Flashpoint : le renseignement au service de la cybersécurité

« *Derrière les attaques, il y a toujours des humains* », explique Gaël Barrez, responsable EMEA de Flashpoint. Cette société américaine a décidé de conquérir l'Europe et la France en particulier, après avoir fait ses preuves aux Etats-Unis. Elle est née au début des années 2000, « *après le traumatisme des attentats du 11 septembre, les agences de renseignement ont demandé à des spécialistes d'aller voir ce qui se passer sur Internet et sur les réseaux sociaux dans le cadre de la lutte anti-terroriste, cette structure est devenue Flashpoint* », indique le dirigeant.

Puis à la fin des années 2000, « *le mode de communication des criminels à basculer en se détournant de Twitter et Facebook pour se réunir au sein de communautés, avec un contrôle stricte pour y entrer (entretiens, cooptation, niveau d'expertise élevé). Ils étaient donc moins visibles* », poursuit Gaël Barrez. Dotés de plusieurs experts, Flashpoint a réussi à intégrer ces forums, communautés, au sein du Dark web et du Deep web.

Infiltrer le gratin du Dark et Deep Web

Dès lors, la société américaine a diversifié son activité en s'intéressant à la cybersécurité pour les entreprises. « *L'objectif est de connaître les individus, les groupes, quels sont leurs liens, leurs expertises et leurs cibles. Nous sommes dans le renseignement », précise le responsable.* Au sein de la face cachée et sombre du web, il distingue plusieurs niveaux, *« le niveau 0 regroupe les vantards inintéressants, le niveau 1 englobe des amateurs, des juniors qui apprennent et font l'objet d'une surveillance. Le niveau 2 correspond aux experts capables de mener des attaques d'Etat* ».

Cette dernière catégorie est la plus intéressante, « *ils ont une maîtrise parfaite de l'environnement et des rapports humains, ils sont capables de coopérer, d'obtenir de l'aide, de s'échanger des exploits* », observe Gaël Barrez. Ce niveau fait l'objet de toutes les attentions des consultants de Flashpoint. Ces derniers sont aussi des experts dans leur domaine, maîtrisant les différentes langues des cybercriminels, « *y compris l'argot du monde cyber* » et disposant de plusieurs profils.

Des rapports, du sur-mesure et des tendances

Grâce à cette présence au sein de ces communautés, Flashpoint fournit à ses clients via la plateforme BRI (Business Risk Intelligence) des rapports « *exploitables par les entreprises* » sur les différentes menaces comme cela a été le cas pour WannaCry ou NotPetya. Concrètement, les échanges sur le Dark et le Deep Web sont retranscrits manuellement puis intégrés dans une base de données, en liant par exemple une attaque avec le profil d'une personne ou d'un groupe. « *L'idée est de faire de la reconnaissance pour dégager des tendances, nous travaillons en amont pas a posteriori* » insiste Gaël Barrez. Et de citer l'exemple de Swift, « *on a constaté que 2 ou 3 ans avant les attaques, il y avait des échanges assez brouillons sur le sujet. Puis au fil du temps, les demandes étaient plus précises, techniques sur les types de format, comment les altérer, etc* ».

Au départ les clients de la firme américaine étaient principalement les gouvernements, mais l'ouverture à la cybersécurité a suscité un intérêt auprès du monde financier et bancaire. Aujourd'hui, elle adresse 18 verticaux, allant des télécoms, des industriels des médias, des sociétés de transport, etc. Dans son portefeuille, Flashpoint propose également des services sur mesure par exemple sur le vol de données, « *nous avons intercepté un jour la vente d'une base de données d'une grande entreprise sur le Dark Web par une personne. Nous avons alerté cette société, elle a identifié la base de données dérobée, ainsi que le salarié responsable* ». Par ailleurs, le spécialiste du renseignement cyber facilite les échanges entre entreprises du même secteur pour coopérer sur des risques communs.

Sur la concurrence, Gaël Barrez reste évasif en vilipendant la collecte automatique de certains éditeurs sur le Dark et le Deep Web. « *Nous sommes sur l'humain, cela demande du temps, de la patience* », conclut Gaël Barrez.

A lire aussi :

Skype, la messagerie préférée des cybercriminels

Comment le ransomware est devenu le gagne-pain des cybercriminels

Photo credit: medithIT via VisualHunt / CC BY