Profession : chasseur de hackers

Chez un éditeur comme Trend Micro, on trouve des armées de spécialistes du traitement des menaces qui chaque jour frappent les clients de l'éditeur. Des équipes spécialisées, fortement taylorisées, qui analysent mails, fichiers ou liens suspicieux (lire notre reportage dans le principal laboratoire de l'éditeur, regroupant 1 200 personnes à Manille). « *Mon équipe est très différente* », dit d'emblée Ryan Flores. Ce jeune chercheur en sécurité fait partie de ce que Trend Micro appelle sa 'Forward Looking Threat Research' (FTR), regroupant une **vingtaine de spécialistes répartis à travers le globe**. Moyenne d'âge : 35 ans. « *Cette équipe n'a que 6 ans d'ancienneté*, explique Ryan Flores, issu des laboratoires de Trend Micro à Manille et qui dirige aujourd'hui l'équipe FTR pour la partie Asie-Pacifique. *Elle a été constituée à l'initiative du Pdg du groupe afin de préparer l'évolution de nos produits* ». L'objectif est de mieux comprendre l'évolution des menaces, via des enquêtes au long cours sur les pratiques des cybercriminels, mais aussi de servir d'atout marketing à l'éditeur (tous les spécialistes se servent des recherches des équipes de ce type comme support de communication).

« *La plus courte de nos investigations a demandé 6 mois avant la publication de l'article détaillant les résultats. La plus longue a approché les 4 ans* », détaille Ryan Flores. Dans de nombreux cas, les chercheurs de Trend Micro collaborent sur ces affaires avec des CERT (Computer Emergency Response Team, centres d'alertes et de réactions aux attaques), voire avec des concurrents. Sur certaines affaires, l'industrie s'est notamment fédérée autour de groupes de travail (comme le Conficker Working Group). « *Mais la philosophie de notre équipe reste centrée sur la collaboration avec les forces de l'ordre. Nous estimons avoir remporté une victoire quand nous avons mené une recherche intéressante qui aboutit à l'arrestation des cybercriminels* », détaille le chercheur philippin. Un des membres de la FTR a ainsi été détaché pour deux ans auprès d'Interpol.

Incognito ou sous une fausse identité

Les activités de la FTR ont ainsi facilité l'arrestation d'auteurs de ransomware ciblant l'Espagne (avec une interpellation à Dubaï, lors d'un transit à l'aéroport), d'un Algérien spécialiste de vol de données bancaires (cueilli lors de ses vacances en Thaïlande) ou encore d'un gang de réfugiés nord-coréens pratiquant l'extorsion après des « *sex chat* » dans toute l'Asie. « *Les cybercriminels tendent à exploiter un filon au maximum si je me fie à mon expérience* », s'amuse Ryan Flores. Ce qui les conduit souvent à échouer entre les mailles des filets des forces de l'ordre.

Cette proximité avec les services de police explique aussi qu'une bonne partie des membres de la FTR demeurent incognito ou opèrent sous de fausses identités. Ce qui n'est pas le cas (au moins officiellement) de Ryan Flores, qui joue un rôle de porte-parole officiel de la FTR pour l'Asie. « *Par ailleurs, nous n'employons pas d'anciens blackhat (hacker mal intentionné, NDLR). Et nos règles d'engagement interdisent toute action réellement offensive contre les infrastructures des cybercriminels. Notre équipe chargée de la conformité réglementaire inspecte régulièrement nos activités.* » Des règles d'engagement qui, peut-on noter, n'interdisent en revanche pas de tromper les hackers, par exemple en leur donnant de fausses informations ou en opérant sous de fausses identités.

Un Cloud pour le cybercrime

Cette plongée quotidienne dans le monde du cybercrime permet aussi aux chercheurs de mieux en comprendre les rouages. Des rouages bien huilés, qui font de plus en plus ressembler ce continent obscur (le darknet) à une **véritable industrie**. « *Les créateurs des outils d'infections ne sont que quelques dizaines, quelques centaines au plus (le FBI parle de 150 personnes dans le monde, NDLR). Ils vendent leurs logiciels malveillants et offrent parfois même un support technique, comme un éditeur de logiciels classique. Ces outils sont ensuite exploités par des opérateurs, parfois sans grandes compétences techniques. Cette structuration du marché du cybercrime a démarré voici 3 à 4 ans* », détaille Ryan Flores.

Comme dans l'économie officielle, ces producteurs et utilisateurs de logiciels s'appuient sur une infrastructure dans le Cloud. « *Certains fournisseurs de services sont au minimum complices des cybercriminels. Et il existe même des prestataires dédiés aux activités délictueuses*, assure le chercheur. *Ces derniers sont souvent situés en Russie ou dans les ex-pays de l'Union soviétique.* »

A lire aussi :

Les logiciels de sécurité soutenus par la demande des entreprises
FIC 2015 : les hackers ont gagné une bataille, pas la guerre