Des failles zero day trouvées chez Kaspersky et FireEye

La rentrée scolaire est toujours synonyme de devoirs. Les éditeurs de sécurité vont pouvoir se remettre au travail, car des hackers ont trouvé des failles critiques dans certains produits. Parmi eux, on retrouve Kaspersky et FireEye.

Dans le cadre de l'éditeur russe, c'est un chercheur de Google, Travis Ormandy qui a twitté sa découverte dans les logiciels antivirus. « *C'est une télécommande, un exploit zero interaction SYSTEM, dans la configuration par défaut. C'est le plus mauvais scénario.* » Dans un autre post, le spécialiste explique qu'il a réussi à utiliser sa technique sur les versions 15 et 16 de l'anti-virus de Kaspersky et promet des détails supplémentaires après « *son dîner* ».

Interrogé sur son fil Twitter sur le fait de savoir s'il existe des paramétrages pour pouvoir se protéger de cette faille critique, il déclare : « *Pas vraiment, il y a beaucoup de bugs dans la plupart des fonctionnalités de base, je suis en train de faire le tri.* » D'autres plus prompts lui demandent s'il est vendeur et combien la vulnérabilité coûte. Heureusement, Kaspersky a été aussi rapide et en moins de 24h a annoncé le déploiement au niveau mondial d'un patch. Une réponse un peu trop rapide au goût des spécialistes de la sécurité qui connaissent les méthodes de Travis Ormandy ; publier les vulnérabilités sans en parler préalablement aux entreprises intéressées. Une action concertée entre Kaspersky et Travis Ormandy ?

Une vague de zero days sur les appliances FireEye ?

FireEye est donc le second éditeur visé par la découverte de failles critiques. Kristian Erik Hermansen, un hacker basé à Los Angeles a expliqué sur Twitter avoir découvert pas moins de 4 vulnérabilités de type zero day dans les produits de la firme américaine. Un comble quand on sait que cette dernière fournit des solutions anti-malwares, mais également de détection des failles zero day et d'APT (menaces avancées persistantes).

Toujours est-il que Kristian Erik Hermansen ne travaille pas pour la gloire et que les brèches découvertes sont monnayables avec des montants pouvant aller à 6 chiffres (6 $ dans son jargon). La faille la plus onéreuse permet de l'injection de commande à distance pour accéder aux fichiers sources de l'appliance FireEye. Il explique dans un message sur Pastebin que « *FireEye et Mandiant (société rachetée 1 milliard de dollars en janvier 2014, NDLR) ont dans leur main plusieurs failles zero day sur leurs produits dont certaines existent depuis au moins 18 mois sans avoir été corrigées* ». Il s'en suit une charge contre Mandiant qui placerait des bugs dans ses produits et contre FireEye qui ne propose pas d'audit de ses solutions par des chercheurs externes.

Parmi les autres failles découvertes, on note aussi un contournement de l'authentification. Mais le franc-tireur de la sécurité estime qu'il n'est pas le seul à travailler sur les défauts de sécurité de FireEye. Dans un échange avec nos confrères de *CSO Online*, il indique que lui et un autre chercheur, Rob Perris, ont découvert pas moins de 30 vulnérabilités dans les produits FireEye.

A lire aussi :

Kaspersky : de faux virus oui, mais nous en avons été victimes

FireEye, Microsoft et consorts identifient un vaste réseau de cyberespionnage chinois

Crédit Photo : Gelbstock-Shutterstock