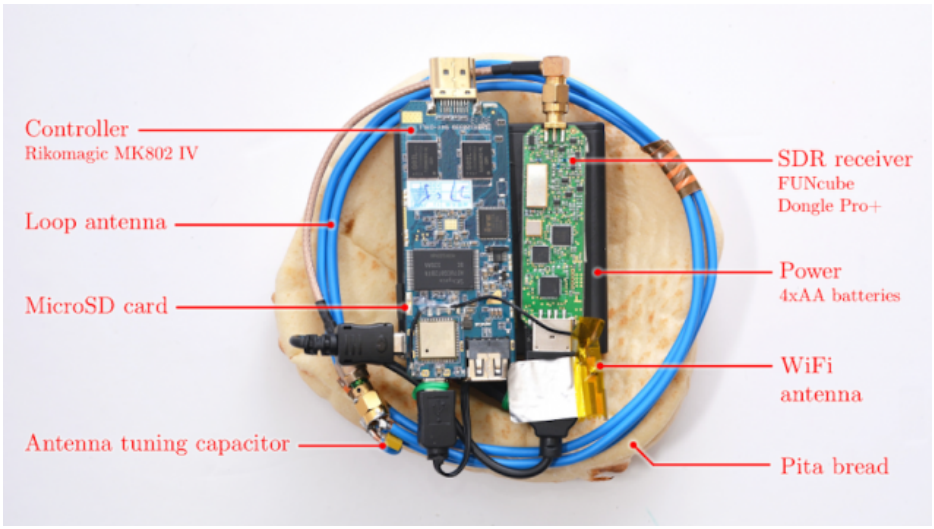
Pour pirater un ordinateur, une pita suffit | Le Net Expert Informatique

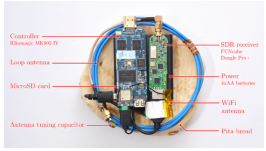


Pour pirater un ordinateur, une pita suffit

Selon une étude de l'université de Tel-Aviv, travailler dans un café pourrait s'avérer risqué pour la sécurité de votre ordinateur

Cette pita, qui donne l'apparence innocente que quelqu'un mange ostensiblement en face de vous dans le café de votre quartier, pourrait contenir un système d'espionnage informatique pouvant infiltrer les protocoles d'encodage les plus sécurisés de votre ordinateur.

Pire encore, ont déclaré les chercheurs de l'Université de Tel-Aviv, les utilisateurs de cet ordinateur ne peuvent pas faire grand chose pour se protéger.
« Des techniques d'atténuation… pourraient inclure des cages Faraday », des écrans en métal spécialement posés au sol qui bloquent les radiations… « Pourtant, la protection peu chère de PC de niveau commercial semble difficile », explique l'équipe.
Dans un article publié mardi, les chercheurs décrivent le très faible coût de l'équipement de type Radio Shack, que l'on peut facilement cacher dans un pain pita standard et qui peut être utilisé pour « lire » des impulsions électromagnétiques provenant du clavier d'un ordinateur standard, y compris les frappes sur le clavier afin de décrypter les documents sécurisés.
De manière amusante, l'Université de Tel-Aviv a appelé l'attaque PITA, Instrument portable pour l'acquisition de signaux.



L'étude, menée par les chercheurs Daniel Genkin, Itamar Pipman, Lev Pachmanov et Eran Tromer a été publiée pour coïncider avec une conférence majeure de sécurité informatique qui va avoir lieu à l'Université de Tel-Aviv (UTA) cette semaine.
« Nous avons pris avec succès des codes d'ordinateurs de divers modèles fonctionnant avec GnuPG (une source populaire d'encodage, en utilisant le standard d'encodage OpenPGP) en quelques secondes », a écrit l'équipe de l'UTA dans l'article, intitulé « Voler des codes de PC en utilisant une radio : des attaques électromagnétiques à moindre coût sur une exponentiation de fenêtres ».
En plus d'OpenPGP, l'équipe a été capable de dupliquer avec réussite les attaques sur d'autres systèmes d'encodages, très sécurisés, y compris RSA et ElGamal.
« L'attaque envoie quelques textes informatiques bien conçus et lorsque ces textes sont décryptés par la cible, ils entraînent l'occurrence de valeurs spécialement structurées dans le logiciel d'encodage », ont déclaré les chercheurs.
En utilisant un appareil qui peut recevoir des signaux radio, une simple radio ou une clé USB pouvant recevoir des émissions et les lire sur l'ordinateur, les chercheurs ont été capables d'observer les fluctuations dans le champ électromagnétique entourant l'ordinateur et de traduire ces fluctuations en frappes de clavier en utilisant un programme d'analyse.
L'article fournit des détails complets sur l'équipement nécessaire (tout est disponible et peu cher dans un magasin local d'électronique ou sur Internet), et sur la façon d'assembler et de connecter les parties, et même de les plier dans un pain pita.

