DoubleAgent détourne les antivirus pour pirater les PC Windows

Les antivirus ont ces temps-ci mauvaise presse. Certains estiment qu'ils sont un poison pour l'écosystème logiciel, d'autres ont trouvé des failles de sécurité dans différentes solutions. Sur ce dernier point, des chercheurs en sécurité de Cybellum, viennent de présenter une technique de piratage, baptisée DoubleAgent.

Cette méthode, qualifiée de Zero Day par la firme israélienne, donne le pouvoir à un attaquant de détourner les anti-virus et les forcer à injecter du code malveillant. Elle est redoutable selon Cybellum, car elle touche toutes les versions de Windows (de XP à la version 10), l'ensemble des architectures (32 bits ou 64 bits) et l'ensemble des utilisateurs (administrateur système et autres).

Injection d'une DLL malveillante

Cet exploit s'appuie sur une application dans Windows datant de 15 ans et qui n'a jamais subi de correctifs de sécurité. Cette fonctionnalité se nomme Application Verifier Provider DLLs et s'adresse aux développeurs pour contrôler, via une DLL, les bugs dans leur programme au moment de l'exécution.

Oui mais voilà, les experts de Cybellum ont constaté que les développeurs pouvaient charger leur propre DLL de vérification au lieu de celle fournie par l'application de Microsoft. Quelqu'un de malintentionné pourrait utiliser une extension malveillante pour changer une clé de la base de registre de Windows sur une application et la détourner à des fins malveillantes.

Les antivirus tardent à corriger le problème

Il se trouve que les applications les plus sensibles à l'attaque DoubleAgent sont les antivirus. Elle a été testée avec succès sur les solutions Avast, AVG, Avira, Bitdefender, Comodo, ESET, F-Secure, Kaspersky, Malwarebytes, McAfee, Norton, Panda, Quick Heal et Trend Micro. Cette liste n'est pas limitative et les sociétés visées ont été alertées de cette menace.

Michael Engstler, CTO de Cybellum, a expliqué à nos confrères de BleepingComputer que « *nous avons signalé la technique à l'ensemble des fournisseurs depuis plus de 90 jours et nous avons travaillé avec certains éditeurs depuis* ». Mais tous n'ont pas corrigé leurs programmes. « *Les seuls à avoir publiés un correctif sont Malwarebytes (numéro de version: 3.0.6 Component Update 3), AVG (numéro de version: 16.151.8007) et Trend-Micro* », assure le dirigeant.

Une dangerosité à prendre en compte pour les autres fournisseurs. L'attaque DoubleAgent peut aussi bien désactiver l'anti-virus, le rendre aveugle à certaines attaques, le transformer en proxy pour mener des campagnes de ransomwares sur le PC et le réseau local, augmenter les privilèges sur d'autres applications, exfiltration des données et *in fine* casser le PC.

Toutes les applications sont concernées

Si dans le blog de Cybellum, DoubleAgent s'est concentrée sur les antivirus. Le CTO précise que toutes les applications sont concernées y compris le système d'exploitation lui-même. Pour cela, il s'appuie sur un POC disponible sur GitHub. « *Sans besoin de le modifier, vous l'exécutez, vous donnez le nom de l'application et vous pouvez automatiquement l'attaquer sans faire la différence entre un antivirus ou une autre application.* »

En matière de protection, Cybellum conseille de mettre à jour les solutions d'antivirus quand elles ont été corrigées. Sinon, la société de sécurité pousse à l'utilisation d'un mécanisme nommé Protected Processes, qui a été introduit dans Windows 8.1. Il permet d'éviter les injections de code, mais il n'est pour l'instant disponible que dans Windows Defender.

A lire aussi :

Un vieux piratage de session Windows remis au goût du jour

Un groupe de pirates menace de réinitialiser 200 millions d'iPhone