Venom, une faille zero day empoisonne des millions de machines virtuelles

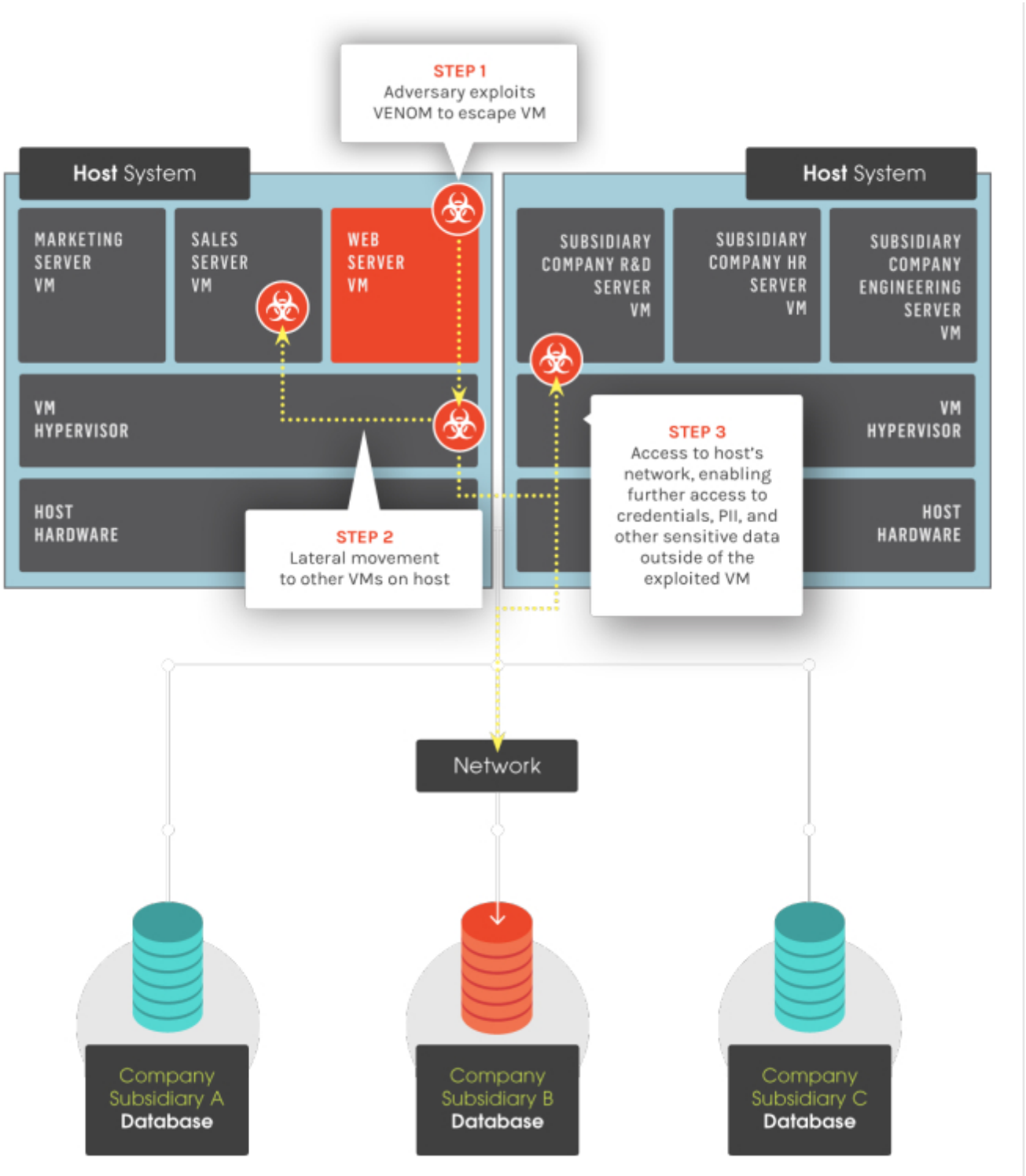
Le nom est fait pour intimider. VENOM, venin en anglais. Derrière cet acronyme qui signifie Virtualized Environment Neglected Operations Manipulation (que l'on pourrait traduire par manipulation d'une fonction obsolète dans un environnement virtualisé) se cache une vulnérabilité découverte par un expert en sécurité de la société CrowdStrike. Jason Geffner a donc trouvé une faille de type zero day en menant une analyse de sécurité sur différentes hyperviseurs.

Le coupable est l'hyperviseur Open Source QEMU (Quick Emulator) et plus exactement dans le contrôleur de disquette virtuelle (floppy disk controller). Cette fonction existe depuis 2004 et elle présente par défaut sur les hyperviseurs KVM, Xen ainsi que sur Oracle VirtualBox. Cela représente une surface d'attaques de plusieurs millions de machines virtuelles qui tournent aujourd'hui dans le monde, sur des serveurs, des appliances ou dans le Cloud. La faille est considérée comme critique pouvant mettre à genoux des fournisseurs de Cloud ou des datacenters d'entreprises.

Pour Jason Geffner, Venom est unique, car elle touche plusieurs types de plateformes de virtualisation (à l'exception de VMware et Hyper-V), elle est agnostique sur les OS (Linux, Windows, Mac OS, etc) et elle permet d'exécuter directement du code arbitraire dans la VM.

Déborder la mémoire du contrôleur

Concrètement, CrowdStrike explique que l'OS invité (*guest*) communique avec le FDC (Floppy Disk Controller) en envoyant des commandes telles que rechercher, lire, écrire, format, etc., au port d'entrée / sortie du contrôleur. Le FDC virtuel de QEMU s'appuie sur une mémoire tampon de capacité fixe pour stocker les commandes et les paramètres associés. Après chaque commande, cette mémoire est effacée à l'exception de deux commandes prédéfinies. Dès lors, un attaquant peut envoyer des commandes particulières pour déborder cette mémoire tampon et exécuter du code malveillant dans l'hyperviseur. (cf schéma ci-dessous).



Les conséquences sont multiples, vol de propriété intellectuelle, fuite de données sensibles et personnelles, etc. A priori, cette faille n'a pas été exploitée souligne Jason Geffner, mais nécessite d'appliquer rapidement des patchs disponibles. Sur son site, CrowdStrike donne deux liens redirigeant vers les correctifs. Pour QEMU Project: https://lists.gnu.org/archive/html/qemu-devel/2015-05/msg02561.html. Et pour Xen Project: http://xenbits.xen.org/xsa/advisory-133.html. Rien n'a été donné pour les solutions KVM.

Plus puissant que Heartbleed ?

Avec la découverte de VENOM, les rapprochements avec Heartbleed (faille dans la librairie de chiffrement OpenSSL) n'ont pas manqué. Jason Geffner a indiqué à nos confrères de *Zdnet* que *« Heartbleed permettait à un attaquant de regarder à travers la fenêtre d'une maison et de recueillir des informations sur la base de ce qu'ils voient. Venom permet de tout casser dans la maison, mais aussi de détruire les maisons du voisinage »*.

Le point commun avec Heartbleed est que Venom pose une nouvelle fois la question de la sécurité du code des solutions Open Source. Avec Heartbleed, des fonds ont été alloués par les grands acteurs IT pour mener des audits et améliorer la sécurité des projets Open Source.

A lire aussi :

Heartbleed : un an après, la faille est tombée dans l'oubli
Après Heartbleed et Shellshock : une faille touche SSL 3.0