Bug Bounty : les chasseurs de bug cèdent-ils à la facilité ?

Les Bug Bounty finiraient-ils par lasser les chercheurs de bugs de trouver des failles complexes ? La question est posée par High-Tech Bridge, société spécialisée dans l'automatisation de la sécurité, sollicitée par nos confrères de *The Register*. « *Les entreprises commencent à faire l'expérience de la « fatigue des Bug Bounty », c'est-à-dire quand les chercheurs ont découvert les failles simples et facilement détectables, mais hésitent à passer des jours et des nuits pour rechercher des vulnérabilités plus élaborées* », indique la société. Une manière aussi pour cette dernière de mettre en avant ses solutions de tests de sécurité et d'expliquer qu'elles sont capables de découvrir en 3 jours d'audit au moins 2 vulnérabilités critiques et non détectées par la majorité des entreprises disposant d'un Bug Bounty privé ou public.

Mais au-delà de l'aspect opportuniste de ce débat, la question de la motivation des chasseurs de bugs est posée. Jay Kaplan de Synack, firme spécialisée dans le pen test et la mise en place de Bug Bounty privé, concède qu'il puisse y avoir un spleen sur les Bug Bounty tout en précisant que des équipes correctement organisées et encouragées sont susceptibles d'aller regarder au-delà *« des fruits accessibles »* (les failles faciles à trouver) pour dénicher des défauts plus complexes. Pour expliquer ce manque de « persévérance » des chercheurs, il précise que « *bon nombre des chasseurs de bug ont du travail pendant la journée en tant que spécialiste de la sécurité et ils participent à ces programmes la nuit et les week-ends, ils veulent donc maximiser leurs temps* ».

Un Bug Bounty c'est vivant !

Pour Korben (Manuel Dorne) qui, avec Guillaume Vassault-Houlière RSSI chez Qwant, a monté Bounty Factory, la plateforme européenne de Bug Bounty, « *la plupart du temps, avant de passer sur un bug bounty public, les sociétés préfèrent commencer d'abord par un audit, puis un bug bounty privé. Cela permet d'éliminer un grand nombre de failles faciles à trouver. Après quand le programme s'ouvre au public, les chercheurs doivent pousser leurs recherches un peu plus loin* ».

Pour autant, le phénomène de lassitude n'inquiète pas le blogueur pour plusieurs raisons. « *En fonction de la criticité de la faille, la récompense peut être plus ou moins élevée. Donc si le chercheur en sécurité veut toucher plus d'argent, il devra trouver des choses un peu plus complexes que ce qui peut être remonté par des scanners. En sachant que ces derniers sont interdits dans les programmes. De même, un bug bounty, c'est vivant, et c'est à la société qui l'a lancé, de le faire vivre en étendant le périmètre, en proposant des récompenses plus élevées.* » Sans oublier, « *le côté « jeu / chasse » avec la satisfaction personnelle de trouver des failles que personne d'autre n'a trouvé, et qui pourront aussi faire l'objet de conférences ou d'une ligne sur le CV* ».

Jay Kaplan milite pour une approche hybride. *« Trouver les failles faciles est une tâche répétitive qui peut être automatisée. »* Et d'ajouter : « *Par contre les attaques avancées exigent l'ingéniosité, la créativité et l'expertise humaine.* » Et de citer l'exemple du programme Hack The Pentagon qui travaille sur avec cette approche hybride.

A lire aussi :

Sécurité : OVH lance son premier Bug Bounty

Apple lance enfin son bug bounty sur iOS et iCloud

Crédit Photo : Vchal-Shutterstock