Pwn2own : Safari, IE, Chrome et Firefox défaits par les hackers

Chaque année lors de la conférence sur la sécurité, CanSecWest, se déroule une compétition nommée Pwn2own. Ce concours a pour objectif de donner la possibilité à des spécialistes de pirater les navigateurs web et ainsi être récompensés par une prime. Cet événement est organisé par le Zero Day Initiative de HP avec le concours de Project Zero de Google. Depuis 8 ans, plusieurs équipes rivalisent d'ingéniosité pour contourner les différentes protections mises en place par les éditeurs : sandboxing, mesures d'atténuation, etc.

La compétition s'est déroulée pendant 2 jours. Le premier a été marqué par l'exploit d'un **Français, Nicolas Joly** qui a récolté un total de 90 000 dollars pour la combinaison d'une vulnérabilité avec exécution de code à distance, plus une faille dans le sandboxing à la fois dans Flash Adobe et dans Reader. Le jeune expert a expliqué avec nonchalance qu'il était venu en vacances au Canada et qu'il avait finalisé son attaque contre Reader dans l'avion. Ce premier jour, le jury a donné la palme de la vitesse à Mariusz Mlynski qui a pris juste **0,512 seconde pour utiliser une faille dans Firefox** pour obtenir une élévation de privilège dans Windows et exécuter du code à distance. Le chercheur glane au passage 55 000 dollars.

Safari, Chrome et IE11 défaits par un seul hacker

Le second jour de compétition vient de s'achever et s'est concentré sur les autres navigateurs web. Carton plein pour **un hacker coréen, JungHoon Lee, connu sous le pseudo lokihardt** qui a cassé les 3 plus gros navigateurs : Chrome (version beta et stable), Safari et Internet Explorer 11. Pour celui de Google, il a utilisé une technique de débordement de tampon, ainsi que des failles dans le noyau Windows. Pour Safari, il s'est appuyé sur un contournement de la sandbox et une corruption mémoire pour le faire tomber. Enfin, IE11 n'a pas sauvé l'honneur en tombant sur un bug de type TOCTOU (time-of-check to time-of-use) permettant de s'octroyer des privilèges. Il a contourné les défenses de la sandbox avec une injection JavaScript. Au total, le hacker a gagné **225 000 dollars**, cumulant les différentes primes sur les navigateurs.

A noter que dans les records de vitesse, une équipe chinoise, 360Vulcan, a créé la sensation en **pliant IE11 en seulement 17 secondes**. Voilà une nouvelle qui va relancer le débat sur la sécurité des navigateurs et sur celle d'IE en particulier. Ce concours intervient au moment où Microsoft va substituer Internet Explorer par le projet Spartan. Les spécialistes de la sécurité n'ont pas encore travaillé dessus, mais il est probable que le concours 2016 s'attellera à cette tâche. En tous cas, tous les éditeurs vont mettre à jour leur navigateur et pousser prochainement les correctifs auprès des utilisateurs.

A lire aussi :

Combien de millions de BIOS voudriez-vous infecter ?
Un ancien de la NSA se joue de la sécurité de Mac OS X

Crédit Photo : Andrei Lishnesky- Shutterstock