Pirater un ordinateur via la LED de son disque dur, c'est possible

Par Marc Zaffagni, Futura

Publié le 24/02/2017

Une équipe de l'université Ben Gourion a mis au point une technique de piratage d'un ordinateur qui s'appuie sur le décodage de l'activité de l'indicateur lumineux de son disque dur. Les chercheurs ont pu récupérer des données en utilisant notamment un drone muni d'une caméra.

Actuellement, l'un des moyens les plus efficaces de protéger un **ordinateur** renfermant des données hautement sensibles consiste à l'isoler totalement de tout réseau **physique** ou sans fil ainsi que du rayonnement électromagnétique. C'est ce qui s'appelle l'*air gap*. Or, il s'avère que des chercheurs en sécurité informatique ont déjà réussi à contourner ces défenses en se servant d'**ultrasons** pour **propager un virus** ou en écoutant la **signature sonore** de la machine lorsqu'elle travaille. On peut désormais ajouter une autre technique aussi étonnante que redoutable.

Des experts du *Cyber Security Research Center* de l'université Ben Gourion du Néguev (Israël) ont trouvé le moyen de **voler des données** dans un ordinateur placé en *air gap* en déchiffrant les pulsations lumineuses envoyées par la **LED** d'activité du **disque dur**. Encore plus fort, ils se sont amusés à récupérer ces informations à l'aide d'un **drone** à l'extérieur du bâtiment qui s'est approché d'une **fenêtre** et a filmé la machine avec une caméra qui détecte ce signal lumineux.

Voici la démonstration de piratage d'un ordinateur via la LED de son disque dr à l'aide d'un drone. Le quadricoptère se place à portée de vue de la machine et filme son voyant lumineux dont les clignotements correspondent au code binaire des données à dérober. © *Cyber Security Labs @ Ben Gurion University*

Il faut que l'ordinateur cible soit infecté par un malware

La manœuvre suppose tout de même de pouvoir infecter l'ordinateur cible avec un *malware*, ce qui ne serait évidemment pas une mince affaire dans le cas d'une configuration *air gap*. Mais tout est possible... Une fois installé, ledit **logiciel** malveillant va alors prendre le contrôle de la LED du disque dur pour la faire flasher à très haute **vitesse** (plusieurs milliers de clignotements à la seconde) de sorte qu'une personne assise devant la machine ne remarquerait même pas cette activité. La méthode s'apparente à du **morse** pour traduire en **code binaire** les données à dérober.

Ce signal est ensuite récupéré par une caméra ou un **capteur** de **lumière** placé à portée de vue de l'ordinateur et donc possiblement sur un **drone**. Mais encore faut-il que le **PC** en question soit visible... Si la technique semble assez complexe à mettre en œuvre sur un ordinateur en *air gap*, elle serait bien plus réalisable dans un contexte classique. Certains pensent aujourd'hui à se prémunir contre le piratage en occultant la **webcam** de leur pc portable et en mettant du ruban adhésif sur le microphone. Il faudra désormais aussi prévoir de cacher le voyant lumineux du disque dur !

Kézako : comment crypte-t-on les données sur Internet ? La cryptographie est la plus ancienne forme de chiffrement. On trouve des traces de son utilisation jusqu'en 2.000 avant J.-C. Cette technique encore utilisée aujourd'hui, notamment sur le Web, dévoile ses mystères en vidéo grâce au programme Kézako d'Unisciel et de l'université Lille 1.

Par Marc Zaffagni, Futura