Yogosha, du hacker solitaire à une communauté au service des grandes entreprises

Oubliez tous les clichés que vous avez (encore) sur les pirates informatiques ! Les hackers constituent aujourd'hui des ressources prisées des corporates qui leur demandent d'éprouver leurs systèmes. Pionnière française sur le créneau, la startup Yogosha met en relation hackers éthiques et grands comptes pour sécuriser les produits et infrastructures de ces derniers.

---

8 janvier 2019

"*Pirate : nom masculin. Informatique : personne qui contourne à des fins malveillantes, ou même détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique.*" La définition est la quatrième mentionnée dans le dictionnaire, après l'aventurier voguant sur les mers, le pilleur de trésors et l'inventeur clandestin. Des définitions quasi mythologiques, toutes connotées négativement. Les maîtres français des Lettres feraient pourtant bien de remettre à jour leur lexique. Car une nouvelle catégorie de pirates a émergé, bienveillante cette fois-ci. Le *whitehacking* - aussi appelé *ethicalhacking* - consiste ainsi à éprouver des systèmes d'information en toute légalité pour mieux les sécuriser. Ce nouveau métier transforme un hacker en une sorte de chercheur en cybersécurité.

Pour éviter la peine, autant plaider sa cause auprès du bourreau. Qui mieux que les hackers éthiques peut s'introduire dans le système d'information d'une entreprise pour en déceler les moindres failles ? C'est bien l'idée derrière Yogosha, startup de la cybersécurité qui a vu le jour en 2015. A l'époque, les entreprises étrangères avaient déjà décelé le potentiel de ces hackers qui testaient les limites de leur sécurité. Certains pirates tentaient - avec plus ou moins de succès - de troquer la découverte d'une faille contre un emploi chez Apple ou Facebook. La plupart monnayaient leurs services sur des plateformes confidentielles. Yogosha a décidé d'importer en France la pratique du *bug bounty*, c'est-à-dire la rémunération –dans le cadre d'une activité légale et encadrée en échange de recherche de failles ainsi que des recommandations associées.

Recruter les bons profils

Ciel ! Peut-on vraiment faire confiance à des hackers pour nous protéger ? "*Il faut dissocier les hackers des cybercriminels*", plaide Yassir Kazar, cofondateur et CEO de Yogosha. En effet, la communauté des hackers se scinde en deux groupes distincts : les *white hats*, des pirates aux intentions nobles, qui ne traquent les failles de sécurité que pour mieux en alerter les entreprises ou les autorités afin de construire un Web sécurisé ; et les *black hats*, dont les activités illégales (piratage et revente de coordonnées bancaires, phishing voire, dans les cas

les plus graves, chantage) ont largement contribué à la vision négative que peut avoir le grand public.

"*Les personnes malveillantes n'ont pas d'intérêt à s'inscrire chez nous*", sourit Yassir Kazar. L'entreprise s'adresse aux *white hats*, qui trouvent chez Yogosha un moyen d'exercer leurs compétences dans un cadre légal tout en étant rémunérés. Et, contrairement à ce que l'on pourrait croire, un hacker se recrute comme n'importe quel freelance ! "*Nous leur faisons passer des tests en ligne, que seuls 20% de candidats réussissent*, explique l'entrepreneur. *Puis nous leur soumettons des tests pédagogiques et techniques. Et ceux qui travaillent avec nous bénéficient aussi de la notation de leur travail par les clients.*" Yogosha rassemble ainsi la crème de la crème des gentils pirates.

C'est une bonne situation, ça, hacker ?

Ces derniers sont des freelances ou des salariés spécialistes de la cybersécurité. *La plupart ont fait des études d'informatique et traquent les failles depuis trois à dix ans,* constate Yassir Kazar. Presque tous sont avant tout autodidactes, s'amusant à infiltrer des systèmes d'information dès leur plus jeune âge, grâce à des connaissances glanées en ligne. Il n'existe pourtant pas de portrait-type du hacker et cela se confirme dans leurs niveaux de vie : "*certains hackers peuvent gagner des centaines de milliers d'euros par an"*, affirme Yassir Kazar, bien que la majorité ait des revenus moindres mais toutefois confortables.

Il faut dire que le *bug bounty* peut être ingrat mais paye bien. En effet, les entreprises ne payent que les failles détectées, "*s'il n'y a pas de faille, il n'y a pas de prime*". Un système vertueux qui encourage les sociétés à mieux protéger leurs systèmes. Mais lorsqu'une ou plusieurs failles sont repérées, celles-ci se monnayent selon leur criticité pour l'entreprise. Quelques dizaines d'euros pour le rapport d'une faille peu importante et des tarifs qui peuvent grimper à plusieurs dizaines de milliers de dollars pour une faille d'une extrême gravité détectée chez un grand groupe de la Tech.

Séduire les grands comptes

Un prix que les entreprises sont prêtes à payer tant les enjeux sont colossaux pour elles. "*La cybersécurité n'est pas un luxe*, assène Yassir Kazar, *c'est un enjeu business. Les grandes entreprises ont beaucoup investi dans la transformation digitale et les données sont le nouvel or noir de la société : il faut les protéger.*" Une exigence d'autant plus impérative depuis la mise en place du Règlement général sur la protection des données (RGPD), entré en vigueur au printemps et qui impose aux entreprises de sécuriser les données transitant par leur site. Et malheur à celles qui prendraient la chose à la légère : le propriétaire d'un site web insuffisamment sécurisé s'expose à une amende pouvant chiffrer jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires global. Un risque que peu d'entreprises sont prêtes à prendre - la grande majorité ne disposant de toute façon pas d'une trésorerie suffisante pour y faire face.

"*Les grands comptes cherchent donc à accéder aux ressources les plus pertinentes pour tester leur sécurité et calculer leur retour sur investissement*", précise Yassir Kazar. La plupart des clients disposent de ressources internes pour effectuer les premières séries de tests puis se tournent ensuite vers Yogosha pour traquer les failles les plus retorses. La startup compte dans

ses clients aussi bien des entreprises du CAC40 (Axa) que des ETI (CDiscount) ou certaines scaleups (PeopleDoc). Malgré l'aura qu'elle a déjà su se constituer auprès des grands comptes, la jeune pousse n'hésite pas à intégrer des programmes de mentorat, comme celui de la Française des Jeux, pour soigner son réseau et trouver de nouveaux partenaires.

"*La cybersécurité est un enjeu majeur pour les entreprises et encore davantage dans le cadre d'une transformation digitale de grande ampleur et nos exigences en la matière sont très élevées,* tranche Aurélie Clerc, responsable Accélérateur Client chez FDJ. *Le bug bounty permet de tester nos produits technologiques en complément des tests d'intrusion classiques qui restent essentiels dès lors que le périmètre à évaluer est moins défini*. Durant six mois, les fondateurs de Yogosha et Xavier Etienne, directeur général adjoint de FDJ, ont partagé leur expérience et échangé leurs bonnes pratiques. Une relation de confiance qui a débouché sur la mise en place d'un premier pilote en cours d'industrialisation.

Maddyness, partenaire média de FDJ.

Article écrit par Maddyness, avec FDJ