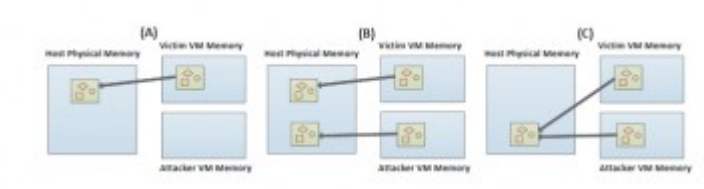
Attaque Flip Feng Shui : Et les VM du Cloud deviennent poreuses

En mars 2015, des experts en sécurité de Google étaient parvenus à réaliser une attaque contre des modules de mémoire vive DDR. Ce procédé, baptisé Rowhammer, consiste à modifier les bits des données stockées dans certaines régions de la mémoire vive. Pour ce faire, des attaquants bombardent de façon répétée des zones de stockage provoquant des modifications des bits d'une zone voisine en raison de la densité des circuits.

Une prouesse technique que d'autres chercheurs en sécurité viennent de peaufiner sous l'appellation Flip Feng Shui (FFS) sur des environnements virtuels. Les experts de l'Université d'Amsterdam en ont fait la démonstration à l'occasion de la conférence Usenix qui s'est déroulée début août. Ils ont couplé deux techniques, Rowhammer citée précédemment et la déduplication mémoire. Cette dernière est utilisée par les fournisseurs de Cloud pour économiser la ressource mémoire des serveurs en partageant des tronçons de données entre plusieurs machines virtuelles.

Un agencement mémoire pour voler des clés

L'attaque hérite son nom de la méthode asiatique qui consiste à agencer un habitat ou un bureau pour optimiser la circulation de l'énergie et ainsi être zen. Flip Feng Shui essaye d'arranger la mémoire partagée entre les VM pour placer y les données sensibles comme des clés de chiffrement. Les attaquants utilisent ensuite la méthode Rowhammer pour récupérer les précieuses informations en question.



Ben Gras, un des universitaires a expliqué à nos confrères d'Ars Technica :« *il y a eu des travaux antérieurs pour montrer que les VM co-hébergées pouvaient dans une certaine mesure s'espionner entre elles, mais notre technique est plus dangereuse* ». Et d'ajouter : « *nous montrons pour la première fois que cette corruption supposée aléatoire peut être en fait ciblée sur des données localisées sur l'ensemble de la pile logicielle, de manière précise et contrôlée* ».

Dans leur présentation, les experts néerlandais ont utilisé Flip Feng Shui depuis une VM pour subtiliser des clés de chiffrement RSA stockées sur une autre VM située dans le même environnement Cloud. Ils ont pu, grâce à cela, obtenir un accès SSH valide et permettre à la VM attaquante de prendre le contrôle de la VM cible. Dans une autre démonstration, ils ont réussi à compromettre la clé GPG utilisée par les développeurs de l'OS Linux Ubuntu afin de vérifier l'authenticité des mises à jour. Ils ont ainsi forcé la VM cible à télécharger et à installer des mises à jour malveillantes.

Les chercheurs prévoient d'affiner leur attaque en ciblant d'autres systèmes de chiffrement basés sur différentes techniques, Digital Signature Algorithm (DSA), Diffie-Hellman, chiffrement sur courbes elliptiques et courbe elliptique Diffie-Hellman.

A lire aussi :

Sécurité du Cloud : le flou demeure entre l'IT et les métiers

Difenso, la start-up de sécurité dans le Cloud, qui monte