Attention, des antivirus auraient des trous de sécurité !

Attention, des antivirus auraient des trous de sécurité !

Des chercheurs israéliens ont découvert une vulnérabilité dans plusieurs antivirus. D'autres failles seront présentées à la Black Hat.

Où l'on reparle de ces produits antivirus qui abritent des failles permettant de contourner les mécanismes de défense de Windows… En septembre 2015, l'expert en sécurité informatique Tavis Ormandy, qui travaille au sein de l'équipe Google Project Zero, avait publié une étude à ce sujet.

Deux de ses confrères – en l'occurrence, Tomer Bitton et Udi Yavo, de la start-up israélienne enSilo, spécialisée dans la détection des attaques en temps réel – avaient approfondi la problématique.

Dans leur rapport, ils pointaient du doigt trois éditeurs (AVG, Kaspersky, McAfee), tout en suggérant que d'autres logiciels étaient probablement concernés par la vulnérabilité qu'ils avaient découverte.

La vulnérabilité en question permet, sans nécessiter de privilèges de niveau administrateur, d'exécuter du code malveillant en déjouant des technologies de type ASLR (distribution aléatoire de l'espace d'adressage) ou DEP (prévention de l'exécution des données).

Pour faire la jonction avec chacun des processus associés à une application (par exemple, plusieurs onglets dans un navigateur Web), l'antivirus leur alloue une zone mémoire avec des permissions en lecture, écriture et exécution (RWX).

Problème : dans de nombreux cas, cette zone est toujours à la même adresse. Un tiers parvenu à prendre le contrôle d'un programme et de son pointeur d'instructions peut donc facilement copier son code malveillant dans ladite zone… et l'exécuter.

Detours de Microsoft sur la sellette

La conférence Black Hat USA 2016, qui aura lieu du 30 juillet au 4 août à Las Vegas, sera, pour Tomer Bitton et Udi Yavo, l'occasion de faire le point sur l'avancée de leurs travaux.

À première vue, il y a des choses à dire : une demi-douzaine de failles ont été dénichées dans plus d'une quinzaine de produits. Mais ce sont potentiellement des milliers de logiciels qui sont affectés. Tout du moins tous ceux qui s'appuient sur la bibliothèque Microsoft Detours, destinée notamment à intercepter des fonctions d'applications et de processus, puis à en réécrire le code pour des fonctions cibles.

Les principaux antivirus exploitent cette technique dite de « hooking » pour détecter des comportements malveillants, entre autres au niveau des fonctions d'allocation de la mémoire (VirtualAlloc, VirtualProtect…). L'essentiel des programmes « intrusifs », comme ceux qui analysent les performances du système, en font aussi usage, dixit ITespresso.

Malheureusement, l'implantation des mécanismes d'injection de code depuis le noyau n'est pas toujours bien effectuée – que ce soit par import de tables, fonctions asynchrones ou modification du point d'entrée de la fonction cible.

enSilo a mis à disposition un outil baptisé AVulnerabilityChecker pour permettre à chacun de vérifier s'il existe, sur son système Windows, une application potentiellement vulnérable… et plus particulièrement un antivirus.

Article original de Silicon

Réagissez à cet article

Original de l'article mis en page : Des trous de sécurité dans les antivirus