Des chercheurs volent des données en utilisant le bruit des ventilateurs d’un PC

Des chercheurs volent des données en utilisant le bruit des ventilateurs d’un PC

Créé par des chercheurs en sécurité israéliens, le malware Fansmitter exploite les ventilateurs d'un ordinateur pour transmettre des données.

Figure 1. A typical exfiltration scenario. A compromised computer (A) - without speakers, and with aud hardware disabled - transmits sensitive information via acoustic signals. This information is received and decoded by a nearby mobile phone (B)

Même le bruit des ventilateurs d'un PC peut être utilisé pour transmettre des données volées sur des machines non connectées à un réseau. Des chercheurs de l'Université Ben Gourion du Néguev en Israël ont en effet trouvé le moyen d'exploiter la vitesse des pales d'un ventilateur équipant un PC classé sensible pour générer des sons particuliers. Les ordinateurs dits sensibles sont isolés et stockent des informations confidentielles. Pour les pirater, les attaquants doivent généralement avoir un accès physique et installer des logiciels malveillants, par le biais éventuellement d'une clef USB.

Figure 1. A typical exfiltration scenario. A compromised computer (A) - without speakers, and with aud hardware disabled - transmits sensitive information via acoustic signals. This information is received and decoded by a nearby mobile phone (B)

Pour leurs tests, les chercheurs ont utilisé un simple PC tour Dell et un mobile Samsung.

Des recherches antérieures ont montré qu'une fois le PC infecté, les données pouvaient être transmises à partir des haut-parleurs de l'ordinateur sous forme de signaux sonores. Il a alors suffi de désinstaller les haut-parleurs pour améliorer la sécurité de ces machines. Les chercheurs israéliens ont donc exploité une autre méthode pour cibler ces systèmes isolés. Leur malware Fansmitter transmet secrètement des données sur les ondes audio générées par les pales d'un des ventilateurs de l'ordinateur, selon un document publié la semaine dernière.

Des ondes sonores créées par le ventilateur

En contrôlant la vitesse de fonctionnement des ventilateurs, le malware arrive à produire différentes tonalités acoustiques qui peuvent être utilisées pour transmettre des données à un smartphone. Pour récupérer les informations, les cyberpirates ont besoin de placer le micro d'un téléphone mobile près du PC isolé afin de décoder les bruits émis par le ventilateur. Une fois les signaux sonores interprétés, le mobile transmet les données aux cyberpirates. Les chercheurs ont testé leur programme malveillant en utilisant un ordinateur de bureau Dell et un mobile Samsung Galaxy S4.

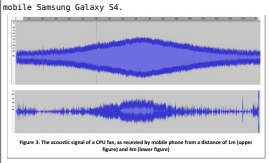

Figure 3. The acoustic signal of a CPU fan, as received by mobile phone from a distance of 1m (upper figure) and 4m (lower figure)

Les ondes sonores interceptées par le mobile sont décodées puis retransmises.

Bien sur, ce malware affiche des limites. Un maximum de 15 bits peut être transmis par minute, ce qui ne paraît pas beaucoup mais suffit pour envoyer des mots de passe et des clefs de chiffrement selon les chercheurs. Pénétrer des PC de cette façon ne semble guère pratique, mais comme la plupart des ordinateurs sont encore équipés de ventilateurs pour refroidir les principaux composants, toutes les machines sont potentiellement vulnérables. Les entreprises et les agences gouvernementales qui exploitent des PC isolés peuvent cependant contrer ces attaques en installant des systèmes de refroidissement à eau ou utiliser des radiateurs passifs, c'est-à-dire sans ventilateur, si les caractéristiques techniques du processeur et des chipsets associés le permettent. Il est également conseillé d'interdire l'utilisation de téléphones mobiles dans les salles équipées de PC isolés et de bloquer, si possible, l'usage des ports USB.

Article de Serge Leblal

Réagissez à cet article

Original de l'article mis en page : Des chercheurs volent des données en utilisant le bruit des ventilateurs d'un PC – Le Monde Informatique