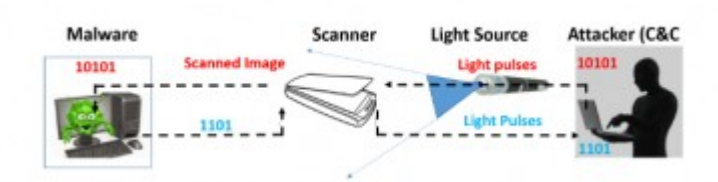
Quand les scanners se font complices des vols de données

Décidément les universitaires israéliens sont passionnés par le piratage à distance avec des techniques dites 'Air Gap' (c'est-à-dire sans connexion à Internet). Récemment, une équipe avait démontré la capacité d'extraire des données depuis le clignotement des LED des disques durs de PC.

Quelques prérequis

Toujours dans les bureaux des entreprises, une autre équipe de chercheurs a jeté son dévolu sur les scanners. Ils ont piraté à distance un scanner pour qu'il puisse transmettre des commandes à un malware installé sur un PC en mode 'Air Gap'. Bien sûr la technique est valable dans l'autre sens, c'est-à-dire que le scanner peut être utilisé pour exfiltrer des données. Ils l'expliquent dans un document intitulé avec malice : « Oops… Je pense avoir scanné un malware »

La technique de piratage repose toujours sur la lumière. Dans le cas du scanner, un faisceau de lumière est considéré comme le binaire 1 et une absence de lumière comme le binaire 0. Pour réaliser leur expérience, les scientifiques attirent l'attention sur 2 éléments : le capot du scanner doit être ouvert pour qu'un laser puisse atteindre les capteurs des assaillants et un malware doit être installé sur un PC relié au scanner. Ce malware est programmé pour activer un scan à une date et heure précises. On est donc clairement dans une attaque ou un espionnage prémédité et ciblé.



Un laser ou via une ampoule connectée

Pour mener l'attaque, les chercheurs ont utilisé différents moyens. Ils ont ainsi mis un laser sur un drone et ont réussi à transmettre des données à une distance de 15 mètres. Avec un support fixe, cette distance est portée à 900 mètres. Ils ont testé également le piratage d'une ampoule connectée pour piloter le scanner et donner ainsi des instructions au PC compromis. Ce type d'attaques est imperceptible, constatent les chercheurs, car la variation de la lumière n'excède pas 5%.

Durant leurs tests, les chercheurs ont par exemple envoyé des commandes de suppression d'un PDF (d x.pdf) ou de chiffrement d'un dossier (en q). Les commandes ont pris entre 50 et 100 millisecondes pour être envoyées. La fuite de données est aussi possible à travers la lumière émise par le scanner, mais les chercheurs assurent que l'extraction est relativement difficile. Mais pas impossible.

A lire aussi :

Les LED des PC, des mouchards en puissance

Quand les ultrasons désanonymisent les utilisateurs de Tor