# Cinq technologies de cyberespionnage utilisées sans connexion à Internet | Le Net Expert Informatique

**Un système connecté à Internet est toujours sujet à des menaces, et ce quel que soit son niveau de protection. De nos jours, tous les adolescents en ont parfaitement conscience. Aucun logiciel de protection ne peut éviter complètement les erreurs humaines dans les codes de programmation ou empêcher des comportements d'utilisateur.**

C'est pourquoi, en général, les appareils dont les fonctions sont spécialement importantes ou dont le contenu est top secret ne sont pas connectés à Internet. Il est toujours préférable d'accepter un inconvénient plutôt que de faire face à des conséquences fâcheuses. C'est de cette manière que sont protégés, par exemple, les systèmes de contrôle de gros objets industriels ou les ordinateurs de certaines banques.
Une déconnexion permanente semblerait être la meilleure solution pour garder des données secrètes : s'il n'y a pas d'Internet, alors il ne peut pas y avoir de fuite de données. Or, ce n'est pas vrai. Les techniques de transfert de données à distance, adoptées depuis longtemps par les services secrets, deviennent chaque année plus accessibles aux utilisateurs " commerciaux ".A présent, il est de plus en plus habituel de rencontrer certains gadgets d'espionnage que James Bond possédait.

**Espionnage électromagnétique**
Tout appareil connecté à une ligne de courant génère des émissions électromagnétiques qui peuvent être interceptées par des technologies éprouvées. Il y a près de cinquante ans, les services de sécurité des Etats-Unis et de l'URSS étaient impliqués dans de telles fuites. La quantité d'informations obtenues depuis lors est énorme. Une partie des activités menées par les Etats-Unis est connue sous le nom de code TEMPEST, et certaines affaires déclassifiées sont aussi passionnantes que des romans policiers.

**Autrefois, les écrans à tube cathodique et les connecteurs VGA sans protection étaient les maillons les plus faibles. Ces dernières années, les claviers sont devenus les jouets favoris des chercheurs en protection des données.**
Bien que beaucoup de temps se soit écoulé, de nouvelles méthodes pour " surfer " sur des ondes électromagnétiques apparaissent à mesure que les équipements électriques évoluent. Autrefois, les écrans à tube cathodique et les connecteurs VGA sans protection constituaient les maillons les plus faibles qui produisaient du bruit électromagnétique. Ces dernières années, les claviers sont devenus les jouets favoris des chercheurs en protection des données. Les recherches effectuées dans ce domaine portent régulièrement leurs fruits. En voici quelques exemples.
Les frappes peuvent être tracées avec haute précision par un appareil artisanal placé à vingt mètres, qui analyse le spectre radioélectrique et qui coûte 5 000 dollars. Il est intéressant de savoir qu'une attaque est aussi efficace si elle vise des claviers USB de premier prix, des claviers sans fil avec chiffrement du signal plus chers, ou encore des claviers intégrés à des ordinateurs portables.
Tous ces appareils fonctionnent de la même manière et génèrent du bruit électromagnétique. La seule différence réside dans la puissance du signal, qui dépend de la longueur de la ligne de transmission de données (par exemple, elle est plus courte avec des ordinateurs portables).
Tous ces appareils fonctionnent de la même manière et génèrent du bruit électromagnétique. La seule différence réside dans la puissance du signal, qui dépend de la longueur de la ligne de transmission de données (par exemple, elle est plus courte avec des ordinateurs portables).

Les données peuvent être plus facilement interceptées si l'ordinateur visé est relié à une ligne de courant. Les variations de tension, qui correspondent aux frappes, génèrent du bruit électromagnétique au niveau du sol. Ce bruit peut être intercepté par un hacker qui est connecté à une prise de courant proche. Le prix de l'équipement, avec une portée effective de 15 mètres, est de 500 dollars.

Comment contrecarrer cette menace ? La meilleure manière de se protéger contre l'espionnage électromagnétique serait de sécuriser une pièce (cage de Faraday) et d'utiliser des générateurs de bruits spéciaux. Si vos secrets ne sont pas si précieux, et si vous n'êtes pas prêts à recouvrir les murs de votre sous-sol avec de l'aluminium, alors vous pouvez simplement utiliser un générateur de bruit " manuel " : taper des caractères inutiles de manière sporadique et les effacer ensuite. Pour saisir des données précieuses, vous pouvez utiliser un clavier virtuel.