L'équipement détecte les fluctuations dans le champ électromagnétique émis par le matériel informatique (clavier et processeur) lorsque l'ordinateur essaie de décrypter les signaux (les modules d'encodage contiennent des composants qui peuvent être exploités pour fonctionner automatiquement lorsque le texte encodé est rencontré).

En envoyant ces textes pièges, les pirates peuvent voler les codes d'authentification sur l'ordinateur de l'utilisateur, leur autorisant un accès libre aux documents et aux données encodés.

Une attaque PITA pourrait probablement être utilisée par des pirates en cas d'une attaque qui « balaie » des données et les documents d'un ordinateur.

Si ces données sont encodées, il est peu probable que les pirates pourront les lire (en fonction de niveau de complexité du codage), mais avec des clés d'encodage, les pirates pourraient trouver des informations encodées comme des numéros de cartes de crédit ou des mots de passe.

La seule mise en garde est que la pita « espion » a besoin de se trouver à 50 centimètres de la cible.

Mais d'après l'équipe, la totalité de l'opération peut être réalisée en quelques secondes, rendant l'attaque parfaite pour les pirates dans les cafés où de nombreux utilisateurs d'ordinateurs profitent des installations électroniques, du wifi et de boissons pour travailler.

Un pirate pourrait obtenir les codes dans une attaque « en marchant », attaque menée en transportant une « pita empoisonnée » sur un plateau avec de la vraie nourriture. L'étude notait pourtant que la « qualité du signal variait fortement en fonction du modèle de l'ordinateur cible et de la position de logiciel espion ».

L'équipe de UTA n'est pas la première à penser à utiliser des impulsions électromagnétiques pour pirater des systèmes.

En 2014, des chercheurs de l'Université Ben Gourion (UBG) ont pu utiliser un programme pirate sur un téléphone portable pour collecter des radiations électromagnétiques provenant de claviers, de moniteurs et d'autres équipements pour lire des informations importantes.

L'équipe de l'UBG a démontré comment les données collectées par le programme espion, auparavant placé sur un ordinateur (à travers une attaque de phising ou une autre méthode), pouvaient être captées par un téléphone portable qui créait un réseau local en utilisant des impulsions émanant de matériel informatique.

Les informations du système cible pouvaient être captées, même s'il n'est pas connecté à internet ou à un réseau local (Ethernet).

Le pire, a déclaré l'équipe, est qu'il n'y a pas grand chose que les utilisateurs d'ordinateur puissent faire pour éviter ces attaques, si ce n'est éviter les cafés et garder leur ordinateurs loin des pitot.

Malheureusement, l'équipe a déclaré « qu'empêcher la fuite à un bas niveau de prévention est presque impossible » parce que mettre en place des mesures efficaces (comme des cages Faraday) serait très gênant à cause du matériel informatique excessif ou ralentirait la capacité au point que les utilisateurs seraient incapables d'accomplir le moindre travail.

« Même lorsqu'un programme cryptographique est sûr mathématiquement, ses mises en place peuvent être vulnérables à des attaques de réseaux secondaires qui exploitent des émanations physiques », a déclaré l'équipe. Le pirate « peut facilement viser les ordinateurs ».

« Nous avons testé de nombreux ordinateurs de modèles variés », et lorsqu'il s'agit d'une attaque PITA, chaque utilisateur d'ordinateur devrait se sentir concerné.

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

Source : http://fr.timesofisrael.com/pour-pirater-un-ordinateur-une-pita-suffit/
Par David Shamah