http://info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,C1761,I1602,Zoom-a33ebda671ee5dd104e282518ac0e938.htm?KM_Session=a2b57cf5f3d74b22191a0e97abd96954

Nadine Touzeau (net-profiler) : « Les actes avatarisés sont bien plus violents que dans le réel »

18-04-2014

Analyste comportementale et environnementale, profiler et net-profiler, Nadine Touzeau nous apporte un éclairage psychologique sur les cybercriminels.

Vous venez d'achever la rédaction d'un ouvrage sur le net-profiling. Qui sont les cybercriminels ?

Ce sont surtout des jeunes qui s'intéressent aux nouvelles technologies de l'informatique et d'Internet. Ils vivent au cœur du monde d'aujourd'hui où l'on ne peut plus se passer des ordinateurs, des smartphones ou des tablettes. Au niveau psychologique, ils font preuve d'un esprit très analytique. A côté de cela, il y a une grande variété de profils de cybercriminels : du jeune qui veut simplement réaliser un exploit jusqu'au vrai bandit qui travaille pour des réseaux malveillants nationaux et internationaux. On peut essayer de dresser une catégorisation des profils psychologiques mais la réalité prouve qu'il n'y a que des exceptions.

Y a-t-il des ressemblances entre les comportements dans les mondes réel et virtuel ?

Plus exactement, il y a des comportements et des attitudes similaires entre les criminels et les cybercriminels mais ils n'appréhendent pas du tout la même façon de se déplacer car le anotion spatiale est différente entre les deux profils. De même que le corps humain ne ment jamais (en d'autres termes, il trahit nos émotions ou sentiments), on arrive à déceler des attitudes qu'il convient d'analyser même s'il s'agit d'une cyberattitude. On arrive ainsi à déterminer si l'on a affaire à une ''petite main'', un maillon important, un jeune qui veut faire un exploit ou un jeune qui en a commis un sans le faire exprès.

Comment dresser des profils alors que les personnes se cachent derrière leur écran ?

Clics, commentaires, actions... toute action sur le réseau laisse des traces. Tout l'art consiste d'abord à analyser ces traces avant de voir ce qu'elles peuvent révéler. Les petits délinquants vont faire des coups ponctuels. D'autres vont jusqu'à monter de faux sites Web. D'autres encore se spécialisent dans l'escroquerie de certaines communautés.

Travaillez-vous avec des informaticiens ?

Non, pas pour l'instant. Mais j'ai des échanges avec certains d'entre eux eux.

Sur quels types d'affaire avez-vous travaillé ?

Pour des entreprises qui ont perdu des marchés, des actifs en propriété intellectuelle en phase de R&D. On a trop tendance à croire que seules les entreprises du CAC 40 sont victimes de la cybercriminalité. Mais j'ai travaillé pour une société de services de 25 salariés qui réalise ses affaires au plan régional région. Cette entreprise, qui avait été infiltrée, avait perdu 40% de son chiffre d'affaires. J'ai enquêté, trouvé des preuves. Derrière l'infiltration, il y avait des réseaux malveillants nationaux et internationaux...

Pourquoi la cybercriminalité augmente-t-elle ?

Face aux agressions, on a toujours rajouté des moyens techniques. Or, en répondant à la technique par la technique, on n'est pas dans la pro-activité. On subit. On se rend compte que ce n'est pas un moyen qui attaque mais un être humain. Certes, les pirates mettent en place les moyens nécessaires pour atteindre leurs objectifs. C'est avec leur cerveau ou même un réseau de cerveaux qu'ils attaquent.

En matière de comportement, quelle différence y a-t-il entre les mondes réels et virtuels ?

La grande différence, c'est la notion spatiale. Dans le monde réel, un individu qui veut tuer sa belle-mère située à 100 km va passer des heures à faire ses repérages, trouver un mode operandi... le tout physiquement. Entre l'idée et le passage à l'acte, il y a toute une graduation. De son côté, le cybercriminel a tous ses outils de malveillance sous la main. Notamment, il va utiliser un avatar. Or cette ''avatarisation'' modifie le comportement du délinquant. Tout d'abord, il va se composer une image assez flatteuse lui-même. Ensuite, avec cette image, il peut agir instantanément et plus librement que dans le réel. Derrière l'écran, tout lui est permis. Mais dès lors qu'il vit au travers de son ou de ses avatars pour agir, il y a une déviance entre l'inconscient et le subconscient. Le cybercriminel en tire alors une certaine jouissance. Le problème, c'est que ses cyberactes ne sont pas mesurés. En revanche, ses actes peuvent avoir des conséquences désastreuses dans le monde réel, sur des personnes réelles : les salariés de l'entreprise attaquée, ses fournisseurs... Les actes avatarisés qui causent du tort à des personnes réelles, connaissent une inflation bien plus importante que dans le réel. En général, les victimes sont très stupéfaites surprises par l'ampleur de cette violence de ces attaques. C'est d'ailleurs le sujet de mes prochaines recherches.

Propos recueillis par Erick Haehnsen