**Cinq technologies de cyberespionnage utilisées sans connexion à Internet**
**1. Faites attention aux lasers**
Il existe des méthodes alternatives d'enregistrement de frappes. Par exemple, l'accéléromètre d'un smartphone, posé près d'un clavier, présente un taux de reconnaissance d'environ 80%. Ce taux n'est pas suffisamment élevé pour intercepter des mots de passe, mais il permet de déchiffrer le sens d'un texte. Cette méthode compare les différentes vibrations produites par les paires de signaux successifs qui correspondent aux frappes.
Un rayon laser, discrètement dirigé vers un ordinateur, constitue la méthode la plus efficace pour enregistrer les vibrations. D'après les chercheurs, chaque frappe produit ses propres vibrations. Le laser doit être dirigé vers une partie d'un ordinateur portable ou d'un clavier qui réfléchit bien la lumière. Par exemple, vers le logotype du fabriquant.
Comment contrecarrer cette menace ? Cette méthode ne fonctionne que si le rayon laser est proche. Par conséquent, essayez de ne pas vous laisser approcher par des espions.

**2. Ecouter la radio**
Il n'est pas toujours utile d'intercepter les données d'un clavier, puisque cela ne donne évidemment pas accès à la carte mémoire d'un ordinateur. Cependant, il est possible d'introduire un malware dans un ordinateur déconnecté par des moyens externes. C'est de cette façon que le célèbre ver Stuxnet s'est infiltré dans un ordinateur cible au sein d'une infrastructure d'enrichissement de l'uranium. Après l'infection, le malware a fonctionné comme un espion infiltré, " aspirant" des informations grâce à un certain support physique.
Par exemple, les chercheurs israéliens ont développé un software qui module les émissions électromagnétiques dans le hardware des ordinateurs. Ces signaux de radio sont puissants et peuvent même être captés par des récepteurs FM standards de téléphone.
Pourquoi une telle complexité ? Les ordinateurs qui comportent des données classifiées sont placés dans des pièces sécurisées, et leur accès est limité afin d'éviter toute fuite possible. Cependant, contrairement à un analyseur de spectre, un téléphone espion peut être facilement introduit dans de telles pièces.
Comment contrecarrer cette menace ? Tous les téléphones, ainsi que tous équipements suspects, doivent rester à l'extérieur des pièces sécurisées.

**Tiède… Chaud… Brûlant !**
Récemment, les chercheurs israéliens que nous avons déjà mentionnés ont exposé un scénario de vol de données un peu plus exotique… par le biais d'émissions thermiques !
Le mode opératoire de l'attaque est le suivant. Deux ordinateurs de bureau sont placés l'un à côté de l'autre (environ 40 centimètres les séparent). Les capteurs thermiques de la carte mère interne de l'un de ces ordinateurs pistent les changements de température de l'autre.
Le malware change périodiquement la température du système en ajustant le niveau de charge et envoie un signal thermique modulé
Par commodité, un ordinateur déconnecté est souvent placé juste à côté d'un ordinateur connecté à Internet, et ce n'est que la stricte vérité. L'ordinateur déconnecté comporte des données classifiées, tandis que l'autre est un simple ordinateur connecté à Internet.

Si quelqu'un introduit un malware dans ces deux systèmes, voici ce qui se produit. Le malware lit les données classifiées, puis change périodiquement la température du système en ajustant le niveau de charge et envoie un signal thermique modulé. Le deuxième ordinateur reçoit et déchiffre ce signal, avant d'envoyer les données classifiées par Internet.

L'inertie thermique du système empêche une transmission rapide des données. La vitesse de transmission est alors limitée à huit bits par heure. A ce rythme, il est possible de dérober un mot de passe, mais le vol d'une base de données est remis en question.

Toutefois, avec le succès que rencontrent les gadgets connectés à Internet, le rôle du deuxième ordinateur, qui aspire les données, peut facilement être rempli par une climatisation intelligente ou un capteur climatique, lesquels enregistrent les changements thermiques avec beaucoup de précision. Le taux de transfert pourrait augmenter de manière significative dans un futur proche.
Comment contrecarrer cette menace ? Ne placez pas un ordinateur déconnecté, qui comporte des données classifiées, à côté d'un ordinateur connecté à Internet.

**Toc, toc, toc. Qui est là ?**
Une pièce bien sécurisée classique n'assure pas une protection complète contre les fuites de données. Les murs en acier sont imperméables au bruit électromagnétique, mais pas aux ultrasons.
Dans le cas d'une technologie à ultrasons, un équipement espion se compose de deux unités compactes. L'une d'elles est discrètement placée à l'intérieur d'une pièce sécurisée, tandis que l'autre est placée quelque part ailleurs. Le taux de transfert de données à travers l'acier pour les ultrasons atteint 12 MB/s. En outre, l'une des unités n'a pas besoin d'être chargée car l'énergie est transmise en même temps que les données.
Comment contrecarrer cette menace ? Si vous possédez votre propre pièce sécurisée avec des murs en acier, alors vous devriez vérifier minutieusement chaque équipement qui y est installé.
En général, connaître les techniques modernes d'espionnage (" modernes " du moins aux yeux du grand public) vous permet de conserver vos données intactes. Sur le plan logiciel, une solution de sécurité élevée est indispensable.

---



---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://blog.kaspersky.fr/when-going-offline-doesnt-help/4607/