Pwn2own : l'Asie fait sauter Safari, Edge, Chrome et Flash Player

Chaque année, le concours de hacking Pwn2own se déroule à Vancouver en marge de la conférence CanSecWest. La 1ère journée a permis la découverte par plusieurs spécialistes en sécurité de failles dans les navigateurs Safari et Chrome, ainsi que dans Flash Player pour compromettre MacOS X et Windows.

Parmi les vainqueurs, il y a la Team 360Vulcan issue la société chinoise de sécurité Qihoo 360 qui a combiné une faille dans Flash Player capable d'exécution de code à distance et une vulnérabilité dans le noyau de Windows pour obtenir une élévation de privilèges. Pour cet exploit, ils ont reçu 80 000 dollars de prime, soit 60 000 dollars pour l'exploit sur Flash Player et 20 000 dollars pour l'élévation de privilèges.

Dans la journée, la même équipe a démontré une attaque via l'exécution de code à distance dans le navigateur Chrome de Google pour Windows et gagnant les droits administrateurs du système. Pour se faire, ils se sont appuyés sur 4 failles : une dans Chrome, deux sur Flash Player et une dans le Kernel Windows. Mais au final, cette attaque a été considérée comme une victoire partielle, car la vulnérabilité sur Chrome avait déjà été soumise à Google par un autre chercheur. Elle ne pouvait donc pas être considérée comme un Zero Day. L'équipe chinoise a néanmoins récolté 52 500 dollars, portant son total de récompense pour la première journée à 132 500 dollars.

Un record pour un sud-coréen

D'autres spécialistes en sécurité ont été récompensés. Ainsi, le chercheur sud-coréen Lee Junghoon, connu sous le nom lokihardt, a démontré une attaque en combinant 4 failles dans Safari pour compromettre MacOS X. Il a gagné au total 60 000 dollars la première journée. Pour mémoire, le chercheur avait remporté l'année dernière, pas moins de 225 000 dollars sur les deux jours de concours.

Il a fallu attendre le deuxième jour pour lokihardt donne la plénitude de son expertise en craquant Edge. Un exploit qui lui a valu une récompense de 85 000 dollars soit la plus forte prime pour un essai unique.

Tencent aligne 3 équipes

Le chinois Tencent était aussi présent en force au Pown2own avec 3 équipes représentant ses différentes filiales. Tencent Security Team Shield a monté un exploit contre Safari à travers 2 vulnérabilités avec à la clé une prime de 40 000 dollars.

La Tencent Security Team Sniper s'en est pris à Flash Player sur Windows avec une élévation de privilège et 50 000 dollars dans la poche. Elle a été l'attraction de la deuxième journée du concours en piratant Safari obtenant ainsi un gain de 40 000 dollars. Elle a récidivé sur Edge en glanant au

passage 52 500 dollars. Enfin la dernière équipe, Xuanwu Lab a tenté un exploit contre Flash dans Edge mais sans succès.

Au final, le compteur des deux journées de concours s'est arrêté à 460 000 dollars de récompense et 21 vulnérabilités jusqu'alors inconnues : 6 pour Windows, 5 pour OS X, 4 dans Flash, 3 dans Safari , 2 sur Edge et 1 pour Chrome. L'année dernière, les participants avaient récolté 550 000 dollars. A noter aussi que cette année, la compétition s'était ouverte aux machines virtuelles de VMware avec une récompense de 75 000 dollars. Mais personne n'a tenté le coup. Peut-être l'année prochaine ?

A lire aussi :

Vente de zero days : une petite entreprise qui ne connaît pas la crise

La politique biaisée de divulgation des zero day de la NSA