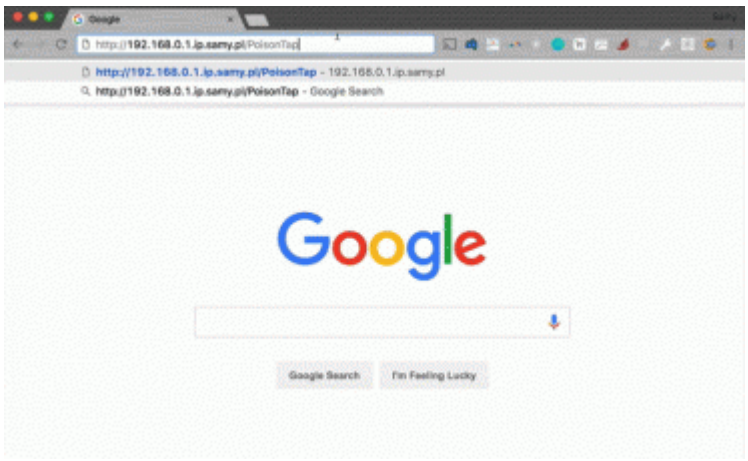
PoisonTap : piratez PC et Mac avec un Raspbery Pi Zero

Le hacker éthique Samy Kamkar vient de lancer une petite bombe dont il a le secret. Le cadeau s'appelle PoisonTap et il s'articule autour du Raspberry Pi Zero (qui coûte 5 dollars) agrémenté d'une bonne dose de logiciels libres. L'objectif de ce module ? Rien de moins que pirater des PC sous Windows ou Mac, même protégés par un mot de passe.

Concrètement, le module se branche sur le port USB (ou Thunderbolt) de l'ordinateur. Mais au lieu d'être reconnu comme un périphérique USB, PoisonTap se fait passer pour une interface Ethernet. Le PC, qui est habituellement en WiFi, envoie donc une requête DHCP pour obtenir l'attribution d'une adresse IP. PoisonTap émet alors une vaste liste d'adresses IP disponibles et en alloue une à l'ordinateur. Un mécanisme classique sur les PC.

Siphonnage en règle, backdoor en prime

Une fois cette adresse IP allouée, le module peut intercepter tout le trafic web non chiffré (à condition qu'un navigateur soit ouvert sur le PC), y compris les cookies d'authentification utilisés pour se connecter à ses comptes. Ces informations siphonnées sont envoyées à un serveur contrôlé par le hacker. De même, PoisonTap en profite pour installer une backdoor permettant de prendre le contrôle à distance des navigateurs et de l'accès au réseau local.



Autre détail et non des moindres, le hack marche sans que le module reste connecté au PC. Il est capable d'infecter la machine en moins d'une minute, assure Samy Kamkar. « *Dans de nombreuses entreprises, c'est assez facile de trouver un ordinateur seul (pause-café, discussion, etc), il suffit juste de brancher PoisonTap pendant une minute et de le débrancher* », résume le hacker. Et d'ajouter : « *même si l'ordinateur est verrouillé, PoisonTap est toujours en mesure de dérouter le trafic réseau et d'injecter la backdoor* ».

HTTPS et fermer le navigateur avant de partir

Pour Craig Smith, directeur de recherche chez Rapid7, interrogé par nos confrères de SiliconAngle, « *Il y a déjà eu des attaques semblables à PoisonTap, mais cette dernière exploite une faiblesse du système très différente. L'émulation d'un périphérique réseau permet d'attaquer tout le trafic sortant du PC ciblé. Cette attaque fonctionne sur les OS Windows et Mac, ainsi que sur les machines verrouillées* ». Et de conclure : « *la méthode est brillante car elle est basée sur la simplicité. A partir d'un Raspberry Pi Zero à 5 dollars, Samy a réussi à rassembler plusieurs attaques habiles* ».

Sur son blog, Samy Kamkar livre quelques pistes de réflexions pour contrer PoisonTap. Sur la partie web, il suggère d'utiliser « *exclusivement* » des connexions HTTPS ou de se baser sur HSTS pour éviter des attaques par dégradation de HTTPS. Sur le poste lui-même, le hacker recommande de « *cimenter* » les ports USB et Thunderbolt (soit les bloquer physiquement), ou de les désactiver, et de fermer son navigateur à chaque fois que l'on s'absente. Tout en se disant conscient de la difficulté de mise en œuvre de pareilles mesures.

A lire aussi :

Une attaque via BadUSB publiée pour forcer les constructeurs à réagir

Tous les périphériques USB sont des pirates en puissance