Les LED des PC, des mouchards en puissance

Pollution visuelle pour certains, outil de surveillance du bon fonctionnement des équipements informatiques pour d'autres, les LED ne laissent pas indifférents. Il faudra maintenant ajouter une corde à leur arc : l'espionnage. Des chercheurs de l'Université Ben Gourion, en Israël, ont réussi à extraire à distance des données d'un disque dur via le clignotement des LED.

Le test a été réalisé avec une caméra embarquée sur un drone pour pirater un PC localisé au 3ème étage d'un immeuble. Cette expérience est basée sur la méthode dite « air gap », qui ne nécessite donc pas de se connecter à l'ordinateur cible. Il est par contre nécessaire d'installer un malware sur la machine pour préparer et transmettre les données à exfiltrer. Dans ce cas précis, le canal d'exfiltration est donc la LED du disque dur.

1 Mo de données transmises toutes les 30 mn

Morchedai Guri, un des chercheurs de l'Université israélienne, explique à nos confrères de *Wired :* « *nous avons constaté que le clignotement de la LED d'un disque dur peut-être contrôlé avec une fréquence de 6000 clignotements par seconde. Un moyen pour transmettre des données très rapidement sur de longues distances* ». Ce clignotement permet d'exploiter un code s'apparentant au Morse, via lequel les chercheurs ont découvert qu'ils pouvaient transmettre des données à des vitesses pouvant atteindre 4000 bits par seconde, soit 1 Mo toutes les 30 minutes. Pas suffisant pour un gros fichier, mais parfaitement adapté pour récupérer un mot de passe ou un fichier chiffré. Le malware est capable de rejouer ces clignotements pour s'assurer que l'ensemble des données a bien été transmis.

La LED comporte beaucoup d'avantages par rapport à d'autres techniques de piratage utilisant le « air gap ». On pense notamment à des méthodes exploitant les haut-parleurs (via les ultra-sons), les ventilateurs, la lumière des écrans ou du clavier. Même si les LED ont une portée limitée et nécessitent que l'ordinateur soit actif. La LED est en revanche opérationnelle même quand le PC est mis en veille.

Besoin d'une caméra haute définition

Parmi les défauts de cette méthode, signalons la nécessité d'employer une caméra évoluée de type GoPro pour récupérer les données des LED. En effet, la caméra d'un smartphone est seulement capable de recevoir des données à 60 bit par seconde en raison de sa faible fréquence d'images. Une caméra de type GoPro supporte 120 bits par seconde. Dans leur expérience, les spécialistes ont utilisé un capteur haute performance Siemens pour atteindre une transmission de 4000 bits par seconde.

Parmi les contre-mesures pour éviter ce type d'attaques, les chercheurs préconisent dans un premier temps de placer les ordinateurs sensibles loin des fenêtres, d'installer des filtres opaques

sur ces dernières ou, mieux, de les placer dans une salle fermée. Autre conseil aussi simple qu'efficace, masquer les LED. Même si, après la webcam, le PC devient alors un vrai aéroport à post-it ou sparadraps. La paranoïa est peut-être à ce prix !

A lire aussi :

Hacker des ordinateurs avec la chaleur des composants

Quand les ultrasons désanonymisent les utilisateurs de Tor

Crédit Photo : Visual Hunt