExpressCard, Thunderbolt et certaines stations d'accueil (PCIe). Les bus plus anciens et non PCI tels que 1394 et CardBus sont encore vulnérables »*, a reconnu Microsoft auprès de notre confrère américain. *« Ils fourniront un paramètre de politique de gestion de groupe dans quelques semaines aux Windows Insiders (qui accèdent aux versions bêta de Windows 10, NDLR) et publiquement plus tard*, a déclaré Sami Laiho à *Bleeping Computer*. Mais *cela protègera seulement les bus les plus récents. »* Et d'inviter les utilisateurs très regardant sur les risques de sécurité à se tourner vers les instructions que fournit le chercheur sur son blog pour protéger les PC plus anciens des attaques DMA.

Lire également

Comment Windows 10 Anniversary Update a détourné deux attaques zero day
AtomBombing, le code malveillant insensible à la protection de Windows
Plus de vulnérabilités chez Apple et Adobe que chez Microsoft en 2017