Bingo : 1 million de dollars pour une faille zero day dans iOS 9

Qui se cache derrière l'équipe de hacker qui a réussi à gagner 1 million de dollars pour avoir découvert une faille non-corrigée dans iOS 9 ? C'est la question qui se pose après le tweet de Zerodium à propos de son concours de chasse aux bugs sur l'OS mobile d'Apple. *« Our iOS #0day bounty has expired & we have one winning team who made a remote browser-based iOS 9.1/9.2b #jailbreak (untethered). Congrats! »*, peut-on lire sur Twitter.

Zerodium, société fondée par le français Chaouki Bekrar (à l'origine de Vupen), se concentre uniquement sur *« les vulnérabilités à haut risque et les exploits entièrement fonctionnels »* affectant largement les systèmes d'exploitation, les logiciels, et les terminaux mobiles et fixes. En septembre dernier, elle a lancé un Bug Bounty spécifiquement sur iOS doté d'une prime d'un million de dollars. Un montant très élevé pour ce genre de performance, mais complétement assumé par Zerodium pour se démarquer d'autres concours existant comme Bugcrowd, HackerOne, Synack, Internet Bug Bounty ou encore les programmes dédiés d'acteurs du numérique comme Mozilla et Google.

Un marché proche de la jungle

Le dirigeant de Zerodium n'a pas dévoilé le nom de l'heureux ou des heureux gagnants mais a précisé dans un e-mail à nos confrères de *Computerworld* que l'exploit, ainsi que les vulnérabilités sous-jacentes proposés par l'équipe gagnante ont été testés, analysés et documentés par Zerodium. Apple n'a pas commenté cette annonce.

Ce type de concours pose une fois de plus la question du commerce des failles zero day. Une activité très fragmentée où se côtoie les acteurs IT, les Etats, les cybercriminels et des sociétés comme Vupen, Hacking Team ou Zerodium. Ces dernières veulent découvrir des failles non corrigées sur des OS ou dans des logiciels non pas pour les publier et pour que les éditeurs les corrigent, mais bel et bien pour les vendre au plus offrant, notamment les Etats. Le million de dollars de récompense ne paraît alors pas si exorbitant quand on sait que sur le marché noir du Dark Web, ce type de faille se monnaye à peu près à ce montant-là.

Devant cette organisation du marché, les Etats commencent à vouloir réguler les exportations des brèches critiques à travers l'arrangement Wassenaar, un accord multilatéral de contrôle des exportations pour armes conventionnelles et équipements et technologies à usage à la fois civil et militaire.

A lire aussi :

Hackers, Etats et Dark Web : le marché des failles Zero Day incontrôlable ?
Dans l'ombre de Vupen, Zerodium programme les chasseurs de failles zero day