Bloatware : des millions de PC Lenovo, Dell et Toshiba piratables

Les bloatwares sont de nouveaux sur la sellette. Ces logiciels préinstallés sur les PC collectionnent les problèmes de sécurité. On se souvient que Lenovo avait été victime de Superfish, un adware qui compromettait les échanges sécurisés et exposait les systèmes aux attaques de type « Man-in-the-middle ». Plus récemment, le même constructeur chinois corrigeait deux failles dans son outil de mise à jour. De même, les PC de Dell avaient été suspectés de contenir ce type de logiciel avant de s'apercevoir qu'il s'agissait en fait d'un certificat douteux.

Mais ce n'est pas fini ! En effet, un chercheur en sécurité, nommé Slipstream/Rol, vient de découvrir des vulnérabilités dans des logiciels préinstallés sur différentes marques de PC. Lenovo, Dell et Toshiba sont visés et ces failles touchent des millions d'ordinateurs aussi bien professionnels que grand public. Le spécialiste a mis en ligne un POC (prototype) pour montrer comment un cybercriminel pourrait exécuter des malwares sur les systèmes, soit via une page web spécialement conçue ou par le biais d'une pièce jointe (que le destinataire devra respectivement visiter ou ouvrir pour livrer le contenu de son PC aux attaquants).

Des applications censées aider les utilisateurs touchées

Interrogé par nos confrères de *ZDNet*, Slipstream/Rol a indiqué ne pas avoir informé Dell, Toshiba et Lenovo des failles avant la publication de son POC. Une menace prise au sérieuse dans un avis du CERT de l'Université Carnegie Mellon sur le « Solution Center » de Lenovo. Ce logiciel préinstallé informe l'utilisateur de l'état de santé du PC (réseau, sécurité, etc). On le trouve sur plusieurs machines : ThinkPad PC et tablettes, ThinkCentre, ThinkStation, IdeaCenter et certains IdeaPad, fonctionnant sous Windows 7 et plus. Les trois failles peuvent exécuter du code à distance avec une élévation de privilège sur le système. Lenovo conscient du problème a annoncé qu'il allait proposer un correctif dès que possible. En attendant, le fabricant conseille de supprimer « Solution Center » pour ne pas être exposé aux brèches.

Le constructeur Chinois n'est pas le seul concerné. Pour Toshiba, c'est le logiciel Service Station, qui recherche notamment les mises à jour pour les programmes présents sur la machine. Slipstream/Rol a indiqué que cette application permet, quand un utilisateur est connecté, de lire des parties du registre comme un utilisateur système soit avec plus de privilège qu'un utilisateur standard. Sans pour autant avoir accès au SAM (Security Account Manager) ou des bootkeys, le hacker concède qu'un pirate peut contourner les permissions fixées dans le registre.

Dell n'échappe pas à cette coupe réglée sécuritaire avec une faille trouvée dans l'application System Detect. Ce programme vérifie l'état du système avant que l'utilisateur ne contacte le service client. Ce logiciel préinstallé peut servir pour contourner une fonction de sécurité de Windows, UAC (User Account Control) et obtenir ainsi une élévation de privilège.

Pour l'instant, on ne connaît pas la réaction de Toshiba et de Dell, ni quand ils vont corriger les vulnérabilités des bloatwares incriminés.

A lire aussi :

Apple permettra de retirer le bloatware de ses iPhone
Samsung retire le bloatware de ses smartphones… en Chine

Crédit Photo : Den Rise-Shutterstock